POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Presidencia con el fin de proteger la Información como uno de los activos más importantes de la Organización, promueve la implementación y ejecución de mecanismos que garanticen la integridad, confidencialidad y disponibilidad de la misma. El área de IT debe velar por la aplicación adecuada de mecanismos, procedimientos y seguimientos con el fin de controlar las vulnerabilidades, así como la sensibilización de los empleados para garantizar altos estándares de seguridad a la información.

1. OBJETO.

Establecer un sistema de administración de seguridad de la información para gestionar adecuadamente los riesgos, proteger la información y mantener la continuidad del negocio.

Unificar, consolidar y definir las políticas, normas y procedimientos para todas las áreas de la compañía.

Comunicar a los Empleados (con contratos a término fijo, temporales, término indefinido, aprendiz etapa lectiva, aprendiz etapa productiva y estudiantes en práctica o pasante), Socios de negocios, Outsourcing, Proveedores y Clientes; las políticas de Seguridad de la información, las cuales son de obligatorio e imperativo cumplimiento.

2. ALCANCE

Elaborar, publicar, capacitar y cumplir con el manual de seguridad de la información para C.I CARBOCOQUE S.A, COLUMBIA COAL COMPANY S.A. e INDUCARBÓN LTDA en adelante "LAS COMPAÑÍAS", Aplicado para todos los Empleados (con contratos a término fijo, temporales, término indefinido, aprendiz etapa lectiva, aprendiz etapa productiva y estudiantes en práctica o pasante), Socios de negocios, Outsourcing, Proveedores y Clientes.

3. DEFINICIONES.

3.1 Amenaza: Potencial para causar un incidente indeseado que pueda resultar en daño al sistema de información.

3.2 Ataques: Tipos y naturaleza de inestabilidad en la seguridad.

3.3 Confidencial: Uno de los principios de la seguridad de la información, donde se establece que la información sólo puede ser vista por los autorizados.

3.4 Incidente: Se define como un incidente cualquier evento, indicio o sospecha inesperados que pueda poner en riesgo la disponibilidad, integridad o confidencialidad de la información

3.5 Malware: Software malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como virus, trojano, parásito, Spyware, etc.

3.6 Manual de Seguridad de la Información: Es un documento de alto nivel que describe en forma detallada las normas, políticas y procedimientos que deben adoptar los empleados y terceros de LAS COMPAÑÍAS respecto a la seguridad de la información.

3.7 PDAs: Dispositivos móviles que permiten las comunicaciones y el almacenamiento de información.

3.8 Riesgo: El riesgo de seguridad es el potencial de que cierta amenaza pueda explotar las vulnerabilidades para así ocasionar pérdidas o daños de información

3.9 Software Antivirus: Clase de software diseñado para reducir al mínimo la amenaza del malware identificando, previniendo y/o quitando varias formas de infección tales como virus, gusanos, Troyanos etc.

3.10 Spam: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican el correcto funcionamiento de los equipos.

3.11 Spyware: Programas elaborados para provocar daños en una máquina y así promover el uso de su reparador.

3.12 Ransomware: Programa malicioso que infecta los equipos con la capacidad de bloquear desde una ubicación remota y encriptar los archivos quitando el control de toda la información y datos almacenados.

3.13 Riesgo: Materialización de vulnerabilidades identificadas, así como el impacto negativo en la operación del negocio.

3.14 Seguridad: Protección contra riesgos.

3.15 Hacker: Persona con conocimientos avanzados que accede a los datos aprovechando las debilidades de los sistemas de información.

3.16 VPN: "Red privada virtual", que permite extender de manera segura los servicios.

3.17 NTC-ISO/IEC 27001: Norma Internacional que define un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

3.18 DUMPS: Errores generados en el sistema SAP a causa de valores no procedentes dentro de una transacción.

4. DESARROLLO.

4.1 PRINCIPIOS QUE GOBIERNAN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:

La Seguridad de la Información es un elemento fundamental en la Gestión de la Empresa, relacionada con aspectos como la administración de Tecnología y el cumplimiento de normas legales, por lo tanto requiere diversas obligaciones y de

estricto cumplimiento para los empleados, socios comerciales, consultores, proveedores y demás personas que ingresan a sus instalaciones.

Todo el personal (es decir: empleados y otros que actúan de forma similar como temporales, contratistas, consultores, aprendiz etapa lectiva, aprendiz etapa productiva y estudiantes en práctica o pasante), son responsables de cumplir con la Política de Seguridad de la información y proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido. Cualquier empleado o tercero que no cumpla con las políticas de seguridad, podrá ser objeto de medidas disciplinarias, incluyendo potencialmente el cese de la relación laboral o contrato.

Todos los empleados de las Compañías deben aceptar los acuerdos de confidencialidad, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Todo el personal debe recibir una formación adecuada y actualizaciones regulares en temas de seguridad de la información. Estos temas incluyen las políticas, normas, procedimientos, leyes, y reglamentos presentados a través de este documento.

Sólo el área de TI está autorizada para la aprobación, compra, conectividad de redes, instalación o desinstalación de software y hardware en las Compañías.

El área de Informática realizará revisiones periódicas al cumplimiento del manual de seguridad de la información.

Es responsabilidad del área de Gestión Humana y del área de IT, dar a conocer este documento a todos y cada uno de los empleados actuales y quien se vincule por cualquier medio a las Compañías. En el contrato de trabajo se debe dejar evidencia del conocimiento, cumplimiento y aceptación del Manual de Seguridad de la Información a través del Anexo 1. Consentimiento Informado de la Política y/o en un item clausular del contrato.

Es de responsabilidad de todos los usuarios de los sistemas de información de la organización Carbocoque incluidos empleados, contratistas, proveedores y terceros, independientemente de la ubicación desde la cual accedan y del tipo de dispositivo utilizado, usar cualquier aplicación, servicio o configuración destinada a ocultar, redirigir o alterar el tráfico de red o el comportamiento del sistema con el fin de eludir controles de seguridad establecidos por la organización. Esto incluye, pero no se limita a: VPN no autorizadas, Proxies o túneles no aprobados, herramientas de anonimización, software diseñado para eludir filtros, firewalls, sistemas de monitoreo o controles de acceso.

4.2 POLITICAS Y REGLAMENTACIÓN:

4.2.1 NORMAS DEL USO DE INTERNET.

La utilización del servicio de acceso a Internet es exclusivamente para asuntos relacionados con su actividad laboral, en caso de no uso para este fin habrán sanciones

Teniendo en cuenta la anterior disposición no está permitido:

• El acceso a páginas con contenido adulto, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética, la moral, las leyes vigentes de las buenas costumbres o políticas aquí establecidas.

• El acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, IM Skype, MSN Messenger, Yahoo, Ares, Net2phone, discos virtuales y cualesquiera otros similares, que tengan como objetivo crear comunidades para intercambiar o descargar información, o en todo caso para fines diferentes a las actividades propias del negocio por lo cual se generará un informe mensual.

• El intercambio no autorizado de información de propiedad de las Compañías, de sus clientes y/o de sus funcionarios, con terceros.

• Realizar o permitir la transmisión de material ilegal, amenazante, ofensivo, pornográfico que constituyan o animen la conducta criminal dando lugar una responsabilidad civil o violar de otra manera cualquier ley.

• La descarga, uso, intercambio y/o instalación de juegos, música, aplicaciones de uso libre, películas, protectores y fondos de pantalla, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros, sin haber pagado las regalías correspondientes al propietario del material y mantendrá exonerado o indemne a la Compañías de todo uso indebido.

• La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) con marcaciones de derecho de autor.

• Cada uno de los usuarios de equipos, hardware y software es responsable de dar un uso adecuado a estos recursos y en ningún momento pueden ser usados para realizar prácticas ilícitas o mal intencionadas que atenten internamente o contra terceros, la legislación vigente aplicable a seguridad de la información, entre otros.

• El servicio de Internet de acceso FULL, debe ser solicitado a nivel de Dirección de área para autorización del Director Administrativo y Financiero. Para los demás

casos se asignará el perfil de navegación según su rol dentro de la compañía.

• El servicio de Internet, está monitoreado permanentemente con el fin de identificar los usuarios que no cumplen las normas vigentes con respecto a la utilización de este servicio de red y será notificado al área de Gestión Humana y al Jefe inmediato.

4.2.2 CORREO ELECTRÓNICO:

Los empleados y terceros autorizados, a quienes las Compañías les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de las Compañías.
- Los mensajes y la información contenida en los buzones de correo son de propiedad de las Compañías. Cada usuario es responsable de mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- El tamaño de los buzones de correo es determinado por el Área de IT de acuerdo con las necesidades de cada usuario y previa autorización del jefe del área correspondiente, sólo tendrá acceso aquellas personas que están inscritas en el servidor de correo y no podrá reenviar las consultas de ese correo a otro dominio.

- El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo con dominio @carbocoque.com proporcionada a cada usuario, por tal motivo no es necesaria la activación de correos personales.

- El envío masivo de un mensaje corporativo "all@carbocoque.com" deberá contar con la aprobación de la Dirección de cada área.

- El tamaño máximo de archivos adjuntos dentro de un correo es de 10 MB a una sola cuenta, por tal motivo si es más de una cuenta se multiplica el valor por el total de cuentas a transmitir.

- El usuario del correo electrónico se compromete a mantener la confidencialidad de su contraseña de acceso, en caso de sentirse vulnerado debe solicitar el cambio al área de IT.

- Todo mensaje enviado con ocasión de sus funciones inherentes al cargo que desempeñe debe ir con la firma e identificación institucional, configurado en las plantillas de los correos a nivel corporativo.

NO ES PERMITIDO:

• Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo, o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico de la compañía, mensajes mal

intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

• Utilizar la dirección de correo electrónico de las Compañías como punto de contacto en comunidades interactivas de contacto social, tales como Facebook y/o Myspace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

• El envío o almacenamiento local de archivos de música, videos, ejecutables de extensión .exe .bat .com. qué no estén relacionados con ejercicio de su labor. En caso de requerir hacer un envío o almacenamiento de este tipo de archivos deberá ser autorizado por el Área de IT en su defecto la Dirección correspondiente; por otro lado, el uso de servidores de almacenamiento externo como dropBox, google drive, etc., debe ser autorizado por el área de IT.

• El correo asignado por la compañía no debe estar en dispositivos telefónicos no empresariales, esto debe estar autorizado por la Dirección correspondiente y/o el Jefe de IT.

4.2.3 RECURSOS TECNOLÓGICOS:

El uso adecuado de los recursos tecnológicos asignados por las Compañías se reglamenta bajo los siguientes lineamientos:

• La instalación o desinstalación de cualquier tipo de software o hardware en los equipos de cómputo de las Compañías es responsabilidad del área de IT exclusivamente, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados de manera legal cumpliendo con las normas de propiedad intelectual conforme a las leyes colombianas y/o internacionales según sea el caso.

• Los usuarios no deben realizar cambios en las estaciones de trabajo, relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, protector de pantalla, entre otros. Estos cambios son realizados únicamente por el área de IT.

• Los usuarios son los responsables de la buena utilización de los recursos tecnológicos asignados por la compañía, en caso de avería o daño por causas propias, asumirá su responsabilidad y deberá responder por los daños. Por tal motivo cada persona debe utilizar el recurso asignado apropiadamente y no permitir el uso indebido del mismo a terceros, ya que en todo caso cualquier daño o utilización indebida de la información que se haga desde el equipo, estará radicada en cabeza del usuario registrado por el área de IT.

• Sólo personal autorizado puede realizar actividades de administración y control remoto de dispositivos, equipos o servidores de la infraestructura de procesamiento de información utilizando esquemas de seguridad y administración definidos por el área de IT.

• Los usuarios están obligados a utilizar las herramientas informáticas que la compañía les proporciona para el desarrollo de su trabajo. En ocasión de requerir alguna herramienta diferente debe ser solicitada a la Dirección previo se haya aprobado el presupuesto de la misma.

• Para el acceso externo hacia cualquiera de los sistemas y servicios ofrecidos por la compañía, se debe hacer exclusivamente por canales seguros (VPN – redes virtuales privadas, Herramientas de conexión remota), establecidos y configurados por el área de IT.

• La sincronización, configuración y manejo de información de propiedad de LAS COMPAÑÍAS desde dispositivos móviles, tales como PDAs, Smartphones, celulares, IPAD, IPHONE, Hand-held, entre otros, debe ser canalizado por el Área de IT, previa autorización de la Dirección del área.

• Del uso de equipos y materiales de trabajo son exclusivos de las compañías y por ningún motivo se permite el acceso a las redes de comunicaciones y/o el uso de canales de internet a través de elementos de trabajo no asignados por las Compañías, cuando por motivos justificados de trabajo sea necesario acceder a dispositivos externos y/o comunicaciones; debe informarse a la Dirección correspondiente para la autorización, previo se haya verificado la terminal por parte del área de Tecnología y se minimice el riesgo de vulnerabilidad como virus o software malintencionado, de lo contrario no se podrá acceder.

• Se prohíbe el uso de computadores personales, tabletas o smartphones no corporativos para acceder a sistemas o manejar información de la empresa, como indica en el manual de Seguridad de la información, en tal evento de requerir por efecto de sus funciones, debe estar aprobado y firmado un consentimiento informado, firmado por el jefe inmediato y el por área de IT.

• Dentro de las auditorias del área de IT en función del cumplimiento del Manual de seguridad de la información que encuentre incumplimientos, es de carácter obligatorio reportar de inmediato al área de IT, para su correspondiente gestión.

• Del uso de impresoras, escáner, copiadoras y otros dispositivos de copia debe utilizarlos y de inmediato proceder a recoger los documentos impresos, dejando las bandejas limpias de información de las compañías, así como los buzones asignados por efectos de escáner.

• De responsabilidad de terminales de trabajo que cuando esté ausente de su puesto bloquear con contraseña la terminal para impedir vulnerabilidad en el acceso de la información y apagar la terminal terminada su jornada laboral, a menos que se le indique que se realizará un proceso administrativo a nivel de máquina como mantenimiento o copias de seguridad del mismo.

• De responsabilidad de terminales de trabajo que cuando termine su jornada laborar, cerrar todas las aplicaciones, apagar los equipos y desconectar del fluido eléctrico. Aplica si el personal por sus labores asignadas realiza desplazamiento entre sedes y/o entidades a visitar, como medida de protección de daño a las

máquinas.

• De salvaguarda y seguridad de las contraseñas se prohíbe la divulgación y o comunicación a personas no autorizadas, de igual forma cumplir con las políticas de construcción de contraseñas, teniendo previsto el cambio de las mismas con periodicidad, si siente que está vulnerada y/o a petición del administrador del sistema.

• De copias de seguridad y custodia de la información es responsabilidad del usuario mantener la estructura de carpetas (Mis Documentos, Correo y Escritorio) las cuales son protegidas por la estrategia de Backup de la compañía, en caso de tener por efectos de su trabajo carpetas con ubicaciones diferentes a las estipuladas dentro de la estructura de la compañía, informar al área de IT para incluir dentro del respaldo.

• De categoría de datos y documentos almacenados, es responsabilidad de los usuarios no tener copias de ejecutables, fotos personales, videos personales y/o documentos que no corresponden a los soportes del cargo asignado.

• De mantenimiento de documentos almacenados es responsabilidad de los usuarios organizar la información de tal manera que no se tenga la misma versión del documento contenido en diferentes carpetas dentro de la estructura definida para ello, teniendo como premisa el buen uso de la información.

• Es de obligatoriedad notificar las incidencias de las que tenga conocimiento a nivel de seguridad de la información al área de IT quienes se encargarán de su gestión y resolución.

• De legalidad del contenido y propósito del Dominio se declara que el Dominio o los Dominios administrados por las compañías no han sido registrados y no serán usados para propósito alguno que sea fraudulento y legítimo o que entre en conflicto con las leyes, reglas, regulaciones políticas, ordenanzas o decretos aplicables al uso del dominio, incluyendo correo, uso sistematizado de programas, violación de derechos legítimos de propiedad intelectual o derechos marcarios o cualquier otra práctica abusiva y pueda ser objetada por los administradores o ente gubernamental.

• De responsabilidad de colaboradores, practicantes, pasantes, personal en formación o estudios paralelos probar herramientas, scripts, IA, software o técnicas sin autorización previa del área de IT, estrictamente prohibido usar datos reales de la empresa para tareas académicas y/o subir información corporativa a plataformas externas. (Ej. IA, nubes, repositorios) sin previa autorización del área de IT, la falta de intensión no exime de responsabilidad.

• Normas explícitas relacionadas con el estudio y experimentación, el colaborador solicita autorización por correo a datosmaestros@carbocoque.com donde describe que quiere probar, qué herramienta usará, qué información se verá afectada con el fin de validar un entorno seguro apoyando el aprendizaje pero de forma

controlada, con aprobación de la Dirección.

• El usuario es responsable del uso adecuado de los equipos asignados a su cargo en el cuidado físico, evitando aplicar fuerza excesiva en los puertos, periféricos y componentes, así como asegurar el transporte seguro y prohibido las modificaciones físicas no autorizadas como remover piezas, forzar conexiones, etc.

4.2.4 SEGURIDAD DE EQUIPOS Y MEDIOS DE INFORMACIÓN FUERA DE LAS INSTALACIONES DE LAS COMPAÑIAS:

Todos los empleados son responsables de velar por la seguridad de los equipos y medios de información de las Compañías que se encuentren fuera de las instalaciones y le hayan sido asignados, siguiendo las siguientes directrices:

• Bajo ninguna circunstancia los equipos de cómputo pueden ser dejados o desatendidos en lugares públicos o a la vista.

• Los equipos portátiles siempre deben ser llevados como equipaje de mano y con las medidas de seguridad necesarias. Se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

• Los equipos de las Compañías cuentan con un seguro que los protege de robo o pérdida, pero es responsabilidad del usuario la buena manipulación y cuidado que exige un equipo fuera de la compañía. Sin embargo, el costo de la suma deducible del respectivo seguro, estará a cargo del usuario si se comprueba que la pérdida del (de los) equipo(s) se produjo por negligencia o descuido, o se encontraba(n) en manos de terceros no autorizados.

• En caso de pérdida, daño o robo de un equipo, se deberá informar inmediatamente al área de IT y se deberá poner la denuncia ante la autoridad competente máximo en los 5 días calendarios siguientes a la fecha del siniestro, so pena de incurrir en la totalidad del costo del mismo.

4.2.4.1 Transporte seguro de equipos en exteriores.

Todo equipo que contenga información de la organización y sea transportado fuera de las instalaciones deberá cumplir las siguientes directrices:

- Utilizar maletines, estuches o embalajes diseñados para protección física, resistentes a golpes, polvo y humedad.
- Evitar dejar equipos desatendidos en espacios públicos o vehículos.
- No exponer los equipos a temperaturas extremas, radiación solar directa o lluvia.
- Cuando aplique, los dispositivos deberán contar con cifrado de información y mecanismos de autenticación.

- El transporte deberá ser realizado únicamente por personal autorizado.

4.2.4.2 Almacenamiento seguro en exteriores o ubicaciones no controladas.

Cuando el almacenamiento de equipos en exteriores o ubicaciones temporales sea necesario, se deberán cumplir las siguientes medidas:

- Almacenar los equipos en contenedores o gabinetes seguros, con protección contra agua, polvo y manipulación no autorizada.
- Mantener los equipos elevados del suelo cuando exista riesgo de humedad o inundación.
- Limitar el acceso únicamente a personal autorizado.
- Realizar inspecciones periódicas para verificar el estado físico del equipo.

4.2.4.3 Notificación de incidentes de seguridad física.

Todo incidente que pueda comprometer la seguridad física del equipo o la información deberá ser notificado de forma inmediata.

Se consideran incidentes, entre otros:

- Caídas, golpes o vibraciones fuertes.
- Exposición a líquidos, humedad o lluvia.
- Manipulación no autorizada o intento de robo.
- Daños visibles o funcionamiento anómalo posterior a un evento físico.

Por tal motivo el incidente deberá ser reportado inmediatamente al área de IT.

- El reporte debe incluir fecha, lugar, descripción del incidente y equipo afectado, estos datos son solicitados dentro de las garantías.
- El equipo no deberá ser utilizado hasta que sea evaluado por el personal autorizado de IT.
- El área de IT evaluará el impacto y definirá acciones correctivas a que dé a lugar.

Escalamiento de garantía con fabricante.

- Después de realizar la revisión técnica del equipo por parte del área de IT y gestionar el caso con fabricante de la marca y aplicación de la garantía, se informará que el escalamiento por garantía fue rechazado y/o aplicado de acuerdo a términos y condiciones de fábrica.

  Según el diagnóstico técnico del soporte del fabricante, si el daño identificado está asociado a una manipulación o uso inadecuado del recurso tecnológico, lo cual se encuentra fuera de las condiciones de cobertura establecidas por la garantía del fabricante, este será informado a recursos humanos y jefe inmediato,

para las acciones correspondientes.

4.2.5 ERP (SAP) Y SOFTWARE DE ALTO IMPACTO - SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBA Y PRODUCCIÓN:

Dentro del sistema LAS COMPAÑÍAS cuentan con tres ambientes para la ejecución de actividades:

- ✓ Desarrollo
- ✓ Pruebas
- ✓ Producción

• En todas las aplicaciones de impacto del negocio, se debe garantizar que se ejecute las anteriores fases para garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad.

• Los usuarios permitidos para la ejecución y manipulación de estos ambientes son los autorizados por el área de IT, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

• Es de carácter Obligatorio el acceso al sistema SAP y otro software de alto impacto desde equipos corporativos asignados a los usuarios por parte de la compañía. Cualquier acceso desde otro equipo no autorizado por el área de IT, se tendrá por no permitido, dando lugar a la aplicación de sanciones disciplinarias, sin perjuicio de las demás acciones legales con que cuentan LAS COMPAÑIAS, para salvaguardar sus derechos, dependiendo del alcance del daño causado, o del uso indebido de la información obtenida por ese medio.

• Es de responsabilidad del usuario si va a acceder desde otro país a la aplicación SAP para desarrollo de sus labores, informar al área de IT con el fin de aperturar los canales del país en la plataforma Cloud, por un espacio de tiempo determinado y autorizado por la Dirección correspondiente.

• Es de responsabilidad del usuario si va a acceder a una transacción no autorizada en la aplicación SAP para desarrollo de sus labores, informar al área de IT con el fin de revisar el rol pertinente a cargo con el líder del módulo para su autorización y afinación del perfil.

• El área de IT con soporte externo, monitorea los sistemas de Desarrollo y Productivo diariamente y previene los DUMPS generados por los usuarios. Es de responsabilidad del usuario si el sistema le genera un error informar inmediatamente al área de IT.

• Es de responsabilidad del usuario la información que se captura debe ser coherente, veraz, integrada, confiable y soportada por documentos de procesos de negocio.

• Es de responsabilidad del usuario que la información que se descarga a través

de las diferentes funcionalidades de integración con otras aplicaciones sea custodiada y utilizada en función del proceso de negocio a cargo.

4.2.6 PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y VIRUS

El área de tecnología debe garantizar que todos los recursos informáticos estén protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red.

NO ES PERMITIDO:

• La desinstalación y/o desactivación de software y herramientas de seguridad instaladas por el área de Tecnología.

• Utilizar medios de almacenamiento físico o virtual sin que se haya realizado la revisión de antivirus por parte del área de IT.

4.2.7 CONTROL DE ACCESOS DE USUARIO

• Todos los Sistemas de información críticos de las Compañías, tienen asignados los privilegios de acceso con base en los roles y perfiles que cada empleado requiera para el desarrollo de sus funciones, definidos y aprobados por los directores de cada área y administrados por el área de IT.

• Todo empleado o tercero que requiera tener acceso a los sistemas de información, debe estar plenamente autorizado y acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y una contraseña (password) asignado(s) por las compañías. El empleado será responsable por el buen uso de las credenciales de acceso que le sean asignadas, así como por el uso que permita de éstas a terceros.

• El usuario es el responsable del cambio periódico de claves y contraseñas seguras asignadas para los diferentes sistemas de información.

4.2.8 COPIAS DE RESPALDO Y ARCHIVO.

El área de IT, debe asegurar que la información con cierto nivel de clasificación contenida en la plataforma tecnológica, como servidores, File server, estaciones de trabajo, entre otros, sean periódicamente resguardadas mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. (Ver Procedimiento "Almacenamiento de información y Backup")

4.2.9 PROTECCIÓN CENTROS DE CÓMPUTO Y MONITOREO DE CÁMARAS.

• Los centros de cómputo instalados en las diferentes sedes deben incorporar medidas de protección para reducir al mínimo la posibilidad de accesos no

autorizados.

• Los responsables del área de IT, están capacitados en la administración, manejo y procedimientos que deben seguir cuando se presente un evento tanto técnico como físico que afecte la continuidad en la operación del centro de cómputo.

• Cuando se realicen adiciones o modificaciones del cableado eléctrico, lógico o de voz, el área de IT debe brindar las pautas para ejecutar el trabajo por parte de contratistas y/o externos del área de Sistemas.

• Los procedimientos del centro de cómputo deben ser aprobados por el Jefe de IT.

• El acceso no autorizado a los centros de cómputo y/o monitores de cámaras procedimientos del centro de cómputo deben ser aprobados por el Jefe de IT y el área de seguridad de la empresa que aplique.

4.2.10 COMUNICACIÓN DE INCIDENTES Y EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

• Se considera como un evento de seguridad, cualquier situación que indica una posible violación a las políticas de seguridad de la información que contiene este documento o las fallas en los controles que no genere un impacto en el desarrollo de las operaciones de la compañía y que pueden ser controlados rápidamente.

• Todo funcionario y/o tercero de las Compañías debe reportar mediante un correo electrónico al Jefe de IT, cualquier situación que se pueda considerar como un evento de seguridad y que comprometa o pueda comprometer la preservación de la confidencialidad, disponibilidad y/o integridad de la información.

• Es responsabilidad del Jefe de IT, determinar si la situación reportada corresponde a un evento o a un incidente de seguridad y ejecutar las acciones necesarias según el caso.

• Es de responsabilidad del usuario que detecte daños físicos visibles, pérdida o robo de equipos, fallas recurrentes en periféricos o hardware en general, síntomas como calentamiento excesivo, olores, sonidos o luces anómalas debe ser reportado inmediatamente al área de IT en un rango no mayor de 2 horas y no esperar cuando el equipo deje de funcionar.

4.2.11 DERECHOS DE PROPIEDAD INTELECTUAL

• Las Compañías cumplirán con las leyes y demás disposiciones aplicables sobre propiedad intelectual vigentes en el país y ejecutarán revisiones periódicas para asegurar que se estén respetando los derechos de propiedad intelectual.

• El área de IT, es responsable de mantener y administrar el inventario y control

de todas las licencias de software, hardware y aplicaciones utilizadas en las Compañías, así como los medios y contratos que se relacionan con la actividad comercial de compra de software y hardware para éstas. Para ello se incorpora dentro del sistema de información de la compañía SAP.

• Está prohibido el uso de software ilegal o no licenciado, los empleados que utilicen software no autorizado en sus estaciones de trabajo asumirán la responsabilidad ante las autoridades competentes y en consecuencia serán objeto de las medidas disciplinarias a que haya lugar, incluyendo el cese de la relación laboral o contrato.

4.2.12 DAÑO, PÉRDIDA, HURTO DE EQUIPOS

De acuerdo con lo señalado en los artículos 58 numeral 3. 149 y 151 del Código Sustantivo del Trabajo, el usuario en su condición de Trabajador autorizará expresamente a las compañías con la suscripción del formulario o acta de entrega del equipo, para que se le retenga de su salario o de la liquidación final de prestaciones sociales, salarios e indemnizaciones si llegara a finalizar el contrato de trabajo por cualquier causa, las sumas de dinero que se generen y que le indique la Compañía, con ocasión de cualquier eventualidad relacionada con la sustracción o no devolución del equipo, así como los daños o del deterioro injustificado que cause personalmente o permita causarlo a terceros, por descuido o negligencia en el(los) equipo(s) asignado(s) y/o en el software y hardware de éste (éstos), para el desempeño de su cargo o labor. Una vez verificado lo anterior el área de IT procederá a expedir él paz y salvo respectivo.

4.2.13 PROTECCIÓN ELÉCTRICA Y DESCONOCEXIÓN SEGURA.

El incumplimiento de esta política podrá derivar en sanciones administrativas y/o la responsabilidad por daños ocasionados a los equipos.

4.2.13.1. Desconexión Segura.

- Todo usuario deberá guardar su trabajo antes de apagar o desconectar el equipo.
- Apagar el sistema operativo correctamente antes de retirar el cable de alimentación.
- Evitar desconectar equipos mientras estén en funcionamiento, salvo en casos de emergencia.
- No desconectar dispositivos de almacenamiento sin utilizar la opción de "expulsión segura".

4.2.13.2. Protección ante picos de voltaje eléctrico.

- Los equipos deberán conectarse únicamente a tomas con regulador de voltaje o UPS. (Naranjas)

- No se permitirá la conexión directa a enchufes sin protección cuando exista riesgo eléctrico.
- Durante tormentas eléctricas o cortes frecuentes de energía, los usuarios deberán apagar y desconectar los equipos si no cuentan con protección adecuada.
- Queda prohibido el uso de extensiones o multi tomas en mal estado.

4.2.14 ACTA DE MOVIMIENTO DE EQUIPOS

Todo funcionario debe reportar al área de IT, el movimiento de(los) equipo(s), que realice fuera de las instalaciones de las Compañías o dentro de las mismas instalaciones, indicando el lugar y fechas de salida y reintegro al lugar en las que éste (éstos) deba(n) permanecer, y cuando sea procedente, contar con la aprobación del jefe inmediato.

4.2.15 CONTROLES DE LOS ACTIVOS TECNOLÓGICOS.

4.2.15.1 Manipulación de puertos y conectores.

- Los usuarios deben conectar y desconectar dispositivos periféricos (USB, HDMI, red, energía) de forma cuidadosa, evitando aplicar fuerza excesiva.
- Los usuarios deben utilizar únicamente puertos y conectores autorizados por la organización.
- Los usuarios deben verificar que los conectores estén alineados correctamente antes de su inserción.
- Es de responsabilidad no forzar la conexión de dispositivos incompatibles, no utilizar adaptadores, extensiones o cables en mal estado y/o conectar dispositivos de almacenamiento externos no autorizados.

Cabe mencionar que el mal uso puede causar incidentes de seguridad o indisponibilidad del servicio, afectando la operatividad del trabajo asignado.

4.2.15.2 Ubicación segura de equipos en escritorios.

- Los equipos de cómputo deben ubicarse sobre superficies estables, limpias y secas.
- Los equipos de cómputo deben mantenerse alejados de líquidos, fuentes de calor y bordes del escritorio, con disposición por SST.
- Los equipos deben contar con ventilación adecuada, evitando obstruir las rejillas de aire.
- Los usuarios de equipos de cómputo deben bloquear la sesión al ausentarse del puesto de trabajo.
- No se permite apilar objetos sobre los equipos de cómputo ni cerrar las tapas de los portátiles con hojas y/o objetos que puedan dañar tanto la carcaza del equipo como su monitor.
- No se permite ubicar los equipos en el suelo o zonas del alto riesgo.
- No se permite conectar los equipos a tomas donde queden los cables tendidos ocasionando tropiezos o caídas.
- Revisar que el cable de conexión esté en condiciones óptimas, sin rupturas de hilos, quemaduras y demás, reporte de inmediato y no conecte la unidad.

4.2.15.3 Verificación básica del estado eléctrico.

- Los usuarios deben verificar que los cables de energía estén en buen estado antes de su uso.
- Conectar el equipo únicamente a tomas eléctricas certificadas o reguladas.
- Reportar chispas, olores, ruidos o calentamiento anormal.
- Los usuarios no deben enchufar con las manos húmedas.
- No se debe sobrecargar tomas eléctricas o extensiones.
- No desconectar equipos de forma abrupta sin el procedimiento adecuado.

4.2.15.4 Responsabilidad del usuario.

- Adoptar hábitos de cuidado físico de los equipos asignados.
- Participar en actividades de concientización en seguridad de la información.
- Reportar oportunamente cualquier condición insegura.
- Garantizar la limpieza del equipo, informar al área de IT para los procesos pertinentes.
- Borrar el caché y las cookies de los exploradores, informar al área de IT para los procesos pertinentes.
- No guardar contraseñas ni usuarios en plataformas en los navegadores.
- Evite entrar en los navegadores como incognito, las actividades a sitios web son monitoreadas por el antivirus de la máquina.
- Mantenga la información crítica de negocio archivada adecuadamente en la carpeta de Documentos.
- Mantenga el escritorio de su computadora limpio; en un espacio ordenado mejora la concentración, el bienestar mental y la eficiencia general, tanto física como digitalmente.
- Cambie periódicamente las contraseñas de las aplicaciones.
- Mantener la confidencialidad, integridad de la información aplicando los principios de la Ley 1581 de Protección de datos, es decir, es responsable por la documentación física y digital de los mismos.
- Debe mantener los principios y valores definidos en el **PTEE** "Programa de Transparencia y Ética Empresarial del Grupo Carbocoque".
- Debe cumplir los lineamientos establecidos en el LA/FT/FPADM – SAGRILAFT "Sistema de autocontrol y gestión del riesgo del lavado de activos y financiación del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva"

Sra. Camila Pachón Coordinador de Procesos _____ Ing. Brayan Daza Técnico de Sistemas _____	Ing. Johan Núñez Analista de Sistemas _____	Ing. Martha Castañeda. Jefe de IT y procesos _____	Dr. Alejandro Navarrete. Director Administrativo y Financiero. _____	13/06/2025

CONTROL DE CAMBIOS:

Versión:	Fecha de Actualización:	Elaboró:	Revisó:	Aprobó:
03	13/06/2025	Sr. Brayan Daza Ing. Martha Castañeda	Ing. Martha Castañeda. Ing. Johan Núñez	Dr. Alejandro Navarrete.

Qué se modifica:

- La ampliación de la sección 4.2.3 con lineamientos de cuidado físico y manipulación adecuada.
- La explicitación de la prohibición de software de evasión en la sección 4.1.
- La nueva sección 4.2.13 sobre protección eléctrica y desconexión segura.
- El refuerzo del protocolo de reporte en 4.2.10 con el límite de 2 horas.
- Las directrices de transporte y almacenamiento seguro en 4.2.4.
- La integración de buenas prácticas en 4.2.15 sobre manipulación, ubicación y verificación eléctrica.

Versión:	Fecha de Actualización:	Elaboró:	Revisó:	Aprobó:
02	18/01/2020	Ing. Juan David Vásquez Analista de Procesos	Ing. Martha Castañeda. Jefe de IT y procesos	Dr. Alejandro Navarrete. Director Administrativo y Financiero

Qué se modifica:

- Actualización de firmas de acuerdo con el Instructivo de Codificación de Documentos Oficiales
- Se amplía el alcance del objetivo del procedimiento a extensiones, creación de material bajo modelo preexistente, y la modificación de materiales.
- Se agregan más campos de diligenciamiento y notas al proceso.

Se agrega los numerales 4.5, 4.6 y 4.7 correspondientes a la creación de materiales: productos semielaborados.				
Versión:	**Fecha de Actualización:**	**Elaboró:**	**Revisó:**	**Aprobó:**
01	03/03/2017	Ricardo Páez Coordinador Operativo de Sistemas	Ing. Martha Castañeda. Jefe de IT y procesos	Dr. Alejandro Navarrete. Director Administrativo y Financiero

Qué se modifica:

- Códigos de estructura del documento y actualización de firmas de acuerdo con el Instructivo de Codificación de Documentos Oficiales