


POLITICAS DE SEGURIDAD INFORMATICA	Fecha de emisión: 2018-12-12	
	Código: CITB.DE.DI.10	
	Versión: 01	

Página 1 de 4

La Alta Dirección de CITB S.A.S. consciente de la importancia de preservar, conservar y manejar la información resultado del proceso de inspección de manera confidencial y segura, ha establecido lineamientos y políticas que deben ser cumplidas por todos los empleados y colaboradores del Organismo de Inspección en todas las actividades desarrolladas, a continuación, se presentan las políticas de seguridad de la información establecidas por el CDA:

Aspecto a Controlar	Descripción de Política
Control de acceso y contraseñas	<ul style="list-style-type: none"> <li>✓ La creación de usuarios, asignación de contraseñas, los permisos de acceso a los sistemas, solo podrá ser habilitada en el software de inspección por el director de sistemas, previa autorización de gerencia.</li> <li>✓ El director de sistemas debe establecerse de acuerdo al cargo, los permisos de acceso y privilegios de los usuarios del sistema, con el fin de restringir la posibilidad de los empleados para leer, escribir, modificar, crear o borrar información del proceso de inspección y de CITB S.A.S.</li> <li>✓ Se debe controlar los usuarios habilitación en el sistema, los usuarios deben ser bloqueados cuando el empleado no pueda asistir por más de 8 días a laboral por motivo de vacaciones, licencias, sanciones, incapacidades, etc.; el usuario debe ser deshabilitado cuando el empleado renuncie, sea despido o termine su contrato laboral y no sea reanudado.</li> <li>✓ Todos los equipos de cómputo deberán tener contraseña para su acceso.</li> </ul>
Software	<ul style="list-style-type: none"> <li>✓ Todo el software utilizado debe encontrarse licenciado y protegido por derechos de autor.</li> <li>✓ Las licencias de software estarán bajo responsabilidad del director de sistemas.</li> <li>✓ La vigencia del software instalado deberá ser controlada por el director de sistemas</li> <li>✓ Está prohibido hacer copias de software instalado</li> <li>✓ No está permitido instalar ningún tipo de software distinto al autorizado para su uso.</li> <li>✓ No se permite instalar software gratuito bajado de internet, a menos que sea aprobado y autorizado por el director de sistemas.</li> <li>✓ El software de inspección debe ser validado antes de poner en funcionamiento en el proceso de inspección.</li> </ul>

# POLITICAS DE SEGURIDAD INFORMATICA

Fecha de emisión: 2018-12-12

Código: CITB.DE.DI.10

Versión: 01



Página 2 de 4

Aspecto a Controlar	Descripción de Política
Software Antivirus	<ul style="list-style-type: none"> <li>✓ Los equipos deben contar con software antivirus perfectamente licenciado que permita la detección oportuna y eficaz de virus, spyware u otras formas maliciosas de intromisión.</li> <li>✓ Los medios de almacenamiento utilizados como USB, deben ser verificados con el software antivirus antes de ser utilizados por los empleados.</li> <li>✓ No se permite el ingreso o utilización de sistemas de almacenamiento extraíbles en servidores, computadoras de la red y equipos de vital importancia para el CDA, sin la autorización del director de sistemas.</li> <li>✓ El director de sistemas debe programar tareas de limpieza para todos los equipos de cómputo con los que cuenta la empresa.</li> </ul>
Copias de seguridad	<ul style="list-style-type: none"> <li>✓ El director de sistemas debe realizar copias de seguridad de servidor y de la información sensible del CDA almacenada en los PC's (ejemplo. Bases de datos, documentación y aplicaciones que garanticen la continuidad del servicio).</li> <li>✓ Las copias deben ser identificadas y almacenadas en un lugar seguro y protegido contra el medio ambiente (polvo, agua e incendios).</li> <li>✓ Se deben guardar copias de la información crítica y vital de CDA en un lugar fuera de las instalaciones u oficinas.</li> <li>✓ El director de sistemas debe realizar y guardar copias de seguridad de aquellos equipos que requieran reparación, antes de realizar la misma</li> </ul>
Uso de internet	<ul style="list-style-type: none"> <li>✓ No se permite el acceso a internet en los equipos informáticos del proceso de inspección y de los demás procesos de CITB</li> <li>✓ No se encuentra permitido el uso de chats así como el ingreso a redes sociales de cualquier tipo.</li> <li>✓ Se encuentra prohibido el envío de información considerada como confidencia por internet.</li> <li>✓ La navegación en internet se debe realizar para fines estrictamente laborales.</li> <li>✓ No se permite la descarga de programas por internet.</li> </ul>
Uso de celulares	<ul style="list-style-type: none"> <li>✓ Se encuentra prohibido el uso de celulares en la pista de inspección por parte de inspectores técnicos.</li> <li>✓ Se encuentra prohibido el envío de imágenes de infraestructura, equipos, pistas de inspección y proceso de inspección del CDA sin autorización de la gerencia.</li> </ul>

# POLITICAS DE SEGURIDAD INFORMATICA

Fecha de emisión: 2018-12-12


Código: CITB.DE.DI.10

Versión: 01



Página 3 de 4

Aspecto a Controlar	Descripción de Política
Equipos e infraestructura	<ul style="list-style-type: none"> <li>✓ El empleado (s) al cual fueron asignados equipos (Tablet, PC, etc.) debe garantizar su adecuado manejo, cuidado y protección ante posibles daños físicos o accesos no autorizados.</li> <li>✓ Se prohíbe el uso de los equipos de la línea de inspección a personal no autorizado, salvo en las actividades de mantenimiento y calibración que deben ser supervisadas por el director de sistemas y el director de mantenimiento.</li> <li>✓ Los equipos de cómputo deben ser utilizados para actividades de trabajo y no para otros fines (intereses personales, juegos y pasatiempos)</li> <li>✓ Los equipos de cómputo por ningún motivo podrán ser trasladados y ubicados en otro sitio, sin previa autorización por escrito del director de sistemas.</li> <li>✓ Ningún empleado se encuentra autorizado para destapar o manipular las partes o piezas constitutivas de cualquier equipo o de la red, el director de sistemas será el único autorizado para realizar dichas actividades o para gestionar y delegar estas actividades a terceros (proveedores de servicios).</li> <li>✓ El personal debe reportar las fallas presentadas en los equipos de cómputo (a nivel físico o de configuración) e informarlas al director de sistemas, quien tomará las medidas pertinentes al caso.</li> <li>✓ Ningún equipo de cómputo o de red podrá salir de las instalaciones sin previa autorización firmada por el gerente.</li> <li>✓ Los equipos de cómputo e infraestructura tecnológica deben protegerse contra riesgos del ambiente como polvo, agua, incendios o demás factores que pongan en riesgo su condición.</li> <li>✓ No se permite fumar, ingerir alimentos o beber mientras se está utilizando el PC, o cualquier equipo de informático.</li> <li>✓ Se encuentra prohibido realizar cambios a la configuración preestablecida del equipo de cómputo ni de la red.</li> </ul>
Acceso remoto	<ul style="list-style-type: none"> <li>✓ Solo será permitido el acceso remoto al proveedor de sistemas y/o equipos de inspección únicamente para mantenimiento de software, actualización de software, mantenimiento de equipos, etc. y con autorización expresa del director de sistemas.</li> <li>✓ El director de sistemas debe realizar seguimiento y control a las actividades desarrolladas por acceso remoto, estas deberán ser registradas.</li> </ul>

POLITICAS DE SEGURIDAD INFORMATICA	Fecha de emisión: 2018-12-12	
	Código: CITB.DE.DI.10	
	Versión: 01	

Página 4 de 4

Aspecto a Controlar	Descripción de Política
	✓ El director de sistemas debe cerciorarse de que las actividades de acceso remoto fueron cumplidas y el objetivo fue logrado.
Firma digital.	✓ La firma digital con la que cuenta el CDA será responsabilidad del Director de Técnico y del auxiliar de ingreso, quienes son los autorizados para interactuar con entidades como el RUNT y el Ministerio de Transporte.

### 1. DOCUMENTOS RELACIONADOS

NOMBRE	CÓDIGO
Procedimiento de Actualización de requisitos legales	CITB.DE.PR.04
Procedimiento de Capacitaciones	CITB.AC.TH.04

### 2. REGISTROS GENERADOS

NOMBRE	CÓDIGO

### 3. CONTROL DE CAMBIOS DEL DOCUMENTO

REV No.	FECHA	DESCRIPCIÓN DEL CAMBIO		SOLICITÓ
		SECCIÓN/NUMER AL	DESCRIPCIÓN DEL CAMBIO	
02	2021-03-02	N/A	Creación del Documento	N/A