TABLA DE CONTENIDO

1. OBJETIVO 2
2. DIRECCIONAMIENTO ESTRATÉGICO 2
2.1. MISIÓN 2
2.2. VISIÓN 2
2.3. PRINCIPIOS Y VALORES 2
3. POLITICAS Y OBJETIVOS 2
3.1. POLÍTICA SIG 2
3.2. OBJETIVOS SIG 3
4. ALCANCE 3
5. REQUISITOS GENERALES 3
6. RESPONSABILIDADES 4
7. DEFINICIONES 5
8. DESCRIPCIÓN 16
8.1. ESTÁNDARES DE SEGURIDAD INFORMÁTICA 16
8.1.1. INFRAESTRUCTURA DE RED DEL CDAV 16
8.1.1.1. *INFRAESTRUCTURA* 16
8.1.1.2. *REDES* 16
8.1.2. SISTEMAS DE INFORMACIÓN 18
8.1.3. INFORMACIÓN 20
8.1.4. SERVICIOS 20
8.1.5. SEGUIMIENTO AL PROCESO 21
8.1.6. RIESGOS 23
8.1.7. PLAN DE CONTINGENCIA 23
8.1.8. PÓLIZAS DE SEGURO VIGENTES 24
8.2. POLÍTICAS DE SEGURIDAD INFORMÁTICA 25
8.2.1. POLÍTICA DE GOBIERNO DIGITAL: TIC PARA LA GESTIÓN. 25
8.2.2. POLÍTICAS INTERNAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 26
8.2.3. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA. 26
8.2.4. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD AMBIENTAL 28
8.2.5. POLÍTICAS Y ESTÁNDARES DE INFRAESTRUCTURA 29
8.2.6. POLÍTICAS Y ESTÁNDARES DE SISTEMAS DE INFORMACIÓN 35
8.2.7. POLÍTICAS Y ESTÁNDARES DE INFORMACIÓN (DATOS) 39
8.2.8. POLÍTICAS Y ESTÁNDARES DE OPERACIÓN 41
8.2.9. POLÍTICAS, ESTÁNDARES DE SEGURIDAD EQUIPOS FINANCIEROS 44
8.2.10. POLÍTICA PARA LA RENOVACIÓN Y ACTUALIZACIÓN TECNOLÓGICAS. 48
9. DOCUMENTOS CITADOS 55
10. VALIDACIÓN DOCUMENTAL 55

1. OBJETIVO

Servir como apoyo a los diferentes servicios que presta el Centro de Diagnóstico Automotor del Valle Ltda., y que requieren de un componente informático para su adecuada ejecución y seguimiento, garantizando la seguridad, integridad, confidencialidad y disponibilidad de la información y por ende la continuidad del negocio.

2. DIRECCIONAMIENTO ESTRATÉGICO

2.1. Misión

Promover una cultura de movilidad, seguridad vial y respeto por el medio ambiente; a través de la formación y evaluación de la capacidad de conducción, revisión del estado de los vehículos, servicios y programas de tránsito y transporte.

2.2. Visión

Ser la empresa líder de servicios de tránsito y transporte en el Valle del Cauca, destacada por la calidad, legalidad y generación de valor a sus grupos de interés, y reconocida por el aporte a la movilidad y seguridad vial.

2.3. Principios y Valores

Los principios tienen como función primordial el desarrollar hábitos y actitudes positivas en los funcionarios de la Entidad, que permitan el cumplimiento de los fines institucionales para beneficio de la comunidad.

El Centro de Diagnóstico Automotor del Valle Ltda., se caracteriza por los principios y valores descritos en el documento interno del proceso de Desarrollo Humano - Código de Integridad.

3. POLITICAS Y OBJETIVOS

3.1. Política SIG

El Centro de Diagnóstico Automotor del Valle Ltda., como organismo de apoyo a la movilidad, seguridad vial y medio ambiente, mediante la presente política se compromete a mantener a la vanguardia en sus tecnologías de la información para

entregar a los usuarios servicios de calidad, garantizando la diligencia en sus procesos, la seguridad, confidencialidad y oportunidad de la información.

3.2. Objetivos SIG

- ✓ Mantener a la vanguardia en tecnología para prestar servicios eficientes.
- ✓ Que los procesos se realicen con diligencia, dentro de los términos legales y sin dilaciones injustificadas.
- ✓ Garantizar la seguridad, confidencialidad y disponibilidad de la información.

4. ALCANCE

Las políticas y estándares de Seguridad de la Información aplican a todo el Centro de Diagnóstico Automotor del Valle, sus funcionarios, contratistas y practicantes, personas con relación contractual que preste algún servicio a la empresa y que tengan acceso a información a través de los documentos, equipos de cómputo, infraestructura y canales de comunicación, incluye procesos y tecnologías vinculados con la empresa. Inicia con la definición de la estructura tecnológica del CDAV y finaliza con las instrucciones para la operación de la plataforma tecnológica.

5. REQUISITOS GENERALES

5.1. NTC-ISO/IEC 17020. Evaluación de la conformidad. Requisitos para el funcionamiento de diferentes tipos de organismos que realizan la inspección.

5.2. NTC 5385. Centros de Diagnóstico Automotor. Especificaciones del servicio.

5.3. NTC 31000. Gestión del riesgo, principios y directrices.

5.4. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

5.5. Decreto No. 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

5.6. Decreto No. 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

5.7. Ley 23 de 1982. Sobre Derechos de Autor.

6. RESPONSABILIDADES

6.1. Gerente: Es el responsable de garantizar la disposición de recursos necesarios, de forma oportuna para la implementación, seguimiento y evaluación de los programas y proyectos de la dirección de tecnología y sistemas de información del CDAV.

6.2. Dirección de Tecnología y Sistemas de Información: Es el responsable de dirigir y garantizar el proceso de formulación y ejecución de políticas, estrategias, planes, programas y proyectos orientados a fortalecer la plataforma tecnológica, de comunicaciones y de sistemas de información del Centro de Diagnóstico Automotor del Valle - CDAV, garantizando la adecuada y oportuna tecnología para cumplir con los objetivos estratégicos del Centro de Diagnóstico Automotor del Valle - CDAV, gestionando con efectividad las integraciones, los desarrollos, proceso de soporte a los aplicativos, dotación de dispositivos y equipos para los colaboradores de conformidad con la normatividad legal vigente y los procedimientos establecidos.

6.3. Líder de Optimización: Es el responsable de Liderar, planear, ejecutar y hacer seguimiento a los proyectos estratégicos asignados bajo su responsabilidad, apoyando la optimización tecnológica mediante iniciativas vinculadas a automatizar procesos en las diferentes áreas del Centro de Diagnóstico Automotor del Valle – CDAV, de conformidad con las disposiciones legales vigentes sobre la materia.

6.4. Profesional universitario grado 4: Efectuar labores de análisis, diseño, programación e implementación de sistemas de información orientados a fortalecer la plataforma Tecnológica y los Sistemas de Información del Centro de Diagnóstico Automotor del Valle – CDAV, de conformidad con las normas legales vigentes, los protocolos y políticas institucionales establecidas.

6.5. Profesional universitario grado 6: Coordinar, supervisar, controlar y evaluar las bases de datos y los sistemas de comunicación *(incluye internet, datos y voz)* del Centro de Diagnóstico Automotor del Valle – CDAV.

6.6. Técnico administrativo Grado 7: Coordinar y ejecutar las labores de soporte técnico y tecnológico requerido por las diferentes dependencias y áreas funcionales del Centro de Diagnóstico Automotor del Valle – CDAV. Así mismo

realizar la valoración técnica a cada solicitud recibida de las dependencias para la renovación o adquisición del inventario y mantenimiento tanto preventivo como correctivo de los equipos de la entidad.

6.7. Directores de áreas: Responsables de formular las solicitudes de actualización tecnológica de sus dependencias.

7. DEFINICIONES

TÉRMINO	SIGNIFICADO
(A)	
Acceso	Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.
Acceso Físico	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo, o bien usar.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Activo de información	Este tipo de activo hace relación a los datos o información que tiene para la entidad valor en los procesos del modelo de negocio, independientemente de su ubicación. Puede ser un documento físico, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.
Amenaza	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Amenaza informática	Es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS), del Centro de Diagnóstico Automotor del Valle Ltda.
Análisis de riesgos:	Uso sistemático de una metodología para estimar los riesgos de los activos o bienes de información e identificar sus fuentes.
Autenticación	Garantía de que un el servidor público es quien realmente se autentica en el sistema al cual está intentando ingresar, se

TÉRMINO	SIGNIFICADO
	realiza a través de la validación de directorio activo del Centro de Diagnóstico Automotor del Valle Ltda.
Antivirus	Los programas antivirus exploran la memoria del ordenador y las unidades de disco en busca de virus. Si localizan un virus, la aplicación informa al usuario y puede limpiar, eliminar o poner en cuarentena cualquier archivo, directorio o disco afectado por el código malintencionado.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.
(B)	
Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
(C)	
Caballo de Troya	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo FUNCIONES NO DESEADAS.
Caché	Cuando se descarga una página Web, los datos se guardan en “caché”, lo que quiere decir que quedan temporalmente almacenados en su ordenador. La próxima vez que se utilice la página, en vez de solicitar el archivo al servidor Web, su navegador accederá a ella de manera automática desde la memoria caché, con lo que la página se cargará más rápido
Centros de cómputo, Centros de Procesamiento de datos o data center.	Es una Entidad, Oficina o Departamento que se encarga del procesamiento de datos e información de forma sistematizada. El procesamiento se lleva a cabo con la utilización de ordenadores que están equipados con el hardware y el software necesarios para cumplir con dicha tarea, estas computadoras se encuentran interconectadas en red.
Confidencialidad	Se refiere a que la información no sea divulgada a personal NO AUTORIZADO para su conocimiento, Propiedad que determina que la información no esté disponible ni sea revelada a individuos, Entidades o procesos no autorizados.
Continuidad del negocio	Plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

TÉRMINO	SIGNIFICADO
Control	Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, ya sean de carácter administrativo, técnico o legal.
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso NO AUTORIZADO y permitir acceso autorizado a un activo.
Copia de seguridad	Copia de respaldo de la información.
Cookie	Bloques de texto colocados en un archivo del disco duro del ordenador. Las páginas Web utilizan las cookies para identificar a los usuarios que las visitan.
Copyright	Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida.
Criticidad	Medida del impacto que tendría la Entidad debido a un incidente de seguridad de un sistema y que éste no funcione como es requerido
Custodio	Ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área
(D)	
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una Entidad autorizada.
DTYSI	Se refiere a la Dirección de Tecnologías y Sistemas de Información de Centro de Diagnóstico Automotor del Valle Ltda.
Dominio	Sistema de denominación de host en internet. Conjunto de caracteres que identifica y diferencian los diferentes sitios.
(E)	
Encriptación	Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encriptación como tal, no existe en el lenguaje español, el término correcto es CIFRADO DE DATOS.
Encargado de Activo de Información	Individuo, cargo, grupo de trabajo o proceso designado por la entidad para administrar y hacer efectivos los controles que el responsable del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

TÉRMINO	SIGNIFICADO
Equipo de Cómputo	Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información
Evento de Seguridad de la Información	Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.
Endian	Es una distribución OpenSource de Linux, desarrollada para actuar no solamente como cortafuegos sino como solución integral para proteger su red de amenazas externas, ofreciendo todos los servicios que brinda un UTM (Gestión Unificada de Amenazas) fácil de usar e instalar.
Equipo y/o terminal móvil:	Computadoras con diferentes capacidades como: procesamiento, memoria, software, conexión permanente o intermitente a una red datos e Internet, que han sido destinados para una función específica, pero se pueden llevar a cabo otras funciones más generales gracias a su facilidad de uso y portabilidad (p.e., computadores de escritorio, portátiles, tabletas, Smartphone, entre otros).
(F)	
Falta administrativa	Es la consecuencia que resulta del incumplimiento de la normatividad.
Free (Software libre)	Programas que se pueden bajar desde internet sin cargo.
Fallo de seguridad	es cualquier incidente que la compromete, es decir que pone en peligro cualquiera de los parámetros con los que se valora la seguridad: la confidencialidad, la disponibilidad o la integridad de la información.
FTP	Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
(G)	

TÉRMINO	SIGNIFICADO
Glpi	Glpi: Herramienta web de código abierto que ofrece una gestión integral del inventario informático de una empresa, además de incluir un sistema de gestión de incidencias.
Gestión de claves	Actividad dirigida a establecer y aplicar los controles que se realizan mediante la implementación de claves criptográficas
Gestión de incidentes de seguridad de la información	Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información
Gestión de riesgos	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la identificación, evaluación y el tratamiento de riesgos
Gusano	Véase Caballo de Troya.
(H)	
Hardware	Se refiere a las características técnicas y físicas de las computadoras.
Habeas data	Derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos
Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.
(I)	
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice.
Incidente de Seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Infraestructura	Conjunto de elementos o servicios que se consideran necesarios para la creación y funcionamiento de una organización cualquiera
Infraestructura Cibernética (Ic):	Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO)
Infraestructura Crítica (IC)	Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
Infraestructura Crítica Cibernética (ICC)	Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es

TÉRMINO	SIGNIFICADO
	indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.
Infraestructura de Procesamiento de Información	Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.
Infraestructura Estratégica (IE)	Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales
Infraestructura Estratégica Cibernética (IEC)	Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales
Información	la información es un conjunto organizado de datos procesados para llegar a una deducción lógica.
Integridad	Se refiere a la pérdida ó deficiencia en la autorización, totalidad ó exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
Internet o World Wide Web (www)	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo.
Inventario de activos	Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del MSPI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
(L)	
Lenguaje de Programación	Sistema de escritura para la descripción precisa de algoritmos o programas informáticos.
(M)	
Maltrato, descuido o negligencia	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad del Supremo Tribunal de Justicia.

TÉRMINO	SIGNIFICADO
Mecanismos de seguridad o de control	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medio removible, (medios magnéticos, medios de almacenamiento)	Medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB, o similares que a futuro llegaren a utilizarse para este fin.
Metodología	Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente.
Modelo de Seguridad y Privacidad de la Información (MPSI)	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de comunicaciones (red telefónica). Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.
(N)	
Nagios:	Software de código abierto que permite monitorear redes informáticas manejando sistemas de alertas por cualquier evento de desconexión
“Necesidad de saber” principio o base	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.
Nodo	Punto principal en el cual se les da acceso a una red a las terminales o computadoras.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.

TÉRMINO	SIGNIFICADO
(O)	
Obsolescencia	La obsolescencia es la caída en desuso de máquinas, equipos y tecnologías motivada no por un mal funcionamiento del mismo, y/o por un insuficiente desempeño de sus funciones en comparación con las nuevas máquinas, equipos y tecnologías introducidos en el mercado.
Ossim	Sistema de seguridad que permite realizar auditoría y control de seguridad de una red, conocer que está ocurriendo en una red en tiempo real, y si hay alguna anomalía en la misma intentar a que se debe: ataques, fallos, desde fuera, desde la propia red, que usuarios, quien consume ancho de banda y en qué servicios.
Osc inventory (Open Computer Software):	Software de código abierto que permite recopilar información sobre el hardware y software de los equipos que hay en la red.
(P)	
Página Web	Ver sitio web.
Parche (patch)	Un parche (algunas veces llamado FIX) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la funcionalidad del mismo.
Password	Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6 a 10 caracteres.
Patch Panel (Panel de Conexiones):	Elemento encargado de recibir todos los cables del cableado estructurado.
Programas malintencionados (malware)	Término genérico utilizado para describir programas malintencionados tales como virus, troyanos, spyware o contenidos activos malintencionados.
Parte interesada externa	Ente de control definido dentro del contexto Gubernamental y que se encuentre autorizado para realizar revisiones a través de auditorías o, actúe como asesor para el monitoreo, revisión y actualizaciones del Modelo de Seguridad y Privacidad de la Información del Centro de Diagnóstico Automotor del Valle Ltda.
Parte interesada interna	servidor público que pertenezca a cualquier área del Centro de Diagnóstico Automotor del Valle Ltda., así como sus proveedores y usuarios finales de los servicios de la Entidad.
Proceso	Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas

TÉRMINO	SIGNIFICADO
Propietario/responsable	Individuo, cargo, grupo de trabajo o proceso, designado por la entidad, que tiene la responsabilidad de identificar, definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información a su cargo.
(R)	
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene. combinación de la probabilidad de un evento y sus consecuencias
Red LAN	Red informática de comunicación que se extiende por un área limitada.
Registrador de teclas (Keylogger)	Un keylogger (derivado del inglés: key (tecla) y logger (registrador); registrador de teclas) es un tipo de software o un dispositivo de hardware específico, que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet a un interesado. El objetivo de utilización de este tipo de mecanismos en equipos o terminales con acceso privilegiado a transacciones financieras, es el de robar información de acceso y demás medios de autenticación en los sistemas o portales transaccionales dispuestos por las entidades financieras, con el propósito de poder usar esta información con fines fraudulentos.
Router (Enrutadores)	Dispositivo que proporciona conectividad a nivel de red, su función principal consiste en enviar o encaminar paquetes de una red a otra.
Responsable de activo de información	Es el Individuo, cargo, grupo de trabajo o proceso, designado por la entidad de velar porque la información a su cargo sea protegida de manera adecuada.
Riesgo	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.

TÉRMINO	SIGNIFICADO
(S)	
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Segregación de tareas	Reparto de tareas sensibles entre distintos servidores públicos, proveedores y contratistas para reducir el riesgo del mal uso, deliberado o por negligencia, de los sistemas o información.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Sensibilidad	Nivel de impacto que una divulgación no autorizada podría generar
Servicio	Es cualquier acto o desempeño que la entidad o sus servidores públicos pueden ofrecer a otras personas, en desarrollo de su objeto y funciones.
Sitio Web	El sitio web es un lugar virtual en el ambiente de internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Software	Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Software Antivirus	Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.
Soportes físicos	Datos en soporte papel (cartas, informes, normas, contratos) o en medios de almacenamiento físico.
Switch	Dispositivo de red que filtra y direcciona paquetes a las direcciones destinadas. El switch opera en la capa de enlace de datos del modelo OSI, y que sirve para conectar varios elementos dentro de una red. Estos pueden ser un pc, una impresora o cualquier aparato que posea una tarjeta ethernet.
(T)	
Tarjeta inteligente	Es una tarjeta de plástico del tamaño de una tarjeta de crédito que incorpora un microchip, en el cual se puede cargar datos como números telefónicos, pagos realizados a través de

TÉRMINO	SIGNIFICADO
	medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.
Terceros	Toda persona jurídica o natural, que se relacionan con el Centro de Diagnóstico Automotor del Valle Ltda., como proveedores o consultores, que proveen servicios y/o productos a la Entidad.
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
Tratamiento de riesgos	Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
(U)	
User-Id (identificación del Usuario)	Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, número o signos.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).
Usurpación de identidad	Ocurre cuando un atacante finge ser usted o se hace pasar por usted. Adquiere información clave, tal como su número de la Seguridad Social, su fecha
(V)	
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o diskettes de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental. Fallo no intencionado de un programa que causa acciones que ni el usuario ni el programa pretendían realizar

8. DESCRIPCIÓN

8.1. Estándares de Seguridad Informática

8.1.1. Infraestructura de Red del CDAV

8.1.1.1. *Infraestructura*

La infraestructura de red que posee el CDAV, está compuesta por un cableado UTP de datos y voz niveles 5 y 6 de igual forma corriente eléctrica que cumple con los estándares reglamentarios.

Las tomas eléctricas de corriente regulada se encuentran debidamente identificadas con color Naranja y las tomas de corriente normal son de color Blanco. En las tomas de regulada se encuentran conectados los equipos de cómputo, en las tomas de red normal los dispositivos periféricos como impresoras, fax, scanner que tienen adaptadores previstos por el fabricante para protegerlos de las fluctuaciones de voltaje.

Para facilitar la comprensión de la infraestructura del CDAV se cuenta con un CATÁLOGO DE INFRAESTRUCTURA en el cual se presenta de manera detallada cada uno de los elementos que conforman la infraestructura de TI, su identificación, ubicación, capacidad, responsables, entre otros y se encuentra en la herramienta de mesa de ayuda.

8.1.1.2. *Redes*

Las redes informáticas surgen de la necesidad de compartir recursos e información. Esto, conduce a hablar de conectividad entre PC's.

La red LAN se encarga de transportar información de una PC a otra y entre éstas y sus periféricos.

Así, las comunicaciones juegan un papel importante en la integración interinstitucional, facilitando el acceso a las bases de datos de las instituciones productoras de información.

Por tal motivo, el CDAV vio la necesidad de implementar una red informática institucional, la cual funciona bajo la arquitectura de cliente servidor, donde se distribuyen los procesos operativos a los diferentes usuarios con la finalidad de acceder a bases de datos a nivel corporativo.

Centros de cableado:

El CDAV. Dispone de cinco centros de cableado, discriminados así:

- Dirección de Tecnología y Sistemas de Información.
- Oficina del Líder Operativo.
- Formación, Habilitación y Evaluación de Conductores.
- Área del Centro de Reconocimiento de Conductores.
- Programa Servicios de Tránsito *(Administrado por tercero)*.

Estos están compuestos por un gabinete, donde se encuentran los equipos activos de red, como los routers (enrutadores), switches, (concentradores) y patch panel (paneles de ponchado). Allí confluyen todos los puntos de cableado de datos, voz y eléctricos, organizados, identificados y conectados en los diferentes puertos de los equipos activos.

Área de servidores:

La plataforma tecnológica está conformada por un centro de cómputo, servidores, equipos de red y telecomunicaciones con el cableado estructurado categoría 5 y 6, que soportan a nivel general todas las actividades informáticas de la entidad. El área de tecnología cuenta con acceso restringido a las instalaciones por medio de una puerta con acceso digital ubicada en la entrada del DTYSI, además de sensores de temperatura, humedad y eléctrico.

Equipos de red:

En el centro de cableado ubicado en la DTYSI, se encuentra un switch interconectado por medio de fibra óptica a la oficina del líder operativo, de igual manera existe un tramo de fibra que interconecta DTYSI con el swicth ubicado en Formación, Habilitación y Evaluación de Conductores

UPS:

La Dirección Operativa es la encargada de la fuente de suministro de energía que protege principalmente los equipos del Centro de Cómputo y todas las estaciones de trabajo.

8.1.2. Sistemas de Información

El CDAV cuenta con un CATÁLOGO DE SISTEMAS DE INFORMACIÓN en el cual se consigna el inventario detallado de las aplicaciones con que cuenta la organización y se encuentran debidamente caracterizadas de tal forma que permite identificar atributos, o características clave de cada uno de los sistemas de información y su aporte a la gestión institucional.

Creación y cuentas de usuario:

Cuando se adquiere un equipo de cómputo, es necesario crear una cuenta de usuario en el dominio, para lo cual el profesional universitario grado 6, ingresa al servidor de dominio como Usuario administrador, ejecuta el programa para Administración de Usuario, selecciona la opción usuario nuevo del menú de usuario y realiza los siguientes pasos:

- En el campo nombre se digita el nombre de usuario
- Iniciales del primer y segundo nombre si lo hay, seguido del apellido.
- En el campo nombre de usuario, digita el nombre completo del usuario.
- En el campo descripción (Description) se digita la función principal que cumplirá este usuario.
- Luego digita el PASSWORD (******) y su confirmación.
- Selecciona el o los grupos a los cuales pertenecerá el usuario.
- Selecciona la opción añadir.
- Registra los cambios realizados en el formato.
- Suministra la información al usuario.

Sustentación de pruebas de usuario.

El funcionario encargado Profesional universitario, realiza las pruebas de software en un ambiente de pruebas, la cual permite que los usuarios actuales o potenciales de la aplicación interactúen con ésta en un funcionamiento real del sistema en distintas plataformas y ambientes de trabajo.

Estas pruebas son las únicas que realmente dan información acerca del posible éxito de las actualizaciones y por lo tanto el manejo adecuado de la información que generan los usuarios es crucial. Las pruebas deben documentarse en la plataforma de mesa de ayuda.

Validación de software:

Las validaciones de software son los procesos que permiten comprobar y revelar la calidad de un producto de software. Son utilizadas para identificar posibles fallos de implementación, calidad u operatividad en el CDAV.

Estas pruebas deben desarrollarse cada vez que se actualice una herramienta de software, se implemente una nueva o existan cambios de índole interno del CDAV, además, esta actividad debe realizarse antes de colocarlas en servicio.

Con el fin de implementar protocolos y reglamentación específica que aplica al proceso de revisión vehículos como organismo de inspección, se tendrá en cuenta las instrucciones definidas en el procedimiento ***PT-GO-07 Validación de software RTMyEC***.

Para realizar la verificación debe utilizarse el formato ***FO-GT-02 Validación de software***, cada proceso podrá disponer de listas de chequeo para realizar las validaciones estas se diligenciarán por los responsables de cada proceso y serán archivados junto con el formato ***FO-GT-02*** por cada área que solicito el requerimiento.

El software o aplicaciones que se deben verificar, son todas aquellas que se utilicen durante la prestación del servicio.

Se ha dispuesto que las validaciones de software deben realizarse teniendo en cuenta las directrices establecidas en la normatividad vigente.

La finalidad de estas validaciones es corroborar que el software utilizado por el CDAV durante la prestación del servicio es adecuado para su uso.

Administración de privilegios:

Cambio de roles o responsabilidades de un funcionario. Cualquier cambio que requiera hacerse a los roles y responsabilidades de algún empleado en la temática de privilegios de acceso a la infraestructura tecnológica del CDAV tales como creación de usuario, asignación de permisos o inactivación por vacaciones, incapacidad o retiro, el director o líder del Área en la que esté adscrito el funcionario, deberá solicitarlo por medio de la mesa de ayuda, el proceso de inactivar claves será realizado por el funcionario asignado.

Para el retiro del funcionario público o de un contratista el área de Desarrollo humano o el área en la cual labora el contratista deberá solicitar la inactivación por medio de la mesa de ayuda.

Permisos de administrador. Solo deben de tener permiso de administrador los funcionarios de tecnología que por sus funciones lo requieran.

Asignación de accesos y recursos de usuario:

El Profesional universitario, es responsable de asignar los perfiles de usuarios de acuerdo con lo establecido en la política de control de accesos***.***

Manejo de claves:

Es responsabilidad de cada jefe de área hacer que el personal que tiene a cargo dé un buen uso a las claves asignadas basándose en el ***Instructivo manejo de claves IT-GT-03.***

8.1.3. Información

La información del CDAV., actualmente cuenta con los componentes de información, que contine al conjunto de datos, la información, los servicios de información y los flujos de información.

La información que utiliza el CDAV es para responder a las necesidades de la entidad, ya sea para tomar decisiones, para los procesos o los grupos de interés.

Estos componentes de información es un comienzo para la implementación de la arquitectura de la información con procesos de calidad e interoperabilidad entre entidades y se cuenta con un inventario de todas las fuentes de datos, identificación de datos maestros, datos abiertos, definición de controles y nivel de acceso a la información y demás actividades propias de la gestión de información.

Para facilitar la comprensión de la información del CDAV se cuenta con una **CATÁLOGO DE DATOS** en el cual se presenta de manera detallada cada uno de los componentes que conforman la información y se encuentra en la herramienta de mesa de ayuda.

8.1.4. Servicios

El CDAV cuenta con un CATÁLOGO DE SERVICIOS socializado a los usuarios de las diferentes dependencias con la finalidad de facilitar la identificación de los principales servicios que se prestados por DTYSI el cual fue construido acorde a las necesidades de los clientes internos y alineados a las mejores prácticas de TIC.

Las solicitudes de servicios requeridas por los diferentes usuarios son manejadas mediante el software de mesa de ayuda GLPI *(https://mesadeayuda.cdav.gov.co/)*, el cual permite llevar un control de los requerimientos en los cuales interviene DTYSI, este aplicativo permite hacer un seguimiento a cada una de las tareas manejando una interacción con el usuario final ya que se puede ir alimentando las solicitudes en cada etapa del proceso.

8.1.5. Seguimiento al Proceso

Las Bitácoras son un componente muy crítico, ya que la falta de monitoreo podría poner en peligro un sistema informático. Se hace seguimiento a las bitácoras mediante la herramienta de gestión de incidentes en la mesa de ayuda la cual se basa en el standard de ITIL. Se describe a continuación diferentes bitácoras dispuestas en la organización para controlar los posibles eventos. Teniendo entre otras:

Bitácoras de Eventos de redes y comunicaciones:

El Profesional universitario grado 6, verifica la disponibilidad y continuidad del servicio de comunicación, con cada una de las sedes y/o proveedores de comunicaciones, actualizando la debida bitácora. Adicionalmente en caso de encontrar fallos se llevará trazabilidad dentro de la misma herramienta.

Bitácoras de eventos de servidores:

El Profesional universitario grado 6 verifica los eventos de los servidores y registra las acciones en la mesa de ayuda e identifica por medio de los trabajos realizados el tipo de labor a la cual corresponde ejemplo: FORMATO BITACORAS DE SERVIDORES.

El Profesional revisa diariamente los logs de los servidores *(Telefonía, Controlador de Dominio, Servidor de Antivirus, Servidor de Archivos y Tuberías),* con el fin de encontrar evidencias o indicadores de fallas en el sistema operativo y su hardware y en cualquiera de los logs registrados por el Visor de sucesos.

- Eventos de hardware.
- Aplicación.
- Seguridad.
- Instalación.
- Sistema.
- Eventos administrativos.
- Servicios de Active Directory.
- Servidor DNS.

En caso de encontrar fallos se lleva trazabilidad dentro de la herramienta La mesa de ayuda.

Bitácoras de eventos de la base de datos:

El Profesional universitario grado 6, revisa diariamente los logs que son enviados por medio de correo automático y registra en la mesa de ayuda un ticket recurrente llamado bitácora de control diario de la base de datos Oracle el log recibido por correo electrónico del monitoreo de la base de datos. En esta bitácora en caso de que haya un evento que comprometa el rendimiento o estabilidad del sistema se hace su respectivo seguimiento hasta quedar solucionado.

Bitácoras de eventos de backups y restauración del Oracle:

El Profesional universitario grado 6, revisa diariamente que se haya generado el backup, verifica la integridad de la copia y que haya quedado comprimida. El backup se genera en unidades de almacenamiento local y storage en la nube.

El Profesional universitario, debe registrar en la mesa de ayuda un ticket recurrente llamado Gestión de la Bitácora de Backups de Oracle en donde plasma las observaciones del punto anterior.

Semanalmente realiza la restauración del backup de la base de datos en un servidor de pruebas para validar la integridad de la información y registra en la mesa de ayuda un ticket recurrente llamado Gestión de la Bitácora de Restauración de Oracle.

Bitácoras de eventos del sistema de seguridad:

Bitácoras de eventos del Firewall. El Profesional universitario grado 6, revisa diariamente los eventos que deja la consola del Firewall y registra la realización de dicho proceso en una solicitud que se elabora mensualmente en el aplicativo de la mesa de ayuda con el nombre de Bitácoras de Eventos del Sistema de Seguridad.

Bitácoras de eventos del antivirus. El Profesional universitario grado 6, revisa diariamente los eventos que deja la consola del sistema antivirus, entre los que se encuentran los siguientes:

- **Informe de ataques de red:**
  El informe contiene información sobre los ataques de red registrados en los equipos cliente.

- **Informe de los equipos más infectados:**
  Muestra los 10 equipos cliente más infectados.

- **Informe de uso de licencia:**
  Informe sobre el estado de las licencias instaladas en los equipos cliente.

- **Informe de virus:**
  Este informe contiene información sobre la actividad de virus en los equipos cliente.

- **Informe del entorno de la protección:**
  Informe sobre la distribución en red de los componentes de protección de Kaspersky Lab para todos los grupos.

- **Informe del estado de la protección:**
  Este informe contiene información sobre el estado de protección antivirus de los equipos cliente para todos los grupos

La consola del antivirus envía un ticket a la mesa de ayuda con los reportes periódicos para que sean validados gestionados con el nombre de Bitácoras de eventos del antivirus**.**

8.1.6. Riesgos

Para llevar a cabo una protección adecuada de la información, es importante tener en cuenta los riegos tanto internos como externos que se pudiesen presentar y saber actuar frente a estos, motivo por el cual el CDAV cuenta con un procedimiento para la gestión del riesgo ***PT-GG-03 Administración de Riesgos*** a través de este se desarrolla una matriz donde se identifican, analizan, evalúan y tratan los diferentes riesgos a los que está expuesta la organización, entre ellos los relacionados con la seguridad de la información.

8.1.7. Plan de contingencia

El responsable del proceso establece las acciones a seguir para garantizar la continuidad del servicio.

En la actualidad el CDAV maneja la base de datos Oracle en Rack lo que permite manejar alta disponibilidad y se cuenta con dos servidores apuntando a la misma base de datos y un servidor virtualizado que funciona como servidor de respaldo, el cual se encuentra configurado de tal manera que permite el funcionamiento de la base de datos, adicionalmente, este tiene una réplica de la información la cuál es actualizada de manera semanal debido a que en este equipo se realizan las pruebas de recuperación de las copias de seguridad y solamente entra en funcionamiento si ninguno de los dos servidores puede prestar el servicio. Ver ***instructivo encendido y apagado de servidores IT-GT-02***.

Se tienen dos servidores para la telefonía IP del CDAV, uno que hace las veces de respaldo, para el momento en que el servidor principal deje de funcionar este tome la configuración del principal y preste el servicio sin ningún inconveniente, Ver ***instructivo encendido y apagado de servidores IT-GT-02***.

En comunicaciones se tiene contratado un canal de backup con el mismo proveedor, el cual se encuentra instalado por una vía diferente y en el momento de presentar falla el canal principal inmediatamente entra a funcionar el backup con la misma configuración del principal sin generar inconvenientes en la prestación de los servicios, la configuración que se tiene con los dos servicios de Internet es el equilibrio de cargas y de atender el Internet cuando haya saturación o desconexión del canal principal, además se cuenta con el canal de Internet manejado por el programa de servicios de tránsito mediante el cual se da acceso a los procesos operativos que lo requieran.

El Profesional universitario, es responsable de realizar el encendido y apagado de equipos cuando se requiera, de acuerdo con lo establecido en el ***instructivo encendido y apagado de servidores IT-GT-02***.

8.1.8. Pólizas de seguro vigentes

La Dirección administrativa y financiera maneja y controla las pólizas de seguros de los equipos.

Los equipos de cómputo de la empresa se encuentran amparados por medio de una póliza que tiene cobertura de equipo electrónico, hurto corriente débil, hurto calificado y hurto simple.

En caso de que se requiera trasladar un equipo, el director o el líder del área respectiva realiza una carta de autorización para salida del equipo y entrega al personal de seguridad para que verifiquen los datos registrados en el documento y los equipos físicamente.

8.2. Políticas de Seguridad Informática

8.2.1. Política de Gobierno Digital: TIC para la gestión.

La Política de Gobierno Digital: TIC para la Gestión es la declaración general que representa la posición de la gerencia del Centro de Diagnóstico Automotor del Valle Ltda., con respecto a la protección de los activos de información (servidores públicos, contratistas y proveedores, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la entidad y apoyan la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), por medio de la generación y publicación de las políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de dicho modelo, lo que garantiza que la Entidad trabaje para promover la cultura de movilidad, seguridad vial y respeto por el medio ambiente; a través de la formación y evaluación de la capacidad de conducción, revisión del estado de los vehículos, servicios y programas de tránsito y transporte[1].

El Centro de Diagnóstico Automotor del Valle Ltda., para asegurar la dirección estratégica de la entidad, establece la compatibilidad de la política y los objetivos del Modelo de seguridad de la información y Gobierno Digital: TIC para la Gestión con los objetivos institucionales, en donde, los objetivos del Modelo corresponden a:

1. Minimizar el riesgo de los procesos misionales de la entidad.
2. Cumplir con los principios de seguridad y privacidad de la información.
3. Cumplir con los principios de la función pública.
4. Mantener la confianza de los servidores públicos, contratistas y proveedores.
5. Apoyar la innovación tecnológica.
6. Implementar el Modelo de seguridad y privacidad de la información.
7. Proteger los activos de información.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información y de Gobierno Digital: TIC para la Gestión.
9. Fortalecer la cultura de seguridad de la información y de Gobierno Digital: TIC para la gestión en los servidores públicos, contratistas y terceros del Centro de Diagnóstico Automotor del Valle Ltda.

[1] https://www.cdav.gov.co/publicaciones/129389/mision-y-vision/

10. Garantizar la continuidad en la prestación del servicio a través de la mejora de la eficiencia e incremento de la capacidad de los servicios de movilidad y seguridad vial en el Valle del Cauca.

8.2.2. Políticas internas de seguridad y privacidad de la información

El CDAV tiene diseñadas y adoptadas las Políticas de seguridad y privacidad de la información alineadas a lo descrito en la Norma ISO/IEC 27002, estas políticas se encuentran desarrolladas en el manual ***MT-GT-02 Modelo de seguridad y privacidad de la información - MSPI*** y se describen de manera general a continuación:

a) Política para dispositivos móviles.
b) Política para trabajo remoto
c) Política para control de acceso.
d) Política para controles criptográficos.
e) Política para seguridad física y del entorno.
f) Política para transferencia de información.
g) Política para desarrollo seguro.
h) Política para relaciones con los proveedores.
i) Política para privacidad y protección de información de datos personales.

8.2.3. Políticas y estándares de cumplimiento de seguridad informática.

La Dirección de Tecnología y sistemas de información del CDAV tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

8.2.3.1. *Licencias de software*

Los estándares de CDAV se actualizan anualmente, de acuerdo a las necesidades incrementales, junto con los avances tecnológicos, de tal forma que se ajusten a las labores organizacionales, asignando un computador de acuerdo a los requerimientos de cada usuario el cuál debe tener instalado como mínimo el siguiente software Sistema Operativo (Windows, Linux), Navegador de Internet, Antivirus, los equipos para los directivos, lideres y todos los que por su actividad lo requieran, deben tener instalado adicionalmente el Software de ofimática para manejo de documentos y correo electrónico.

Cualquier software adicional que se requiera debe ser solicitado por medio de la mesa de ayuda, con la debida justificación, el Dirección de Tecnología y Sistemas de Información evalúa la disponibilidad de acuerdo al inventario de software y procede a la respectiva instalación o en su defecto al proceso de adquisición de dicha licencia.

8.2.3.2. *Derechos de Propiedad Intelectual*

Está prohibido por las leyes de derechos de autor y por el CDAV, realizar copia no autorizadas de software, ya sea adquirido o desarrollado por el CDAV.

Está prohibido por las leyes de derechos de autor y por el CDAV, almacenar en el equipo de escritorio o portátil, música y videos que no hayan sido adquiridos por el CDAV.

Los sistemas desarrollados por personal interno que controle DTYSI, son propiedad intelectual del CDAV.

8.2.3.3. *Revisiones del cumplimiento*

DTYSI, realiza acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática. Se considera una falta grave el incumplimiento de dichas políticas. Y se trata en el comité disciplinario según lo establecido en los procedimientos **PT-GH-04 Control Disciplinario Verbal** y **PT-GH-05 Control Disciplinario Ordinario.**

DTYSI, implementa mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado se considera una falta grave y se trata en el comité disciplinario según lo establecido en los procedimientos **PT-GH-04 Control Disciplinario Verbal** y **PT-GH-05 Control Disciplinario Ordinario**

8.2.3.4. *Violaciones de seguridad informática*

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la DTYSI.

Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de información.

Ninguna persona puede probar o intentar comprometer los controles internos a menos

de contar con la aprobación de la DTYSI, con excepción de los Órganos Fiscalizadores.

Ningún usuario del CDAV debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por DTYSI.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, o similares diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del CDAV.

8.2.3.5. *Confidencialidad – Integridad de la Información*

Todo personal que ingresa al Centro de Diagnóstico Automotor del Valle Ltda, debe tener una inducción o reinducción en el tema de seguridad, disponibilidad y protección de datos por parte de la dirección del área responsable.

8.2.3.6. *Seguridad de la información en la gestión de proyectos*

Los proyectos que se denominen estratégicos y/o sean prioritarios, impacten los procesos de la Entidad y/o la actualización e/o implementación de un nuevo sistema de información, deben asegurar que los riesgos de Seguridad y Privacidad de la Información asociados a los mismos sean gestionados, usando una combinación de controles automáticos y manuales.

Se deben especificar de manera clara los requerimientos de Seguridad y Privacidad de la Información en los proyectos, garantizando el balance entre seguridad, funcionalidad y los demás objetivos establecidos.

8.2.4. Políticas y estándares de seguridad ambiental

El CDAV cuenta con el Programa ***PM-GG-01 Manejo de residuos*** que describe los lineamientos internos definidos por la organización para el adecuado manejo de los residuos sólidos generados en Centro de Diagnóstico Automotor del Valle Ltda y para su óptimo tratamiento.

8.2.5. Políticas y estándares de Infraestructura

Seguridad del cableado:

El técnico administrativo, es responsable de que el cableado tanto de energía como de telecomunicaciones se encuentre en buenas condiciones y que esté protegido mediante tubería y canaleta para no permitir el acceso al cableado por parte del personal no autorizado.

Debe revisar cada tres o cuatro meses en la fecha de mantenimiento de los equipos, el cableado eléctrico y estructurado y registrar su estado en el aplicativo de la mesa de ayuda.

Los usuarios no deben mover o reubicar los equipos de cómputo ni los de telecomunicaciones, ni instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de DTYSI, en caso de necesitar movilizar los equipos, se requiere que se envíe la solicitud a DTYSI, a través de la mesa de ayuda y que se autorice por medio del líder directo el área.

Administración de Bienes Informáticos, la DTYSI se encargará de documentar la entrega de los bienes informáticos, para ello, cuando a un usuario se le instale un bien informático, el Departamento de Tecnología y sistemas de Información-DTYSI, se encargará de hacer firmar al usuario, con esto, el usuario se acredita como el responsable de dicho activo y deberá conservarlos en la ubicación autorizada por DTYSI, con lo establecido en el formato ***FO-GT-07 Entrega, traslado y préstamo de equipos o dispositivos.***

El equipo de cómputo asignado debe ser para uso exclusivo de las funciones que desempeña el empleado o contratista del CDAV.

Es responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas empresariales que se utilizan en su equipo, a fin de evitar riesgos por mal uso y aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar su información, únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas, sistemas, utilerías informáticas, etc.

Mientras se opera el equipo de cómputo, no se debe consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete, con el propósito de mantener el buen funcionamiento del equipo informático.

Se debe mantener el equipo informático en un entorno limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deben ser notificados con anticipación al líder de servicios generales y mediante la mesa de ayuda a la Dirección de Tecnología y Sistemas de Información con un plan detallado de movimientos debidamente autorizados por el director del Área que corresponda.

Mantenimiento del equipo informático:

El técnico administrativo es responsable de realizar las actividades de mantenimiento preventivo de los equipos siguiendo los lineamientos establecidos en el ***instructivo IT-GT-01 Mantenimiento de Equipos.***

Eliminación Segura y/o reusó de equipo:

Todas las computadoras, laptops y/o discos externos que contengan información almacenada y vayan a ser reasignadas a otro usuario o a otra área distinta de la que actualmente se encuentra, deben ser revisadas por el usuario para que éste respalde su información, ya que cuando este equipo llegue a DTYSI, se realizará la eliminación de la información que contenía.

Desaparición, pérdida, robo o extravío de equipo de cómputo:

El usuario que tenga bajo su custodia algún equipo de cómputo u otros dispositivos informáticos será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo con la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

La seguridad para las tabletas, portátiles, celulares, modem u otros dispositivos informáticos tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

En caso de desaparición, robo o extravío del equipo de cómputo o accesorios que estén bajo custodia de un usuario, debe dar aviso de inmediato a DTYSI, para iniciar el trámite interno e informar a la Dirección administrativa y financiera e interponer la denuncia ante la autoridad competente.

Salida e ingreso de equipos:

El funcionario o proveedor que ingresa o retira de las instalaciones un equipo de cómputo, portátil, tabletas, equipos de comunicación u otros dispositivos informáticos)**,** realizará el siguiente procedimiento de acuerdo con el caso:

- **Ingreso de equipo,** para el caso de equipos que no son propiedad de la entidad, se debe registrar en la portería principal los datos de identificación de los equipos para su posterior retiro.

- **Para el retiro de equipos propiedad de la entidad,** el área que custodia el equipo debe elaborar un oficio firmado por el director del área y por el Director De Tecnología y Sistemas de Información, indicando el sitio al cual es trasladado, los datos de identificación del equipo como seriales, numero de activo e identificación dada por la DTYSI y registrar en la mesa de ayuda el retiro.

- **Para el préstamo de equipos** se debe diligenciar el formato ***FO-GT-07*** **Entrega*, traslado y préstamo de equipos o dispositivos*** establecido para este requerimiento.

Uso de dispositivos:

El uso de los grabadores de discos compactos y/o dispositivos de almacenamiento tales como memorias USB, discos duros, etc. son exclusivos para respaldos de información que por su volumen así lo justifiquen, por lo anterior se tendrá un bloqueo de dichos dispositivos.

La asignación de este tipo de equipo será previa justificación por escrito y autorización del líder inmediato correspondiente y no se incluirán en la política de bloqueo.

El usuario que tenga bajo su custodia este tipo de dispositivos será responsable del buen uso que se le dé.

Daño del equipo:

El equipo de cómputo o cualquier recurso de tecnología de información que sufra algún daño por maltrato, descuido o negligencia por parte del usuario, éste deberá

cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso, DTYSI determinará la causa de dicho daño.

Administración de la configuración:

Los usuarios de los diferentes procesos del CDAV no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del CDAV, sin la autorización por escrito o respuesta dada en la mesa de ayuda previa solicitud hecha por el usuario.

Seguridad para la red:

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por DTYSI, en la cual los usuarios realicen la exploración de los recursos informáticos en la red CDAV, así como de las aplicaciones que operan sobre dicha red, con fines de detectar y mostrar una posible vulnerabilidad se tratara en el comité disciplinario según lo establecido en los procedimientos **PT-GH-04 Control Disciplinario Verbal** y **PT-GH-05 Control Disciplinario Ordinario.**

Acceso a los equipos de cómputo:

Cada equipo de cómputo del CDAV está configurado para ser utilizado únicamente por personal asignado, por tal motivo cada uno de ellos maneja una cuenta de usuario compuesta por usuario y contraseña de acceso de sesión para impedir que personas ajenas los usen; la responsabilidad de cambiar estas contraseñas recae sobre el Profesional universitario grado 4, quien debe de configurar la solicitud de cambio periódico de la clave de ingreso al sistema.

Por lo anterior, todos los equipos del CDAV están protegidos a través de las restricciones establecidas en los equipos de cómputo con el objetivo de evitar el uso no autorizado de sus aplicaciones.

Todos los consultores externos que realicen actividades de manera conjunta con el personal del CDAV en lo que respecta la infraestructura tecnológica, requieren previamente obtener un permiso del director del Área donde estarán brindando la asesoría especializada o desempeñando la actividad por la cual fueron contratados, posteriormente, el director o el líder de esa Área, elaborara un ticket explicando:

- El motivo por el cual se les debe dar acceso a la infraestructura Tecnológica
- El tiempo que requiere el acceso lógico

Restricciones al conectar a la red CDAV:

Está prohibido conectar a la red del CDAV, sin autorización de DTYSI, laptops personales para realizar trabajo oficial, ya que cuando se solicita conectar una laptop que no es propiedad de la entidad, se necesitarían recursos adicionales que permitan mantener segura la administración de las operaciones. *(Licencias de antivirus, antimalware, antispam y antispyware)*, incrementar el ancho de banda, dando como resultado un decremento en la velocidad de respuesta tanto de los sistemas informáticos como en el uso de internet.

Servicio de conexión remota por redes privadas virtuales (VPN):

El túnel VPN permite acceder a determinados servicios de red del CDAV desde cualquier ubicación no segura en Internet, y operar como si se hiciera desde dentro de la entidad.

Para ello se requiere la instalación en el PC de un software específico (cliente de VPN) que será enviado al correo corporativo del trabajador autorizado.

Para poder usarlo con ciertas garantías y seguridad, se deberán tener en cuenta lo siguientes:

Solicitud: El área que requiere la conexión deberá realizar a la mesa de ayuda la solicitud de acceso VPN conforme a esta normativa/procedimiento establecido.

Servicios que se utilizarán con la VPN: En la solicitud debe de incluir una breve descripción de los servicios a utilizar para el cual se requiere la conexión VPN así como fechas durante las que deberá estar activo (que no deberá superar los 12 meses).

Trascurrido este periodo, si es necesario mantener el servicio de VPN, se deberá solicitar expresamente una prórroga adicional de tiempo.

Definición de responsables: para cada solicitud se deberán definir dos responsables de la aprobación del ticket en la mesa de ayuda:

- Un responsable, director o líder del área o servicio que autoriza el acceso VPN para la prestación del servicio.

- Un responsable para el uso, que será el titular del acceso, quien utilizará la conexión VPN para realizar exclusivamente las tareas mencionadas.

También será la persona de contacto con la dirección de tecnología y sistemas de información para cualquier ajuste, configuración necesaria o incidencias que puedan ocurrir sobre la conexión por VPN.

Uso exclusivo del servicio y obligaciones: Todos los usuarios que tengan habilitado el servicio de VPN se obligan expresamente a cumplir lo indicado en el acuerdo de uso y activación del servicio de VPN el cual es remitido a sus correos empresariales en el momento de enviar la información para la conexión VPN.

Finalizada la relación contractual con el CDAV, o alcanzada la fecha de finalización del servicio, se cancelará la conexión automáticamente.

Conectividad: En el plazo establecido en los acuerdos de servicio de la mesa de ayuda, el funcionario de la dirección de tecnología asignado para dar respuesta al ticket, se contactará con los responsables especificados para indicarles las claves definitivas del acceso, así como los datos necesarios para configurar el cliente de VPN, o la denegación de su solicitud.

Incidentes de seguridad: En caso de que se produjese algún incidente de seguridad originado por la conexión VPN, ambos responsables que figuren en la solicitud colaborarán de forma activa con la dirección de tecnología y sistemas de información, aportando la información que se le pudiera requerir.

Acuerdo de uso y activación del servicio de VPN:

El utilizar la información remitida para la conexión remota se entenderá como una conducta inequívoca de que usted como titular de los datos personales se compromete a cumplir con los lineamientos indicados en la política de gobierno digital y las políticas de seguridad establecidas por el CDAV.

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado esto incluye, usuario, password y certificados de acceso necesarios para acceder a la información y la infraestructura tecnológica del CDAV, por lo cual se deberá mantener de forma confidencial y de uso unipersonal.

Tratar los datos de carácter personal con la máxima cautela con el fin de garantizar su confidencialidad e integridad, adoptando las medidas técnicas y organizativas necesarias en lo que respecta a la custodia, almacenamiento y conservación con el fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado.

En caso de que ocurra pérdida o hurto de un equipo asignado por la Dirección Tecnología y Sistemas de Información y en el cual se lleven actividades remotas como parte del trabajo remoto, será de cargo del trabajador remoto informar el evento de forma inmediata, y seguir las indicaciones para reporte de incidente descritas en la mesa de ayuda del CDAV, con el objeto de realizar las medidas de seguridad adecuadas para la protección de la información contenida.

8.2.6. Políticas y estándares de Sistemas de información

Instalación de Software que no es propiedad del CDAV:

Los usuarios que requieran la instalación de software que no sea propiedad del CDAV, deberán justificar su uso y solicitar su autorización a DTYSI, enviando una solicitud mediante la mesa de ayuda elaborado por otro funcionario indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el propietario del software aporte los derechos de autor de dicho software.

Si el dueño del software no presenta los derechos de autor del software, el personal asignado por DTYSI, procederá de manera inmediata a desinstalar dicho software.

Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del CDAV, que no esté autorizado por DTYSI. Y se tratara en el comité disciplinario según lo establecido en los procedimientos ***PT-GH-04 Control Disciplinario Verbal y PT-GH-05 Control Disciplinario Ordinario.***

Internet:

El acceso a internet provisto a los usuarios del CDAV es exclusivamente para las actividades relacionadas con las necesidades del cargo y las funciones que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo con lo que determine el comité disciplinario y lo establecido en los procedimientos ***PT-GH-04 Control Disciplinario Verbal y PT-GH-05 Control Disciplinario Ordinario.***

La autorización de acceso a paginas restringidas, deberá solicitarse por medio ticket a la mesa de ayuda por parte del director o líder del área, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del director del Área correspondiente.

Todos los accesos a internet tienen que ser realizados a través de los proveedores de internet pagados por el CDAV.

Los usuarios con acceso a Internet del CDAV tienen que reportar todos los incidentes de seguridad informática a DTYSI, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

El acceso a la red wifi privada debe ser solicitada por medio de ticket a la mesa de ayuda y previamente autorizado por DTYSI.

Obligaciones y/o monitoreo de usuarios que tienen el servicio de navegación en Internet:

- Serán sujetos de monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización de DTYSI.
- La utilización de internet es para el desempeño de su función y cargo en el CDAV y no para propósitos personales.

Internet público:

El CDAV cuenta con servicio de internet wifi por medio de un portal cautivo, cuya clave de acceso es suministrada por las áreas operativa, mercadeo, ventas y gerencia, con la finalidad de brindar a sus clientes la facilidad de consultar algunos datos desde sus celulares o cualquier dispositivo portátil.

Esquema de permisos de acceso a internet y mensajería instantánea o chat:

La restricción de acceso a internet se realiza mediante en Endpoint Security Cloud, la cual se ajusta al nivel de perfil de seguridad que corresponde con las funciones, DTYSI creara los niveles de perfiles que se requieran.

PERFIL 1: Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea o chat

PERFIL 2: Internet restringido y servicios de mensajería o chat: Los usuarios podrán hacer uso de internet y servicios de mensajería instantánea o chat, aplicándose las políticas de seguridad y navegación establecidas por DTYSI.

PERFIL 3: Internet restringido y sin servicios de mensajería o chat: Los usuarios sólo podrán hacer uso de internet aplicándose las políticas de seguridad y navegación establecidas por DTYSI.

PERFIL 4: El usuario no tendrá acceso a Internet ni a servicios de mensajería o chat.

Controles contra código malicioso:

El CDAV a través de DTYSI trabaja en la organización, utilizando las siguientes políticas para evitar que software malicioso se propague en sus equipos de cómputo a través de su intranet:

a) Adquirir sistemas operativos licenciados para recibir las actualizaciones de los parches de seguridad de forma automática, las cuales deben ser operadas únicamente por este Dpto.

b) El Profesional universitario grado 4, es responsable de configurar que todos los equipos tengan cuentas limitadas y no de administrador, excepto el personal de soporte facultado, esto con el fin de evitar instalaciones no autorizadas de software en los equipos y propagación de virus, ya que al ser infectada la maquina por cualquier virus este no podrá ejecutarse por encontrarse en una cuenta limitada y en la posterior ejecución del software antivirus ser eliminados sin mayores inconvenientes.

c) El Profesional universitario grado 4 es el responsable del correcto funcionamiento y permanente actualización del antivirus tanto en la consola de administración, como en los equipos clientes con el apoyo del técnico administrativo en el momento en que se requiera.

Para prevenir infecciones por virus informáticos, los funcionarios del CDAV, debe evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por DTYSI.

Almacenamiento como: memorias USB, discos duros externos y CD´s, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado DTYSI.

El usuario debe verificar mediante el software de antivirus autorizado por DTYSI que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

Ningún usuario del CDAV debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autoreplicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software.

Tampoco debe probarlos en cualquiera de los ambientes o plataformas del CDAV. El incumplimiento de este estándar será considerado una falta grave se tratará en el comité disciplinario según lo establecido en los procedimientos ***PT-GH-04 Control Disciplinario Verbal y PT-GH-05 Control Disciplinario Ordinario.***

Ningún funcionario del CDAV o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de DTYSI.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá elaborar el ticket a la mesa de ayuda, llamar a DTYSI y dejar de usar inmediatamente el equipo para la detección y erradicación del virus.

Cada usuario que tenga bajo su custodia algún equipo de cómputo portátil o de escritorio deberá dejarlo encendido los días martes para realizar automáticamente el chequeo de virus, en caso de que sea un portátil y o se haya dejado encendido y conectado a la red el usuario será responsable de solicitar mediante ticket a la mesa de ayuda las actualizaciones del software de antivirus.

Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por DTYSI en:

- Antivirus
- Outlook
- Office
- Navegadores u
- Otros programas.

Debido a que algunos virus son extremadamente complejos, ningún usuario del CDAV debe intentar erradicarlos de las computadoras, lo indicado es reportar a través de la mesa de ayuda al personal de DTYSI, para que realice dicha actividad.

Uso del correo electrónico:

El Centro de Diagnóstico Automotor del Valle Ltda, dispone del nombre de dominio CDAV.GOV.CO CDAV.COM.CO y DIAGNOSTICENTRODELVALLE.COM.CO para publicar en la red de Internet, servicios que la entidad a través de sus funcionarios y/o contratistas utilizan como medio de comunicación digital para interactuar con otras entidades y ciudadanía; es así que el sufijo cdav.gov.co es el nombre OFICIAL que la entidad tiene y garantiza como medio de envío y recepción de información a través de Internet; con este nombre de dominio se establecen los servicios principales como son:

- Nombredeusuario@cdav.gov.co = para el servicio de correo electrónico en Internet.
- www.cdav.gov.co = para el servicio de publicación de información institucional en la página Web.

Debido a que el espacio de las cuentas incide directamente sobre el espacio del servidor, se establece que todos los usuarios deben revisar frecuentemente su correo electrónico para leer sus mensajes y de manera periódica ir borrando los mensajes más antiguos para no afectar de esta manera el espacio en el servidor.

Cuando el funcionario sea retirado de la institución por algún motivo, la cuenta de correo será inactivada. Los lineamientos para el uso del correo se encuentran establecidos en el documento ***IT-GT-04 Instructivo Manejo del Correo Institucional***.

8.2.7. Políticas y estándares de Información (DATOS)

Uso de medios de almacenamiento:

Políticas de almacenamiento de medios de respaldo. El Profesional universitario grado 4 realiza las copias de seguridad de todos los procesos operativos y administrativos incluyendo los resultados de las revisiones realizadas por el OI y las licencias de conducción expedidas, esto con el objetivo primordial de garantizar la continuidad del negocio relacionada con la información en el evento que sea necesario.

Toda la información de las pruebas realizadas por el OI es registrada en la base de datos automáticamente después de terminar cada revisión.

El Profesional universitario grado 4 es responsable de la realización de las copias de seguridad de la base de datos a diario y de verificar las copias de respaldo teniendo

en cuenta los criterios definidos en el instructivo ***manejo, almacenamiento y seguridad de la información IT-GT-05.***

Los usuarios sólo pueden consultar su correo, utilizando como medio de acceso el cliente de Microsoft Outlook o por la web.

Cada usuario es responsable de realizar una copia de seguridad de la información que maneja en el equipo asignado, incluyendo la información manejada por la herramienta Outlook, es de aclarar que el correo queda almacenado en la Web.

Cuando un empleado requiera usar o consultar la información que se tiene almacenada de otro funcionario de la misma Área, el director del Área creara un ticket a la mesa de ayuda donde:

Explicará brevemente cuál es el fin de permitir compartir la información que se tiene en los medios de almacenamiento de un empleado a otro. Nombre y Cargo del funcionario público al que se le brindarán los derechos solicitados.

Los usuarios deberán mantener actualizada la información en el onedrive y verificar que se encuentre permanentemente actualizada con la finalidad de que la información pueda ser acezada desde cualquier lugar.

En caso de que se requiera algún respaldo en CD, DVD, Blu-ray etc. debido a que se tiene mucha información, este servicio deberá solicitarse mediante la mesa de ayuda.

Los trabajadores del CDAV deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que han sido emitidas para la protección de los datos personales y a los procedimientos institucionales para proporcionar a los particulares el acceso a la información pública que sea requerida al CDAV.

Para conservar la seguridad de la información, se llevará a cabo auditoría informática, es decir, se estarán realizando revisiones periódicas a las actividades informáticas que cada trabajador realiza, con la finalidad de detectar anomalías.

Para conservar la seguridad de la información en los equipos financieros se debe detallar en el formato ***FO-GT-06 Checklist Seguridad y Privacidad de la Información*** realizando un checklist por cada equipo financiero.

Políticas de conexión a la red de datos:

Bajo ninguna circunstancia está permitida la conexión a la red física de la entidad, de

cualquiera de los equipos dentro de esta clasificación; sin embargo, si llegase a ser necesario por las condiciones contractuales o por algún requerimiento legal, estos equipos se conectarán a una red lógica diferente a la administrativa y se definirá bajo los mayores niveles de seguridad la forma como accederá a los datos necesarios. Aquel tercero que desee una conexión física a Internet, deberá resolver esta necesidad de acuerdo a las condiciones establecidas por la dirección de tecnología y sistemas de información, el cual podrá consultar al personal encargado de infraestructura en la dirección de tecnología y sistemas de información para aclarar cualquier duda respecto a la seguridad e integridad de la red. Esta restricción deberá contemplarse en la elaboración de todos los contratos con terceros que vayan a trabajar dentro de las instalaciones físicas de la entidad. La única red a la que podrán acceder los equipos y dispositivos externos será a la red Wi-Fi del CDAV, la cual tiene cubrimiento en casi toda la infraestructura física de la entidad. La contraseña de acceso a esta red es administrada por el personal de la mesa de ayuda y es modificada periódicamente y comunicada por el correo institucional a todos los empleados.

8.2.8. Políticas y estándares de Operación

Identificación del incidente:

El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática debe reportarlo a DTYSI, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que la información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización, se debe notificar al director del área

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del CDAV, debe ser reportado a DTYSI.

Dicho incidente se registrará en la mesa de ayuda y se asignará el técnico que se encargará de solucionarlo.

Controles de acceso lógico:

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario(userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica del CDAV, por lo cual deberá mantenerlo de forma confidencial.

DTYSI, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del CDAV, otorgándoles los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio “Necesidad del saber”.

Otras políticas:

- ✓ No se autoriza que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

- ✓ No se debe albergar datos de carácter personal en las unidades locales de disco de las computadoras de trabajo y la entidad no se hará responsable por perdida de información personal.

- ✓ No debe Intentar obtener otros derechos o accesos distintos a aquellos que les han sido asignados.

- ✓ No debe Intentar acceder a áreas restringidas de los sistemas de información o de la red, software o hardware, cuartos de telecomunicaciones, gabinetes de telecomunicaciones y centro de cómputos, entre otros.

- ✓ Prohibido Intentar distorsionar o falsear los registros (log) de los sistemas de información.

- ✓ No se permite ejecutar o mantener programas que pudieran interferir sobre el trabajo de otros usuarios, dañar o alterar la información y los recursos informáticos.

- ✓ Intentar utilizar las áreas y espacios físicos designados para las telecomunicaciones como almacén o área para guardar los efectos y materiales de limpieza. Las cajas y papeles acumulan humedad y polvo y se pueden incendiar fácilmente. Los detergentes emiten gases químicos que deterioran los cables y corroen los equipos.

- ✓ Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura del CDAV de igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del CDAV o hacia redes externas como internet.

- ✓ Los usuarios del CDAV que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir a DTYSI, para solicitar asesoría.

- ✓ El usuario deberá reportar de forma inmediata al Líder de Servicios Generales, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

- ✓ El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su custodia, aun cuando no se utilicen y contengan información reservada o confidencial.

- ✓ Es responsabilidad del usuario evitar en todo momento la fuga de la información del CDAV que se encuentre almacenada en los equipos de cómputo que tenga asignados.

- ✓ Los documentos que se trabajen en los equipos de cómputo deben ser almacenados en el OneDriver, Teams o SharePoint oficial del CDAV.

- ✓ Proteger la información restringida o confidencial (documentos impresos, dispositivos de almacenamiento y medios removibles en general) bajo llave en sus escritorios y/o sitios de trabajo, cuando se retiren temporalmente de sus puestos de trabajo o en horas no laborales.

- ✓ Adicionalmente, se requiere que la información que se envía a las impresoras sea recogida inmediatamente, al imprimir documentos que conserven el carácter de confidencial abstenerse de reutilizar y antes de reciclar destruir papel que contenga información sensible de la entidad.

- ✓ Los usuarios deben apagar sus computadoras u otros recursos tecnológicos cuando hayan terminado su jornada laboral diaria con la finalidad de proteger los equipos ante eventuales cortes de energía eléctrica, excepto los martes, día en él se realiza el chequeo de antivirus y la DTYSI.

- ✓ Está prohibido que los usuarios utilicen la infraestructura tecnológica del CDAV para obtener acceso no autorizado a la información u otros sistemas de información del CDAV.

- ✓ Todos los usuarios de servicios de información son responsables de su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

- ✓ Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del CDAV, a menos que se tenga autorización de DTYSI.

- ✓ Cada usuario que accede a la infraestructura tecnológica del CDAV debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de Usuario por varios usuarios, exceptuando las áreas cuyos procesos operativos requieren el compartir los computadores por varios funcionarios.

- ✓ Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

- ✓ Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usuarlo.

8.2.9. Políticas, estándares de seguridad equipos financieros

Los usuarios deben utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura del CDAV de igual forma, deben proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del CDAV o hacia redes externas como internet.

Lineamientos:

A continuación, se presentan los requerimientos mínimos en seguridad de la información e informática que deben cumplir las entidades públicas de orden nacional y orden territorial en cuanto a los equipos o terminales móviles utilizados para la realización de transacciones financieras con recursos públicos, a través de los portales de internet que las entidades bancarias disponen para tal fin.

8.2.9.1. *Lineamientos de seguridad lógica*

La entidad debe asegurarse de lo siguiente:

a) Requerir credenciales de autenticación para el ingreso y/o uso, las cuales deberán estar obligadas a cambiarse periódicamente y tener especificaciones mayores de seguridad (longitud mínima de ocho caracteres alfanúmeros y caracteres

especiales) de conformidad con la tecnología y mecanismos técnicos que dispongan las instituciones financieras para este fin.

b) Controlar el tiempo de inactividad del usuario a través de bloqueo automático del equipo o terminal móvil, para lo cual se sugiere un tiempo máximo en las áreas administrativas de 10 Minutos (10) y sin bloqueo automático en las áreas operativas por lo tanto dicho bloqueo es responsabilidad del usuario.

c) Limitar los privilegios de la(s) cuenta(s) de usuario(s) utilizada(s) para realizar transacciones financieras en los equipos y/o terminales para este fin, a efecto de reducir el riesgo de que con la misma sea posible la instalación de software malintencionado o controladores de dispositivos no autorizados.

d) Restringir en lo posible la ejecución de archivos como (.exe, .vbs, .com .scr, etc.) que no hagan parte de los sistemas necesarios para la elaboración de las actividades propias del cargo y que hayan sido descargados de sitios web o recibidos vía correo por parte del usuario del equipo por medio del cual se realizan las transacciones financieras.

e) Establecer procedimientos automatizados o por medio del soporte técnico que disponga la entidad, para efectuar el borrado regular de: archivos temporales del sistema operativo, archivos temporales de Internet, cookies, historial de navegación y descargas (se sugiere mínimo una vez a la semana).

f) Establecer los mecanismos necesarios para que la instalación, actualización o desinstalación de programas o dispositivos en el equipo o terminal móvil, sea realizada únicamente por los funcionarios del área de sistemas o tecnología, o el personal designado por la Entidad para este tipo de requerimientos, adicionalmente, estas actividades deben ser revisadas y aprobadas por el funcionario que desempeñe el rol de oficial de seguridad de la información, y/o las áreas responsables de la seguridad de la información y/o los designados por la entidad para efectuar este tipo de aprobaciones.

g) Restringir la instalación de software que permita conexión remota (TeamViewer, LogMeIn, Hamachi, VNC, entre otros) evitando con esto que personas externas se puedan conectar fácilmente al equipo o terminal desde el cual se realizan las transacciones. Excepto los autorizados por DTYSI.

h) Asegurar que el equipo y/o terminal móvil cuente mínimo con: antivirus (con módulos de anti - keylogger, firewall personal, antispyware), software licenciado y actualizado de forma automática o supervisada.

i) Restringir los puertos que permitan la conexión y/o acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).

j) Activar mecanismos para que el equipo o terminal pueda recibir las actualizaciones de seguridad de forma automática, cada vez que sean emitidas por el fabricante para el sistema operativo respectivo y aplicaciones.

k) Mantener activos y en operación sólo los protocolos, servicios, aplicaciones, usuarios, entre otros, necesarios para el desarrollo de las actividades, en el equipo o terminal.

l) En lo posible, el equipo o terminal deberá ser destinado de manera exclusiva para la realización de las transacciones financieras.

m) En lo posible, apagar el equipo o terminal cuando no se esté utilizando, sobre todo si dispone de una conexión permanente a Internet.

8.2.9.2. *Lineamientos de seguridad física*

Las entidades deben asegurar que el acceso físico a las áreas donde estén los equipos o terminales móviles sea lo más restringido posible y de manera exclusiva al responsable directo de la realización de las transacciones.

A continuación, se listan los controles a ser implementados:

a) Restringir el acceso al área física desde donde se realizan transacciones financieras sólo para personal autorizado.

b) En lo posible, contar con cámaras de video, las cuales deben cubrir al menos el acceso principal al área y el funcionario que utilice el equipo o terminal móvil. Las imágenes deberán ser conservadas por lo menos seis (6) meses o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

8.2.9.3. *Lineamientos de seguridad de la red*

a) Restringir el acceso a correos personales, redes sociales, y en general a otros sitios no asociados con las funciones del operador, desde el equipo y/o terminal. Esto con el objeto de evitar que, de forma intencional o accidental, se descargue, instale o ejecute software malintencionado.

b) Deberá evitarse realizar transacciones financieras desde dispositivos móviles o conexiones a redes inalámbricas de terceros no confiables.

c) Asegurar las redes inalámbricas (WIFI) para que cuenten con las mejores condiciones y estándares técnicos disponibles. Definir un usuario con contraseña robusta y cambiarla periódicamente.

d) Si la entidad cuenta con una red inalámbrica (WIFI) para invitados, esta deberá estar totalmente aislada y segmentada de las redes LAN de la entidad.

8.2.9.4. *Lineamientos de seguridad frente a la entidad financiera*

a) Asignar una dirección IP fija pública al equipo o terminal móvil, la cual debe ser informada a la(s) entidad(es) financiera(s), de forma que solo esta dirección IP fija sea la utilizada para realizar transacciones en los portales empresariales.

b) Garantizar la protección de las claves y dispositivos de acceso al equipo o terminal móvil y al portal empresarial de la entidad financiera. En desarrollo de esta obligación, las entidades deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en el equipo y/o terminal móvil de la entidad deberá ser única y personalizada.

c) Utilizar las medidas de autenticación y control que le ofrecen la(s) entidad(es) financieras a través de la(s) cuales realizan transacciones. Particularmente, definir perfiles de autorización de transacciones, utilizar la preinscripción de beneficiarios, parametrizar montos y horarios para la realización de operaciones y realizar la inscripción para recibir notificaciones en línea.

8.2.9.5. *Lineamientos de seguimiento y monitoreo de controles*

a) El máximo responsable del área financiera de la Entidad, deberá coordinar con las áreas de TI y/o de seguridad de la información y/o las Oficinas de Control Interno, el responsable de verificar el cumplimiento de las condiciones de seguridad del equipo y en general, las consagradas en este instructivo, al menos cada tres (3) meses.

b) Para la verificación del cumplimiento de las condiciones de seguridad y los lineamientos aquí establecidos, se deberá diligenciar la lista de chequeo para seguimiento y evaluación del cumplimiento de lineamientos para equipos financieros establecida en el formato **FO-GT-06** Checklist Seguridad y Privacidad de la Información, el cual deberá ser suscrito tanto por el responsable del área financiera, como por el designado para la respectiva verificación.

8.2.9.6. *Recomendaciones de seguridad en la realización de las transacciones*

a) Acceder a la página de la entidad financiera o a través de la cual va a realizar la transacción únicamente digitando la dirección en el navegador. Nunca realice esto a través de links, motores de búsqueda o de los favoritos o marcadores del navegador.

b) Siempre cerrar la sesión del portal transaccional al terminar las transacciones.

c) En lo posible y teniendo en cuenta la afectación de algún servicio, parametrizar ante su banco de tal manera que ninguna transacción financiera pueda realizarse antes de las 6:00 a.m. y después de las 8:00 p.m., ni durante los fines de semana y/o días festivos.

d) Asegurar la restricción en el acceso a los portales transaccionales de los usuarios durante sus períodos de vacaciones o licencias y darlos de baja en casos de traslado o retiros.
e) Llevar un adecuado control de los usuarios y perfiles del equipo. Estos deben ser personalizados y de uso restringido al funcionario asignado (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).

f) Mantener los mecanismos de comunicación con la(s) entidad(es) financiera(s) actualizados, con el fin de informar inmediatamente en caso de identificar algún evento de riesgo que tenga relación las transacciones financieras (ej. pérdida de token, vulneración de clave, solicitud reiterada de credenciales, demoras y retardo en respuestas del Portal, mensajes de mantenimiento, notificaciones de ingresos y transacciones no reconocidas, etc.).

g) Asegurar que las personas que realizan transacciones financieras con los recursos de la entidad cuentan con capacitación en relación con la seguridad de la información y de las medidas que debe adoptar para mitigar los riesgos de fraude financiero.

8.2.10. Política para la renovación y actualización tecnológicas.

El CDAV velará porque los softwares instalados en la entidad, en equipos de cómputo y servidores, se encuentren legalmente licenciados y durante su vigencia se ejecute la política de renovación y actualización con las últimas versiones de software correspondiente; esta medida es obligatoria, salvo en aquellos casos en los cuales, por limitaciones técnicas en los computadores no se pueda llevar a cabo, en este caso, se debe renovar el equipo de cómputo para evitar fallos que comprometan la seguridad de la información.

El CDAV, garantizara la renovación y /o actualización oportuna de sus equipos basado en el diagnóstico y niveles de obsolescencia definidos en el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**.

Los siguiente lineamientos permiten dar cumplimiento a la política los cuales son necesarios para la toma de decisiones y poner en práctica o ejecutar las estrategias, programas y proyectos específicos del nivel institucional referentes a los procesos de renovación y actualización tecnológica.

Tienen como objetivo garantizar la renovación constante y eficaz de los equipos que soportan las TICs en el CDAV, indispensables para el buen desempeño de las actividades misionales y la adecuada prestación del servicio, proporcionando los elementos tecnológicos necesarios para que las diferentes áreas de la Entidad presten un mejor servicio a los usuarios, sea a través de los equipos de escritorio, portátiles, Tablet, dispositivos móviles, los servidores del centro de datos y todos los periféricos y equipos de comunicación para brindar un servicio óptimo y permanentemente con alta disponibilidad dentro y fuera del CDAV.

Una vez la Gerencia aprueba la compra de equipos, se escoge comercialmente la mejor referencia posible del mercado que cumpla con los requerimientos exigidos por el proceso, proyectando las máquinas para un servicio mínimo de 5 años. La asignación de los computadores se realiza mediante un estudio de necesidades, utilizando un proceso de redistribución que comprende la rotación de máquinas, donde el objetivo final es entregar a los usuarios una herramienta adecuada para el buen desempeño del proceso y retirar del inventario aquellos equipos, que por sus características ya cumplieron su vida útil.

8.2.10.1. *Inventario* y hoja de vida de computadores

El CDAV tiene implementado un sistema de información que le permite conocer la cantidad de equipos de cómputo y software identificando los datos técnicos de los mismos, también cuenta con los datos de los mantenimientos preventivos y correctivos que se le ha hecho a cada equipo o software reportados en los casos de seguimiento de la Mesa de ayuda. Este sistema de información es actualizado por el grupo de soporte tecnológico de la dirección de tecnología y sistemas de información.

8.2.10.2. Actualización y renovación de equipos

Se hará teniendo en cuenta el tiempo de funcionalidad el cual varía de acuerdo a las características del equipo, el tiempo de uso, las actividades para las cuales se hayan

adquirido y las condiciones ambientales y de utilización donde estén o hayan operado de acuerdo a los niveles de obsolescencia definidos en el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**.

8.2.10.3. Actualización y renovación de equipos servidores

Se hará teniendo en cuenta el tiempo de funcionalidad el cual varía de acuerdo a las características del equipo, el tiempo de uso, las actividades para las cuales se hayan adquirido de acuerdo a los niveles de obsolescencia definidos en el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**

Los equipos obsoletos podrían seguir realizando las operaciones habituales o podrán ser usados para nuevas tareas o proyectos que no sean considerados inicialmente como de misión crítica, dado los niveles de obsolescencia en que se encuentren.

Debe considerarse en los costos de los proyectos de renovación o reemplazo de la tecnología de servidores los costos de la migración de los datos y aplicaciones, de forma que no impacten los servicios del CDAV.

8.2.10.4. Actualización y renovación de racks, gabinetes de telecomunicaciones y centros de cableado

Se renovarán cuando las necesidades de ampliación, actualización y de cambios tecnológicos así lo exijan. Estos serán dados de baja cuando los elementos de fijación de los equipos de cómputo no sean adecuados, o las medidas de los racks no sean útiles para alojar los nuevos equipos. Su actualización estará supeditada a la valoración realizada por el personal de soporte tecnológico de la dirección de tecnología y sistemas de información.

8.2.10.5. Actualización y renovación de sistemas de alimentación y distribución de energía

Los equipos y dispositivos de alimentación y distribución de energía deberán satisfacer plenamente las necesidades de soporte eléctrico para mantener en funcionamiento los equipos instalados en el Centro de Cómputo y aquellos conectados a la red regulada. Las UPS proveerán de energía a todos los equipos de cómputo de misión crítica, por el periodo de tiempo necesario para el restablecimiento del servicio de energía o la entrada de abastecimiento de las plantas de energía suplementarias. Su actualización está supeditada a análisis técnico realizado en conjunto entre la dirección de tecnología y sistemas de información y la dirección operativa del CDAV. Ver el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**

8.2.10.6. Actualización y renovación de unidades de Distribución de Energía (PDU - Power Distribution Unit)

Son unidades de múltiples tomas de energía que deberán tener condiciones de regulación de sobrecargas eléctricas y contar con medidores de carga para ajustar la distribución de energía en los centros de cómputo. Su actualización está supeditada a análisis técnico realizado en conjunto entre la dirección de tecnología y sistemas de información y la dirección operativa del CDAV. Ver el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**

8.2.10.7. Aire acondicionado

Este equipo deberá proveer condiciones satisfactorias de refrigeración, manteniendo una temperatura máxima de 24 ºC y una humedad relativa máxima del 68%; razón por la cual deberán contar con lectores de temperatura y humedad. Su actualización y manteniendo periódico corresponde al área de gestión logística a cargo de la dirección administrativa y financiera. Los equipos de aire acondicionado dejarán de ser funcionales cuando su capacidad de refrigeración no cubra las necesidades de regulación de temperatura al interior de las instalaciones del centro de cómputo o datacenter. Si un equipo de aire acondicionado deja de ser funcional se debe efectuar una reposición de este o adquirir uno adicional de apoyo; en cualquier caso el equipo nuevo deberá contar con características iguales o superiores al que reemplaza. La adquisición, reposición, instalación y mantenimiento de equipos de aire acondicionado de los centros de cómputo será responsabilidad del área de gestión logística a cargo de la dirección administrativa y financiera, pero deberán presentarse las características técnicas al personal de la dirección de tecnología y sistemas de información y se podrá pedir el concepto de los fabricantes o proveedores del hardware utilizado en los centros de cómputo. Ver el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**

8.2.10.8. Actualización y renovación de equipos de detección y extinción de incendios

Todo centro de cómputo deberá contar con los elementos necesarios de detección y extinción de incendios. Su adquisición, instalación y mantenimiento será responsabilidad de la dirección de tecnología y sistemas de información con la asesoría del proveedor cuando se requiera. Ver el **instructivo IT-GT-08 Identificación de la obsolescencia para los activos de información**

8.2.10.9. Obsolescencia tecnológica

Es conocido que toda tecnología tiende a ser obsoleta a medida que pasa el tiempo, pero conscientes a que en la mayoría de los casos esta obsolescencia se da generalmente por la renovación tecnológica, la dificultad para conseguir repuestos y por los requerimientos y exigencias de las necesidades de los usuarios, se han establecido los siguientes parámetros en lo referente al hardware y a las redes de comunicación de acuerdo a los niveles de obsolescencia definidos en el instructivo IT-GT-08 Identificación de la obsolescencia para los activos de información.

Obsolescencia en el hardware de las estaciones de trabajo (equipos de escritorio, portátiles y demás periféricos)

Los equipos adquiridos por la entidad tendrán una vida útil de acuerdo a los niveles de obsolescencia definidos en el en el instructivo IT-GT-08 Identificación de la obsolescencia para los activos de información**.**, la dirección de tecnología y sistemas de información, apoyada en las solicitudes de las dependencias y los conceptos de soporte tecnológico, dará el visto bueno para el reemplazo de estos equipos, los cuales serán enviados a Almacén para ser dados de baja del inventario del CDAV.

Obsolescencia en el hardware de Servidores

Su vida útil al igual que con las estaciones de trabajo debe considerarse de acuerdo a los niveles de obsolescencia definidos en el en el instructivo IT-GT-08 Identificación de la obsolescencia para los activos de información**.**, sin embargo, muchos equipos (servidores o unidades de almacenamiento) pueden seguir prestando servicio en aplicaciones complementarias, secundarias o como prototipo para nuevos proyectos para desarrollar servicios. Deben considerarse acciones muy puntuales para servidores cuya información no pueda ser migrada o transferida a una nueva plataforma, sea por costos, capacidades técnicas o licenciamiento del software para manipulación de dicha información, en este caso deberá evaluarse la relación costo/beneficio de mantener activos dichos servidores y documentar dichas decisiones.

Obsolescencia de redes de comunicaciones

Se considera una vida útil de acuerdo a los niveles de obsolescencia definidos en el en el instructivo IT-GT-08 Identificación de la obsolescencia para los activos de información.; sin embargo, dicho período estará sujeto a los requerimientos de los servidores y/o servicios prestados a la comunidad. El equipo técnico de la dirección de tecnología y sistemas de información será el encargado de comprobar, si los equipos pueden continuar prestando el servicio para el cumplimiento de los propósitos

institucionales, esta revisión será obligatoriamente anual a partir del período de obsolescencia.

Obsolescencia de equipos de soporte eléctrico de la sala de servidores

Estos serán tratados similarmente al hardware de servidores; sin embargo es importante hacer una revisión de circuitos y equipos una vez se presente una modificación del parque de servidores para verificar que las cargas finales correspondan a la capacidad de los equipos de respaldo. Su actualización está supeditada a análisis técnico realizado en conjunto entre la dirección de tecnología y sistemas de información y la dirección operativa del CDAV. Ver el instructivo IT-GT-08 Identificación de la obsolescencia para los activos de información

8.2.10.10. Políticas para equipos y dispositivos que no son propiedad de la entidad.

Estas pautas deben tenerse en cuenta para todos los equipos que acceden la plataforma tecnológica de la entidad pero que no ha sido adquirida por esta. Dentro de esta clasificación entran los equipos de los contratistas.

8.2.10.10.1. Políticas de renovación tecnológica para terceros

Dado que estos equipos no se encuentran en control de la entidad se le hace solo la recomendación al contratista o usuario final de estas políticas de renovación tecnológica.

8.2.10.11. Actualización, renovación y asignación de impresoras

En cada dependencia, le será asignada una impresora conectada en red, lo que permitirá que cada equipo de la dependencia o de otras dependencias puedan aprovechar dicho recurso. En caso de requerirlo, la dependencia podrá hacer un requerimiento debidamente justificado a la Dirección de tecnología y sistemas de información. Debido a la optimización de recursos impulsada por Dirección de tecnología y sistemas de información no debería haber dos impresoras de similares características en una misma dependencia, por lo que las impresoras de han instalado distribuidas geográficamente para cubrir las diferentes áreas de la entidad. Ver el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información.**

8.2.10.12. Renovación y actualización del software

Dado que todo el software instalado en los servidores y equipos de la entidad está legalmente licenciado, se debe procurar que se mantengan actualizadas todas las instalaciones con las últimas versiones y subversiones de dicho software; esta medida es obligatoria salvo en aquellos casos en los cuales, por limitaciones técnicas en los computadores, no se pueda llevar a cabo, en cuyo caso deberá gestionarse contemplando todos los criterios posibles, la renovación del hardware para evitar un rezago en el uso de la tecnología y posibles fallas en la seguridad, integridad y estabilidad en la plataforma tecnológica de la entidad. Ver el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información**

8.2.10.13. Renovación y actualización del software desarrollado internamente

Para el caso de cualquier software desarrollado por dirección de tecnología y sistemas de información se realiza el procedimiento de calidad vigente y estipulado para tal fin. Ver el instructivo **IT-GT-08 Identificación de la obsolescencia para los activos de información.**

8.2.10.14. Distribución y asignación del hardware y equipos de cómputo

La distribución de equipos de hardware la hará el Director de tecnología y sistemas de información sobre la base de la proyección hecha para cada uno de los centros. Los equipos de cómputo se asignarán a los funcionarios y contratistas, de acuerdo a las renovaciones adquiridas y a los requerimientos adicionales hechos por las dependencias. Ningún funcionario a excepción de los asignados a la dirección de tecnología y sistemas de información o aquellos que lo justifiquen a través del líder o director de dependencia pueden tener a su cargo dos o más equipos de cómputo. Al recibir el equipo, el usuario se compromete a mantenerlo en las condiciones de Hardware y Software descritas en el documento políticas y estándares de seguridad informática.

9. DOCUMENTOS CITADOS

9.1. MA-GT-02 Manual modelo de seguridad y privacidad de la información -MSPI
9.2. PM-GG-01 Programa Manejo de Residuos.
9.3. PT-GG-03 Procedimiento Administración de Riesgos.
9.4. PT-GO-07 Procedimiento Validación de software RTMyEC.
9.5. PT-GH-04 Procedimiento control disciplinario verbal.
9.6. PT-GH-05 Procedimiento control disciplinario ordinario.
9.7. IT-GT-01 Instructivo Mantenimiento de equipos.
9.8. IT-GT-02 Instructivo Encendido y Apagado de servidores.
9.9. IT-GT-03 Instructivo Manejo de Claves.
9.10. IT-GT-04 Instructivo Manejo del Correo Institucional.
9.11. IT-GT-05 Instructivo Manejo, Almacenamiento y Seguridad de Información.
9.12. IT-GT-08 Instructivo Identificación de la obsolescencia para los activos de información.
9.13. FO-GT-02 Formato Validación de Software.
9.14. FO-GT-06 Formato Checklist seguridad y privacidad de la información.
9.15. FO-GT-07 Formato Entrega, traslado y préstamo de equipos o dispositivos.
9.16. Documento Interno. Código de Integridad.

10. VALIDACIÓN DOCUMENTAL

Elaborado por:	Autorizado por:
Nombre: Emerson Vela Londoño	**Nombre:** Emerson Vela Londoño
Firma	Firma
Cargo: Director de Tecnología y SI	**Cargo:** Director de Tecnología y SI
Fecha: 2022-02-18	**Fecha:** 2022-02-18