1. PROPÓSITO

Establecer y orientar las prácticas y métodos más adecuados que permita mantener un nivel confiable de Seguridad Informática y el uso responsable de los recursos tecnológicos. Con el fin de garantizar la continuidad de la operación.

2. ALCANCE

Aplica para los sistemas de información y telecomunicaciones; incluyendo las actividades de generación, distribución, almacenamiento, uso, recuperación, mantenimiento y disponibilidad de la información. Además la administración de los proveedores de productos y servicios.

3. COMENTARIOS Y ACLARACIONES

Las políticas de seguridad en informática de la empresa emergen como el instrumento para concientizar a sus empleados dentro de la compañía, acerca de la importancia y responsabilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permita la continuidad del negocio.

DEFINICIONES

Software: Se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware.

Hardware: Corresponde a todas las partes tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado; contrariamente, el soporte lógico es intangible y es llamado software.

- **Seguridad informática:** es el conjunto de reglas, planes y acciones que permiten asegurar la información contenida en un sistema computacional.

- **Política de seguridad informática (PSI):** Son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de daño sobre: los computadores de sus sistemas y los elementos físicos empleados con éstos (instalaciones, impresoras, discos, cables, dispositivos de interconexión, entre otros), el software y la información almacenada en tales sistemas y los usuarios del sistema.

- **Sistema de información:** Es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Está conformado por:

  - ✓ *El equipo computacional:* el hardware necesario para que el sistema de información pueda operar.
  - ✓ El recurso humano que interactúa con el Sistema de Información, el cual está formado por las personas que utilizan el sistema.

- **Recurso Informático:** Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y telecomunicaciones) que facilitan servicios informáticos.

- **Información:** Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes o expuesta en una conversación. Cualquiera sea la forma que adquiere la información o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

- **Usuarios Terceros:** Todas aquellas personas naturales o jurídicas, que no son empleados directos, pero que por las actividades que realizan en la empresa, deban tener acceso a Recursos informáticos.

- **Ataque cibernético:** intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

- **Directorio Activo: Active Directory** (**AD**) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos(principalmente LDAP, DNS, DHCP, Kerberos...).

  Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

4. ETAPAS DEL PROCESO

La empresa, para la administración de la seguridad de la información y la comunicación, definió los siguientes parámetros:

1. Equipo administrador de TIC en Covitec (Describir la responsabilidad de cada integrante frente a TIC)
2. Infraestructura.
3. Inventario de las herramientas informáticas- Software
4. Inventario de los equipos – Hardware
5. Seguridad de la información. (Backup, archivos físicos).
6. Actualización de los software.
7. Definir planes de mantenimiento Preventivo para los software y los hardware.
8. Planes de contingencia.
9. Reporte de daños de TIC.
10. Administración de reportes de servicios.
11. Acuerdos de confidencialidad (clientes internos = Empleados, podría ser en el contrato de trabajo y el cliente externo en el contrato que se realiza.)
12. Acuerdo de servicios (Administración del contrato).
13. Capacitación en TIC (capacitaciones puntuales frente a un nuevo software o hardware, capacitación al personal nuevo que tenga como herramienta de trabajo software o hardware.
14. Planes tácticos de innovación

1) Área de soporte TIC en Covitec conformado por:

Coordinador de las TICs: Responsable de velar por el cumplimiento de los objetivos estratégicos (disponibilidad de la información- continuidad del negocio e innovación tecnológica. Así como el control, seguimiento e implementación de acciones de mejora al proceso.

Practicante: Apoyo al coordinador de TICs para la atención de requerimientos en el tiempo estipulado , mttos preventivo y correctivo de HW Y SW y control de las políticas de seguridad de la información implementadas por la compañía.

2) INFRAESTRUCTURA:

Se cuenta con 4 centros de cableado estructurado distribuidos asi:

- un cuarto tecnico central en el 3 piso de la nueva sede dotado con un rack cerrado donde están instalados los equipos activos(suiches, routers, planta telefónica, servidor ppal de datos) de donde se distribuye todo el cableado para voz y datos en categoría 6A para los 6 pisos de la nueva sede.

- Un centro de cableado en gabinete de pared, ubicado en el 2 piso **(Archivo Inactivo)** de la sede de la calle Colombia; dotado con dos suiches de 24 puertos 10/100 y patch panel 24 puertos. De donde se distribuye el cableado estructurado en categoría 5E para los puestos de trabajo del 2 piso de la sede Colombia.

- Un centro de cableado en gabinete de pared, ubicado en el 3 piso de la sede Colombia **(corredor entre depto. Tecnico y central de monitoreo)**, dotado con un suiche de 24 puertos y patch panel de 24 puertos. De donde se distribuye el cableado para el tercer piso de la sede Colombia.

- Un centro de cableado en la central de monitoreo, dotado con un rack abierto y el cual tiene instalados los equipos para el monitoreo de alarmas(surgard, suiche 10/100/1000, PCs, servidor de contingencia, servidor firewall; de donde se distribuye el cableado exclusivo para la central en categoría 6.

- Todos los enlaces están conectados por medio de cable un cable cruzado acogiéndonos al estándar 568A y 568 B. Para el enlace entre el suiche de 48 Ptos 10/100/1000, del cuarto tecnico de la nueva sede y el suiche existen 2 cables como contingencia en cat 6 A.

Se cuenta con tres servidores distribuidos así:

Un servidor ubicado en cuarto tecnico de la nueva sede en el cual está alojada toda la información de todos los usuarios y las areas, el sistema contable y el controlador de dominio.

Otro servidor que se encuentra ubicado en la central de monitoreo en la sede de la calle Colombia, custodiado en cuarto cerrado en donde está alojado el S.O del fondo de empleados y se tiene replicado el controlador de dominio.

3) **Inventario de las herramientas informáticas- Software**

La empresa tiene actualizada esta información mediante registro **Ver RTI02** Inventario de Herramientas de TIC – Software. Unidad k:/sistemas de gestión /TICs/formatos/rti02.

4) Inventario de los equipos – hardware

La empresa tiene actualizada esta información mediante el registro **Ver RTI05** – Hojas de vida equipos de cómputo. K: /Sistemas de gestión /TICs /Hojas de vida equipos de cómputo/RTI05.

.

5) Seguridad de la información

La empresa tiene estipuladas las siguientes políticas de seguridad de la información:

- En los equipos de cómputo de la empresa está prohibido instalar por el usuario programas no autorizados como por ejemplo juegos online, programas de descarga de software, música, videos, instalación de programas de mensajería o chats diferentes al interno (Comunication Assistant), acceso a páginas prohibidas (sexo, facebook, you tube, redes sociales, etc), instalación de antivirus diferentes al autorizado (Kaspersky).

- Periódicamente está programado el cambio de claves personales de cada equipo de computo, cada 180 días. Estos cambios se deben reportar al coordinador de TICs, para su actualización y custodia.

- Es prohibido enviar cadenas de correo electrónico, spam o correos con archivos pesados, ya que esto atenta contra el rendimiento del canal de comunicaciones, cualquier correo sospechoso, debe eliminarlo inmediatamente o informar al área de soporte, para proceder adecuadamente contra situaciones que puedan afectar el equipo asignado.

- Se tiene una solución de antivirus **(Kaspersky versión 6.0 y 8.2**) el cual está instalado en cada equipo y programado para ejecutarse automáticamente en cada equipo de computo o manualmente por el usuario. Este antivirus puede ser administrado desde una consola central instalada en el equipo del coordinador de TICs.

- COVITEC Ltda. tiene restricción a las páginas de internet por medio del firewall y solo están autorizadas aquellas páginas de consulta para nuestras actividades diarias como: Supervigilancia, Procuraduría, Contraloría, Cámara de Comercio entre otras.

- Se tiene la unidad de red pública K:/ destinada para el almacenamiento de carpetas para cada area las cuales solo tienen permisos para el personal autorizado.

- Se tiene la unidad de red x:/ destinada para el almacenamiento de las carpetas personales de cada usuario, a las cuales se les realiza el backup diariamente de lunes a sabado por parte del proveedor de servicios SIMA TECNOLOGIA.

- La información de SGC está almacenado en la unidad W:/ a la cual solo tiene acceso la dirección de calidad con su usuario y contraseña.

- Cuando un empleado nuevo ingresa a la compañía se le informa y se le hace entrega del documento **RTI03** políticas internas de control y seguridad de la información, el cual debe ser firmado comprometiéndose a cumplirlas del cual se deja copia en la hoja de vida.

6) Actualización de software.

Se tienen programadas las actualizaciones automáticas en los equipos con los cuales se ha empezado el proceso de legalización bajo Windows 7.

En el contrato con cada proveedor de servicios se tiene el compromiso entre las partes para la información oportuna de recomendaciones e instalación de actualizaciones de los diferentes software contratados.

En el caso del antivirus se tiene programado automáticamente la actualización diaria en busca de bases de datos actualizadas.(Solución Kaspersky).

7). Planes de mantenimiento Preventivo

Se cuenta con un cronograma de mttos preventivos anuales, dándole cubrimiento a todos los equipos tecnológicos de la compañía incluyendo la sede de cali.

Se tienen programados tres mantenimientos preventivos en el año para el hardware que incluye (Equipos de cómputo, y equipos activos de la red de datos).Esta labor está siendo realizada por el practicante.

Dentro del contrato con el proveedor de servicios SIMA tecnología se tiene estipulado mantenimiento preventivo 2 veces al año a las impresoras y los servidores de internet y datos y 3 veces al año del software, el cual incluye (borrar los archivos temporales, se desfragmentan las unidades de disco, se corre el antivirus, se borran archivos que el usuario no necesite y autorice al área de TICs para borrarlos.

Para el software de monitoreo de alarmas SIMS II se tiene un contrato de mantenimiento preventivo y correctivo vigente por un año en horario de lunes a viernes de 08:00 a 17:00, con el proveedor de servicios SIMS WARE realizado remotamente .

8) Planes de contingencia.

Se realiza un backup diario de la información de lunes a sábado programado a las 23:00(sistema contable **(SIESA)** y herramienta ofimática en un disco externo que permanece conectado al servidor de datos basado en el S.O en Windows server 2003 en el cuarto tecnico de la central de monitoreo, realizado remotamente por el proveedor de servicios actual SIMA tecnología.

Se tiene como respaldo otro disco duro externo en el servidor del cuarto.Tecnico de la nueva sede conectado al servidor de datos basado en Windows server 2008.

Se tiene garantizado el servicio de internet con dos canales a 6 Mb uno por F.O que tiene su acceso por la calle 49 y otro canal en cobre por la calles Colombia y donde el CPE está ubicado en el centro de cableado del 3 piso de la sede Colombia. Adicionalmente se tiene cobertura con el WIFI por medio de un AP y Router Inalámbrico para toda el área administrativa. Bajo el protocolo 802.11 G y con seguridad wep personal.

Se cuenta con una réplica del AD (directorio activo) entre el servidor de datos ubicado en la nueva sede con S.O Windows server y servidor ubicado en la sede de la calle Colombia con S.O Windows server 2003.

También se realizan dos backup del software de monitoreo de alarmas SIMS II, todos los días programado automáticamente, por medio de la herramienta backup4 profesional. Esté es verificado por el coordinador de TICs semanalmente. Del cual llega un correo de confirmación de que se realizó con éxito o con errores.

Se tiene como contingencia un equipo espejo del primario donde se recepcionan las señales de alarmas por si llegara a fallar el principal.

Se tiene implementada una central de contingencia en otro lugar del área metropolitana designado por la gerencia. Dotada con los equipos tecnológicos y líneas telefónicas necesarios con lo que se podría seguir la operación de llegarse a presentar una situación catastrófica en la sede principal.

Sistema Eléctrico:

Como sistema de contingencia se cuenta con UPS de 10 kva para la nueva sede, la cual nos puede dar un respaldo de 30 minutos suficientes para que en caso de irse el fluido eléctrico tenga el tiempo para guardar cambios en los archivos y apagar los equipos

Para la central de monitoreo se tienes una UPS dedicada exclusivamente para la central de 6 KVA y según prueba realizada nos da un respaldo de 24 horas debido a que tiene un banco de baterías de 55 Amph por cada batería y son 10 Kva.

Para los pocos equipos de la sede de la calle Colombia se cuenta con una UPS de 6 Kva la cual nos da un respaldo de 20 Min.

9). Reporte de fallas o nuevos servicios TICs

- Al usuario presentársele una dificultad relacionada con hardware o software, agotara el recurso tratando de solucionarla por si mismo si esta a su alcance.

- De no poder darle solución, el usuario diligencia la novedad atraves del reporte de servicios RTI01, inmerso dentro del formato integral de requerimientos **(PIR),** haciendo una breve descripción de la falla y recurso agotado. Este reporte se encuentra en la unidad K:/sistemas de gestión/requerimientos/Nuevo formato. Será enviado vía E-mail dirigido al área de TICs al correo requerimientos@covitec.com.co

- El area de TICs (Coordinador de TICs y practicante, lo recepcionan y lo clasifican según la prioridad, dependiendo de la afectación a la operación de la empresa. Según el siguiente rango.

    - **Prioridad Alta** (Debe atenderse en un tiempo no >= a 1 hora.
    - **Prioridad media** (Debe atenderse en un tiempo no >= a un día hábil.
    - **Prioridad baja** (Debe atenderse en un tiempo no >= a 3 días hábiles.
    - **Sujeto a compras** (Debe atenderse en un tiempo no >= a 10 días hábiles.

- Posteriormente, el área de soporte realiza un diagnostico y de poder darle solución cierra el reporte, de no poderlo realizar se escala al proveedor que le competa la reparación. Cuando se de solución se cierra el reporte adjuntando toda las observaciones que se pudieran generar en el proceso de reparación y posibles acciones para que nose vuelva a presentar la falla.

10). Administración del reporte de servicios:

Se tienen tabulados los reportes de servicios RTI01 los cuales nos dan una tendencia del reporte del daño más frecuente, persona que lo reporta, causa, tiempo de respuesta y posible solución. Con lo que podemos realizar acciones de mejora al sistema para tratar de minimizar las posibles falencias.

De estos requerimientos se lleva un indicador de número de requerimientos mes/ nro de requerimientos atendidos en el tiempo estipulado. Al cual se le realiza mes a mes análisis de causas y seguimiento plasmado en el SGC. **K:/ Sistema de Gestion/indicadores/cuadro de mando**

11). Acuerdos de confidencialidad de la información

En los contratos con los diferentes proveedores de servicios se anexa la siguiente clausula:

1. **CLAUSULA– CONFIDENCIALIDAD – EL CONTRATISTA** se obliga a que toda información que a partir de la fecha reciba de los funcionarios de EL CONTRATANTE, de manera directa o indirecta, en forma verbal, escrita, gráfica, en medio magnético o bajo cualquier otra forma, que no sea pública, (que en adelante se denominará la "información"), sea mantenida en forma estrictamente confidencial. En consecuencia, EL CONTRATISTA tomará todas las medidas necesarias para que la información no llegue a manos de terceros bajo ninguna circunstancia y se obliga a no utilizarla para ningún objeto diferente al de adelantar las tareas que se deriven directamente del cumplimiento del presente contrato. Adicionalmente, EL CONTRATISTA se obliga a devolver toda la información, tan pronto como termine la labor encomendada, en el momento en que EL CONTRATANTE lo solicite.

2. En el formato RTI03 (Políticas internas de control y seguridad de la información) se tiene la siguiente cláusula de confidencialidad con los empleados:

   CLAUSULA– CONFIDENCIALIDAD – EL EMPLEADO se obliga a que toda información que a partir de la fecha de su vinculación reciba de LA EMPRESA para el desempeño de sus labores, de manera directa o indirecta, en forma verbal, escrita, gráfica, en medio magnético o bajo cualquier otra forma, que no sea pública, sea mantenida en forma estrictamente confidencial. En consecuencia, EL EMPLEADO tomará todas las medidas de precaución necesarias para que la información no llegue a manos indebidas bajo ninguna circunstancia y se obliga a no utilizarla para ningún objeto diferente al de adelantar las tareas que se deriven directamente del cumplimiento de su cargo. Adicionalmente, EL EMPLEADO se obliga a devolver toda la información, tan pronto como cese su contrato laboral con la empresa.

Los empleados tienen los siguientes deberes:

- Los usuarios no deberán suministrar información confidencial y privada de la empresa a ningún ente externo sin las autorizaciones respectivas.

- Los usuarios no deben destruir, copiar o distribuir los archivos de la empresa sin los permisos respectivos.

- Los usuarios que utilicen los recursos de los sistemas de la empresa, tiene la responsabilidad de velar por la integridad, confidencialidad y disponibilidad de la información que manejen, especialmente si dicha información ha sido clasificada como datos sensible.

12.) Acuerdo de servicios (administración del contrato)

En los contratos con los proveedores de servicio sea software o hardware se tiene estipulados una seria de acuerdos que son necesarios en el proceso de TIC como son:

- Se debe especificar un plan de mantenimientos preventivos y correctivos si le aplica al servicio por el tiempo en que se tenga el contrato.
- Informe de actualizaciones tanto de software como hardware.
- Ficha técnica de todos los equipos y software.
- Acuerdos de confidencialidad de la información.
- Recomendaciones y planes de mejora.
- Programa de capacitaciones durante el tiempo que dure el contrato

13.) Capacitaciones en TIC

Se tienen programadas una serie de capacitaciones anuales con el fin de dar a entender a todos los empleados de nuestra compañía el objetivo de TIC, seguridad de la información y minimizar fallos por malas prácticas. (De la cual se deja acta con registro de asistencia)

.

14) Planes tácticos

Se tienen a cargo planes tácticos como objetivo estrategico con los cuales se tiene como objetivo modernizar, mejorar y agilizar la productividad de los procesos. Por medio de desarrollo de nuevos SW a la medida y actualización de otras herramientas.

Del cual se lleva medición de indicadores en el cuadro de mando del SGC. **K:/Sistema de gestión/indicadores/cuadro de mando.**

ELABORO	**APROBO:**
CESAR AUGUSTO BOTERO AGUIRRE **Coordinador TICs**	**CARLOS ARTURO GRISALES CARMONA** **Presidente**