POLÍTICAS DE SEGURIDAD INFORMATICA

CONTROL DE VERSIONES SGC- CAMBIOS- REVISIONES

Fecha (D-M-A)	DESCRIPCIÓN DE LA MODIFICACÍÓN, REVISIÓN O CAMBIO	VERSION SGC	RESPONSABLE
30-11-11	Documento original	1	Julio Ernesto Herrera Orjuela
18-10-12	Cambio de codificación del documento	2	Julio Ernesto Herrera Orjuela
25-07-13	Cambio de versión SGC	3	Julio Ernesto Herrera Orjuela

CORPORACION FONDO DE EMPLEADOS DE LA INDUSTRIA PETROLERA COLOMBIANA

"CORPECOL"

POLITICA DE SEGURIDAD INFORMATICA CORPECOL

INTRODUCCION:

Este documento pretende, servir como guía, estableciendo las reglas, normas, controles y procedimientos que regulen la forma en que CORPECOL, prevenga, proteja y maneje los riesgos de seguridad en diversas circunstancias. Las normas y políticas expuestas en este documento sirven de referencia, no proyectan en convertirse en normas absolutas, ya que éstas buscan ser flexibles y adaptarse a las circunstancias y experiencias empresariales que contribuyan con el fortalecimiento de la seguridad.

En términos generales estas políticas de seguridad informática, propende por englobar los procedimientos más adecuados, tomando como lineamientos principales cuatros criterios, que se detallan a continuación:

Seguridad Organizacional: Dentro de este, se establece el marco formal de seguridad que debe sustentar CORPECOL, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.[1]

Seguridad Lógica: Trata de establecer e integrar los mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.[2]

Seguridad Física: Identifica los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.[3]

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los funcionarios, asociados y usuarios de la red institucional bajo la reglamentación de la normativa interna de CORPECOL; en cuanto al recurso humano, tendrá sanciones aplicables ante faltas cometidas de acuerdo con la Ley o la normativa interna estipulada.[4]

---

[1] Universidad de Oriente de San Miguel (El Salvador). Normas y Políticas de Seguridad Informática. http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica (extraído el 1 de mayo de 2011). P 3.

[2] Universidad de Oriente de San Miguel (El Salvador). Normas y Políticas de Seguridad Informática. http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica (extraído el 1 de mayo de 2011). P 3.

[3] Universidad de Oriente de San Miguel (El Salvador). Normas y Políticas de Seguridad Informática. http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica (extraído el 1 de mayo de 2011). P 3.

[4] Universidad de Oriente de San Miguel (El Salvador). Normas y Políticas de Seguridad Informática. http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica (extraído el 1 de mayo de 2011). P 4.

Cada uno de los criterios anteriores, sustenta un entorno de administración de suma importancia, para la seguridad de la información dentro de la red institucional de CORPECOL.

OBJETIVO:

Establecer las responsabilidades, principios, criterios, directrices y conductas dentro de los lineamientos de ética y el buen gobierno de CORPECOL, que orientan la gestión segura de la información.

ALCANCE:

El alcance de la misma es aplicable a CORPECOL y las unidades de negocios de PROYECTOS CORPECOL SAS; es de obligatorio cumplimiento por parte de los administradores, funcionarios y contratistas, así como todas aquellas personas que tengan establecida o establezcan relaciones comerciales con CORPECOL, las cuales tengan acceso a cualquier activo de información de propiedad de CORPECOL o de terceros con vínculos comerciales o laborales con el fondo de empleados.

BASE LEGAL:

La elaboración de la política de seguridad informática, está fundamentado bajo las normas:

ISO/IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements

ISO/IEC 27002:2005. Information technology – Security techniques. Code of practice for information security management.

Alineadas con el reglamento interno de trabajo y otra normativa interna de CORPECOL.

VIGENCIA:

Esta política de seguridad entrará en vigencia al ser aprobado como documento técnico de seguridad informática por el Gerente de CORPECOL y quedé debidamente registrado en el Sistema de Gestión de Calidad del fondo de empleados. Esta normativa deberá ser revisada y actualizada de acuerdo con las exigencias de CORPECOL, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la red institucional.

GLOSARIO:

Activos de información: Es cualquier elemento físico, tecnológico o intangible que genera, almacena o precisa información y tiene valor para la organización. La información, como activo corporativo, puede existir de muchas formas: impresas, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en videos, suministrada en una conversación, conocimiento de una persona, entre otros.

Administración Remota: Forma de administrar los equipos informáticos o servicios de CORPECOL, a través de terminales o equipos remotos, físicamente separados del fondo de empleados.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Archivo Log: Ficheros de registro o bitácoras de sistemas, en los que se recoge o anota los pasos que dan (lo que hace un usuario, como transcurre una conexión, horarios de conexión, terminales o IP´s involucradas en el proceso, entre otros)

Ataque: Evento, exitoso o no, que atenta contra el buen funcionamiento del sistema.

Confiabilidad: La información debe describir la realizada por el fondo de empleados, es decir debe reflejar fielmente sus transacciones y operaciones. La falta de confiabilidad puede exponer a CORPECOL a algún tipo de incumplimiento regulatorio.

Confidencialidad: La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legitima para la realización de sus funciones. La revelación no autorizada de la información con confidencialidad alta o media implica un grave impacto en CORPECOL, en términos económicos, de su imagen y ante sus clientes.

Cuenta de usuario: Mecanismo de identificación de un usuario o método de acreditación o autenticación del mismo mediante procesos lógicos dentro de un sistema informático.

Consentimiento: La información tratada por CORPECOL, debe ser utilizada con los fines para los cuales fue obtenida y/o creada, y con el conocimiento y aceptación informada de su titular o propietario.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadores necesarios para la operación normal del negocio.

Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso; la no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad de nuestros clientes.

Encriptación: Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

Impacto: Consecuencia de la materialización de una amenaza.

ISO: (Organización Internacional de Estándares) Institución mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.

IEC: (Comisión Electrotécnica Internacional) que en equipo con la ISO, desarrolla estándares que son aceptados a nivel internacional.

Integridad: La información de CORPECOL, debe ser clara y completa y sólo podrá ser modificada por las personas expresamente autorizadas para ello. La falta de integridad de la información puede exponer a la empresa a tomar decisiones incorrectas, lo cual puede ocasionar pérdidas de imagen o pérdidas financieras.

Normas de seguridad: Son un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y

acorde con las necesidades de seguridad establecidas para el entorno administrativo de la red institucional. [5]

Outsourcing: Contrato por servicios a terceros, tipo de servicio prestado por personal ajeno a la institución.

Políticas de seguridad: Son una forma de comunicación con el personal, ya que las mismas constituyen un canal formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una empresa previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de éstos. [6]

Responsabilidad: En términos de seguridad, significa determinar qué individuo en la entidad, es responsable directo de mantener seguros los activos de cómputo e información.

Riesgo: Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

Servicio: Conjunto de aplicativos o programas informáticos, que apoyan la labor operativa y/o administrativa, sobre los procesos diarios que demanden información o comunicación de CORPECOL.

Soporte Técnico Primer Nivel: Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores o equipo de oficina dentro de CORPECOL.

Soporte Técnico Segundo Nivel: (Personal en Outsourcing), personal designado o encargado de velar por el correcto funcionamiento a nivel hardware de las estaciones de trabajo, servidores o equipo de oficina dentro de CORPECOL; o cuando el incidente requiera un conocimiento más especializado.

Terceros: Proveedores de software u otros que tengan acuerdos contractuales con CORPECOL.

Tratamiento de la información: Desarrollo de las siguientes actividades sobre la información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.

Usuario: Define a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional.

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

DESARROLLO:

1. SEGURIDAD ORGANIZATIVA

1.1. POLÍTICAS DE SEGURIDAD

[5] Universidad de Oriente de San Miguel (El Salvador). Normas y Políticas de Seguridad Informática. http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica (extraído el 1 de mayo de 2011). P 8.

[6] Universidad de Oriente de San Miguel (El Salvador). Normas y Políticas de Seguridad Informática. http://es.scribd.com/doc/2023909/manual-de-politicas-y-normas-de-seguridad-informatica (extraído el 1 de mayo de 2011). P 8.

1. Los servicios de la red institucional son de exclusivo uso operativo, técnicos y para gestiones administrativas, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento.

2. CORPECOL nombrará a un responsable, que haga seguimiento al cumplimiento de la normativa y propicie el entorno necesario para crear una cultura de seguridad informática, el cual tendrá entre sus funciones:

a) Velar por la seguridad de los activos informáticos.

b) Gestionar y procesar la información.

c) Cumplir y verificar la aplicación de las políticas.

d) Elaborar informe que permita por parte del Gerente la aplicación de sanciones.

e) Elaborar planes de seguridad informática.

f) Capacitar o propender por la formación de los usuarios en temas de seguridad informática.

g) Gestionar y coordinar esfuerzos, por crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de CORPECOL. El mismo orientará y guiará a los funcionarios, la forma o métodos necesarios para enfrentar cualquier eventualidad que se presente.

h) Informar sobre problemas de seguridad a la alta administración de CORPECOL.

i) Hacer seguimiento y control sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

3. El dueño de cada proceso y su asistente (si aplica), dentro de la red institucional es el único responsable de las actividades procedentes de sus acciones.

4. El Coordinador de Sistemas es el encargado de mantener en buen estado los servidores dentro de la red institucional.

5. Todo usuario de la red institucional de CORPECOL, gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad de la red institucional, sus servicios o cualquier otra red ajena a CORPECOL.

6. Los usuarios tendrán el acceso a Internet, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la Coordinación de Sistemas.

1.2. CLASIFICACIÓN Y CONTROL DE ACTIVOS

1.2.1. RESPONSABILIDAD POR LOS ACTIVOS

1. Cada Coordinación, tendrá un responsable por el/los activo/s crítico/s o de mayor importancia para CORPECOL.

2. La persona responsable de los activos de cada Coordinación, velará por salvaguardar los activos físicos (hardware y medios magnéticos, aires acondicionados, mobiliario, entre otros), activos de información (bases de datos, archivos, documentación de sistemas, procedimientos operativos, configuraciones) y activos de software (aplicaciones, software de sistemas, herramientas y programas de desarrollo).

3. Los administradores de los sistemas son los responsables de la seguridad de la información almacenada en esos recursos.

1.2.2. CLASIFICACIÓN DE LA INFORMACIÓN

1. De forma individual, las Coordinaciones de CORPECOL, son responsables, de clasificar de acuerdo con el nivel de importancia, la información que en ella se procese.

2. Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:

a) Pública
b) Interna
c) Confidencial

3. Los activos de información de mayor importancia para CORPECOL deberán clasificarse por su nivel de exposición o vulnerabilidad.

1.3. SEGURIDAD LIGADA AL PERSONAL

Referente a contratos:

1. Se entregará al contratado, toda la documentación necesaria para ejercer sus labores dentro de CORPECOL, en el momento en que se dé por establecido su contrato laboral.

El funcionario:

2. La información procesada, manipulada o almacenada por el funcionario es propiedad exclusiva de CORPECOL.
3. CORPECOL no se hace responsable por daños causados por sus funcionarios a la información o activos de procesamiento, propiedad de CORPECOL, daños efectuados desde sus instalaciones de red a equipos informáticos externos.

1.3.1. CAPACITACIÓN DE USUARIOS

1. Los usuarios de la red institucional, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

2. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación al personal ajeno o propio de CORPECOL, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga material de importancia considerable para CORPECOL.

1.3.2. RESPUESTAS A INCIDENTES Y ANOMALÍAS DE SEGURIDAD

1. Se realizarán respaldos de la información (back up), diariamente, para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado mensualmente, el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.

2. Las solicitudes de asistencia, efectuadas por dos o más funcionarios o Coordinaciones, con problemas en las estaciones de trabajo, deberá dárseles solución en el menor tiempo posible.

3. El Coordinador de Sistemas deberá elaborar un documento donde deba explicar los pasos que se deberán seguir en situaciones contraproducentes a la seguridad y explicarlo detalladamente en una reunión ante el personal de respuesta a incidentes.

4. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, posterior a la revisión de los registros o log de sistemas con el objetivo de verificar la situación y dar una respuesta congruente y acorde al problema, ya sea está en el ámbito legal o cualquier situación administrativa.

2. SEGURIDAD LÓGICA

2.1. CONTROL DE ACCESOS

1. El Coordinador de Sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros.

2. Cualquier petición de información, servicio o acción proveniente de un determinado usuario o Coordinación, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por CORPECOL, para realizar dicha acción; la no aplicación de este procedimiento implica:

a) Negar por completo la ejecución de la acción o servicio.

b) Informe completo dirigido al Gerente, comunicando la anomalía.

c) Sanciones aplicables por la Gerencia.

2.1.1. ADMINISTRACIÓN DEL ACCESO DE USUARIOS

1. Son usuarios de la red institucional los funcionarios de CORPECOL y toda aquella persona, que tenga contacto directo como funcionario y utilice los servicios de la red institucional de CORPECOL.

2. Cuando se cuente con la misma, se asignará una cuenta de acceso a los sistemas de la intranet, a todo usuario de la red institucional, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.

3. Los visitantes (miembros de Junta Directiva, Comités o Comisiones entre otros), son usuarios limitados, estos tendrán acceso únicamente a los servicios de Internet (de acuerdo con la navegabilidad permitida por el administrador de red) y recursos compartidos de la red institucional (debidamente autorizado por la Gerencia), cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.

4. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con CORPECOL fuera del ámbito de funcionario y siempre que tenga una vinculación con los servicios de la red institucional.

5. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia el fondo de empleado y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

6. No se proporcionará el servicio solicitado por un usuario o Coordinación, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

7. Se creará una cuenta temporal del usuario, en caso de olvido o extravío de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando se muestre un documento de identidad personal.

8. La longitud mínima de caracteres permisibles en una contraseña se establece en 6 caracteres y máxima de 12, los cuales tendrán una combinación alfanumérica, con mayúsculas y minúsculas,

incluyendo en esta mínimo un carácter especial.

2.1.2. RESPONSABILIDADES DEL USUARIO

1. El usuario es responsable exclusivo de mantener a salvo su contraseña.

2. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.

3. Se debe evitar el guardar o escribir las contraseñas en cualquier papel, superficie o dejar constancia de ellas, a menos que esté guardada en un lugar seguro.

4. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por la Coordinación de Sistemas o a quien este delegue, que contenga información que pueda facilitar a un tercero la obtención de datos de su cuenta de usuario.

5. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de parientes, como fechas de cumpleaños o alguna otra fecha importante.

6. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en el, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

7. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos CORPECOL, está obligado a reportarlo a los administradores del sistema.

8. Los usuarios visitantes (miembros de Junta Directiva, Comités o Comisiones entre otros), son responsables de guardar sus trabajos en USB o similar, siempre y cuando hayan sido revisados y autorizado por una persona competente, para evitar cualquier pérdida de información valiosa y/o sensible.

Uso de correo electrónico:

1. El servicio de correo electrónico, es un servicio gratuito, y no garantizable, se debe hacer uso del mismo, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

2. El correo electrónico es de uso exclusivo, para los funcionarios de CORPECOL y para quien determine el Gerente.

3. Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

4. El usuario será responsable de la información que sea enviada con su cuenta.

5. La Coordinación de Sistemas, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

6. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

2.1.3. SEGURIDAD EN ACCESO DE TERCEROS

1. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.

2. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado y acatar las responsabilidades que devengan de la utilización del mismo.

3. Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno del fondo de empleado, además de los requisitos expuestos en su contrato con CORPECOL.

2.1.4. CONTROL DE ACCESO A LA RED

Coordinación de Sistemas y afines

1. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios y éste será permitido mediante un mecanismo de autenticación.

2. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.

3. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoría de seguridad.

4. La Coordinación de Sistemas deberá emplear dispositivos de red para el bloqueo, enrutamiento o el filtrado de tráfico, evitando el acceso o flujo de información no autorizada hacia la red interna o desde la red interna hacia el exterior.

5. Los accesos a la red interna o local desde una red externa de CORPECOL, se harán mediante un mecanismo de autenticación seguro y el tráfico entre ambas redes o sistemas, será cifrado con una encriptación de 128 bits.

6. Se registrará todo acceso a los dispositivos de red, mediante archivos de registro o log, de los dispositivos que provean estos accesos.

7. Se efectuará una revisión de log de los dispositivos de acceso a la red en un tiempo máximo de 48 horas.

2.1.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO

1. Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, entre otros) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.

2. Al terminar una sesión de trabajo en las estaciones, el usuario, evitará dejar encendido el equipo, pudiendo proporcionar un entorno de utilización de la estación de trabajo.

3. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador.

4. Los funcionarios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

5. Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas, en ningún momento se obviarán situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

2.1.6. CONTROL DE ACCESO A LAS APLICACIONES

1. Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso especificas para cada usuario del entorno operativo de la aplicación.

2. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo con el nivel de ejecución o criticidad de las aplicaciones o archivos y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

3. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

4. Las salidas de información, de las aplicaciones, en un entorno de red, deberán ser documentadas y especificar la terminal por la que deberá ejecutarse exclusivamente la salida de información.

5. Se deberá llevar un registro mediante log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

2.1.7. MONITOREO DEL ACCESO Y USO DEL SISTEMA

1. Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de log o bitácoras de sistemas.

2. Los archivos de log, almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

3. Se efectuará una copia automática de los archivos de log y se conducirá o enviará hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

2.2. GESTIÓN DE OPERACIONES Y COMUNICACIONES

2.2.1. RESPONSABILIDADES Y PROCEDIMIENTOS OPERATIVOS

1. El personal administrador de algún servicio, es el responsable absoluto por mantener en óptimo funcionamiento ese servicio, apoyarse con el Coordinador de Sistemas, para fomentar una cultura de administración segura y servicios óptimos.

2. Las configuraciones y puesta en marcha de servicios, son regladas por la Coordinación de Sistemas.

3. El personal responsable de los servicios, llevará archivos de registro de fallas de seguridad del sistema, revisará, estos archivos de forma frecuente y en especial después de ocurrida una falla.

2.2.2. PLANIFICACIÓN Y ACEPTACIÓN DE SISTEMAS

1. La Coordinación de Sistemas o personal de la misma, efectuará todo el proceso propio de la planificación, desarrollo, adquisición, comparación y adaptación del software necesario para CORPECOL, teniendo en cuenta su Plan Estratégico de Tecnología de la Información “PETI”.

2. La aceptación del software se hará efectiva por la Gerencia CORPECOL, previo análisis y pruebas efectuadas por el personal de sistemas.

3. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado de sistemas.

4. La aceptación y uso de los sistemas no exonera, de responsabilidad alguna al Coordinador de Sistemas, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

5. El software diseñado localmente (desarrollado por programadores internos), deberán ser analizados y aprobados, por el Coordinador de Sistemas o a quien el designe, antes de su implementación.

6. Es tarea de programadores o personas que realicen esta tarea, el realizar pruebas de validación de entradas, en cuanto a:

- Valores fuera de rango.
- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores.
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.
- Procedimientos operativos para validación e integridad de las salidas.

7. Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

8. Cualquier prueba sobre los sistemas, del ámbito a la que esta se refiera deberá ser documentada y cualquier documento o archivo que haya sido necesario para su ejecución deberá ser borrado de los dispositivos físicos, mediante tratamiento electrónico.

2.2.3. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

1. Se adquirirá y utilizará software únicamente de fuentes confiables.

2. En caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

3. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

2.2.4. MANTENIMIENTO

1. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal de la Coordinación de Sistemas o del personal de soporte técnico.

2. El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el Coordinador de Sistemas.

3. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

2.2.5. MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

1. Los medios de almacenamiento o copias de seguridad del sistema de archivos o información de CORPECOL, serán etiquetados de acuerdo con la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

2. Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

3. Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial a la cual tendrá acceso únicamente la Gerencia y/o a quien ella delegue, esta caja no debería ser removible; para futuros manejos se recomienda tener una copia adicional que será resguardada por un tercero, entidad financiera o afín.

4. Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

3. SEGURIDAD FÍSICA

3.1. SEGURIDAD FÍSICA Y AMBIENTAL

3.1.1. SEGURIDAD DE LOS EQUIPOS

1. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

2. Los servidores, sin importar al grupo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

3. Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el Coordinador de Sistemas y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

3.1.2. CONTROLES GENERALES

1. Las estaciones o terminales de trabajo, con procesamientos críticos no deben contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.

2. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

3. Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los equipos.

4. Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para salvaguardar los recursos tecnológicos y la información.

5. Toda visita a las oficinas de tratamiento de datos críticos e información (sala de servidores o similar) deberá ser debidamente analizada y supervisada por el Coordinador de Sistemas, previa autorización por parte de la Gerencia.

6. La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas de la Coordinación de Sistemas o cualquier otra, mediante una división, en lo posible, recubierta de material aislante o protegido contra el fuego. Esta sala deberá ser utilizada únicamente por las estaciones prestadoras de servicios y/o dispositivos a fines.

7. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto, el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

8. El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.

9. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

10. Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.

SEGURIDAD LEGAL

4.1. CONFORMIDAD CON LA LEGISLACIÓN

4.1.1. CUMPLIMIENTO DE REQUISITOS LEGALES

Licenciamiento de Software:

1. CORPECOL, se reserva el derecho de respaldo, a cualquier miembro, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

2. Todo el software comercial que utilice CORPECOL, deberá estar legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias.

3. La adquisición de software por parte de personal que labore en CORPECOL, no expresa el consentimiento del fondo de empleado, la instalación del mismo, no garantiza responsabilidad alguna para CORPECOL, por ende el fondo de empleado no se hace responsable de las actividades de sus funcionarios.

4. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, CORPECOL respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.

5. El software comercial licenciado a CORPECOL, es propiedad exclusiva de CORPECOL, la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

6. En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para su efecto y se acatarán las medidas de licenciamiento relacionadas con la propiedad intelectual.

7. Las responsabilidades inherentes al licenciamiento de software libre son responsabilidad absoluta de CORPECOL.

8. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y basado en las disposiciones de la respectiva licencia.

9. El software desarrollado internamente, por el personal que labora en CORPECOL es propiedad exclusiva del mismo.

10. La adquisición del software libre o comercial deberá ser gestionada con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.

11. Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar, las medidas necesarias de seguridad, nivel de prestación del servicio y/o el personal involucrado en tal proceso.

4.1.2. REVISIÓN DE POLÍTICAS DE SEGURIDAD Y CUMPLIMIENTO TÉCNICO

1. Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en la violación.

2. El documento de seguridad será elaborado y actualizado por el Coordinador de Sistemas, pero su aprobación y puesta en ejecución será responsabilidad de la Gerencia.

3. Cualquier violación a la seguridad por parte del personal que labora, para CORPECOL, así como terceros que tengan relación o alguna especie de contrato con CORPECOL se harán acreedores a sanciones aplicables de ley.

4.1.3. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS

1. Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red, trimestral, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto personal capacitado en el área de seguridad.

2. Toda auditoria a los sistemas, estará debidamente aprobada por la Gerencia.

3. Cualquier acción que amerite la ejecución de una auditoría a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos, así como razones para su ejecución, personal involucrado y los sistemas implicados.

4. La auditoría no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados, en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

5. Las herramientas utilizadas para la auditoría deberán estar separadas de los sistemas de producción y en ningún momento estas se quedaran al alcance de personal ajeno a la elaboración de la misma.

JULIO ERNESTO HERRERA ORJUELA
Gerente / (Representante Legal)