RESUMEN – TRABAJO DE GRADO

AUTORES	GUSTAVO CASTILLA VERGEL, GISELLE ECHAVEZ CASADIEGOS, JUAN CARLOS RODRIGUEZ OSORIO, DIANA MARCELA SANDOVAL SANJUAN
FACULTAD	INGENIERÍAS
PLAN DE ESTUDIOS	ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
DIRECTOR	MSc (C). ANDRÉS MAURICIO PUENTES VELÁSQUEZ
TÍTULO DE LA TESIS	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA OFICINA DE CONTROL Y VIGILANCIA EN LA CORPORACION AUTONOMA DE LA FRONTERA NORORIENTAL "CORPONOR" TERRITORIAL OCAÑA

RESUMEN

(70 palabras aproximadamente)

SE PROPONE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA OFICINA DE CONTROL Y VIGILANCIA DE CORPONOR TERRITORIAL OCAÑA; ESTA PROPUESTA TIENE COMO FIN APORTAR A LA CORPORACIÓN A AUMENTAR LA CANTIDAD Y CALIDAD DE LOS CONTROLES INFORMÁTICOS, A DETECTAR LOS NIVELES DE MADUREZ TANTO DE LAS CARACTERÍSTICAS FÍSICAS COMO LÓGICAS QUE DAN SOPORTE AL PROCESO Y ALMACENAMIENTO DE LA INFORMACIÓN, A DEJAR SENTADOS LOS ELEMENTOS CONCEPTUALES Y TEÓRICOS QUE LES PERMITIRÁN A LAS PERSONAS QUE ALLÍ TRABAJAN TOMAR LAS DECISIONES ADECUADAS PARA UTILIZAR ADECUADAMENTE LA TECNOLOGÍA Y CONTRIBUIR A DISMINUIR LOS NIVELES DE INSEGURIDAD DE LA INFORMACIÓN DE LA ORGANIZACIÓN.

CARACTERÍSTICAS

PÁGINAS: 92	PLANOS: 0	ILUSTRACIONES: 0	CD-ROM: 1

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA OFICINA DE CONTROL Y VIGILANCIA EN LA CORPORACION AUTONOMA DE LA FRONTERA NORORIENTAL "CORPONOR" TERRITORIAL OCAÑA

GUSTAVO CASTILLA VERGEL
GISELLE ECHAVEZ CASADIEGOS
JUAN CARLOS RODRIGUEZ OSORIO
DIANA MARCELA SANDOVAL SANJUAN

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA
2014

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA OFICINA DE CONTROL Y VIGILANCIA EN LA CORPORACION AUTONOMA DE LA FRONTERA NORORIENTAL "CORPONOR" TERRITORIAL OCAÑA

Proyecto desarrollado como requisito para optar el título de Especialista en Auditoría de Sistemas

GUSTAVO CASTILLA VERGEL
GISELLE ECHAVEZ CASADIEGOS
JUAN CARLOS RODRIGUEZ OSORIO
DIANA MARCELA SANDOVAL SANJUAN

IS. Esp. MSc(c) ANDRÉS MAURICIO PUENTES VELÁSQUEZ
DIRECTOR

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS
OCAÑA

2014

TABLA DE CONTENIDO

TABLAS

FIGURAS

INTRODUCCIÓN

La información constituye el activo más importante en las organizaciones, ya sean públicas o privadas; teniendo en cuenta esta premisa, es fundamental que se realicen investigaciones que busquen aportar en la preservación de las características básicas de la misma: confidencialidad, disponibilidad e integridad. Nunca se ha tenido más conciencia de la importancia de preservar estas características en la información como ahora, y es en gran medida, por el alto grado de conciencia que se tiene sobre la posibilidad latente de que dicha información de las organizaciones se vea afectada por amenazas externas que vengan a aprovecharse de las vulnerabilidades que presente la infraestructura tecnológica de las organizaciones.

En el presente documento se plantea una propuesta de Sistema de Gestión de Seguridad de la Información para la oficina de control y vigilancia de CORPONOR territorial Ocaña; esta propuesta tiene como fin aportar a la corporación a aumentar la cantidad y calidad de los controles informáticos, a detectar los niveles de madurez tanto de las características físicas como lógicas que dan soporte al proceso y almacenamiento de la información, a dejar sentados los elementos conceptuales y teóricos que les permitirán a las personas que allí trabajan tomar las decisiones adecuadas para utilizar adecuadamente la tecnología y contribuir a disminuir los niveles de inseguridad de la información de la organización.

En las diferentes secciones del presente proyecto se presentan los elementos que sustentan la importancia y las fases para llevar a cabo la propuesta (capítulo uno), después se sientan las bases teóricas, conceptuales, históricas, legales y contextuales que dan soporte a la propuesta (capítulo dos), a continuación se plantea la estrategia metodológica que se ha estado empleando para dar solución al problema de investigación (capítulo tres), se demuestra la consecución exitosa de los objetivos planteados a través de la presentación de resultados (capítulo cuatro), finalmente se expresan las conclusiones posteriores a la elaboración del trabajo investigativo que tuvo como resultado el Sistema de gestión de Seguridad de la Información para CORPONOR territorial Ocaña.

1. SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA OFICINA DE CONTROL Y VIGILANCIA EN LA CORPORACION AUTONOMA DE LA FRONTERA NORORIENTAL "CORPONOR" TERRITORIAL OCAÑA

1.1 PLANTEAMIENTO DEL PROBLEMA

En la dirección territorial Ocaña de la Corporación Autónoma de la frontera Nororiental (CORPONOR) se cuenta con una serie de elementos de infraestructura tecnológica que dan soporte al procesamiento de información (hardware y software); con el paso del tiempo, estos elementos de hardware y de software van cambiando con el fin de mejorar tecnológicamente sin tener en cuenta la necesidad de acompañar este proceso de cambio de una adecuada gestión de la seguridad de la información.

En la territorial Ocaña de la Corporación, y específicamente en la oficina de control y vigilancia no existe un sistema de gestión de seguridad de la información; allí se están llevando a cabo actividades para estructurar y consolidar los sistemas de gestión de la calidad, medio ambiente y salud y seguridad laboral, sin embargo, todavía no se ha definido una política eficaz en la implementación de la gobernabilidad de TI, sistema de soporte de seguridad de la información, sistematización de procesos misionales y copias de respaldo. Por estas razones, se encuentra una brecha en cuanto al manejo adecuado que debe hacerse de la seguridad de la información con el fin de otorgar unos niveles de protección de los activos relacionados con el almacenamiento y procesamiento de los datos, para evitar que se materialicen las diferentes amenazas.

1.2 FORMULACIÓN DEL PROBLEMA

¿Un Sistema de Gestión de Seguridad de la Información para la oficina de Control y Vigilancia de CORPONOR Ocaña, constituirá un instrumento que permita efectivamente gestionar y mitigar al máximo los riesgos asociados al procesamiento y almacenamiento de la información?

1.3 OBJETIVOS DE INVESTIGACIÓN

1.3.1 General

Diseñar un sistema de gestión de seguridad de la información para la oficina de control y vigilancia en la corporación autónoma de la frontera nororiental "CORPONOR" territorial Ocaña.

1.3.2 Específicos

- Elaborar un estudio para diagnosticar los elementos del proceso de control y vigilancia que se desarrolla en la territorial de Ocaña con el fin de identificar riesgos de TI/SI.

- Identificar los elementos que conforman el SGSI – Sistema de Gestión de Seguridad de la Información para la oficina de control y vigilancia en la corporación.

- Documentar formalmente las actividades y políticas requeridas para gestionar adecuadamente la seguridad de la información en la oficina de control y vigilancia en la corporación.

1.4 JUSTIFICACIÓN

Teniendo presente los avances tecnológicos con los que se cuentan hoy en día es acertado que CORPONOR Territorial Ocaña cuente con las tecnologías a la vanguardia de la seguridad de la información para lograr enfrentarse a los mercados competitivos que existen y que avanzan cada vez más a pasos agigantados. El contar con un grupo de Políticas aprobadas por el Directorio se reconocería como un paso principal para brindar dirección y alineamiento de los distintos actores, brindando legitimidad al equipo de Seguridad para dirigir los temas de Seguridad de la Información en la corporación.

La corporación autónoma de la frontera nororiental "CORPONOR" territorial Ocaña cuenta con unos procesos misionales que son la base y la misión de la corporación como la principal empresa y de referencia obligatoria en cuanto al medio ambiente se refiere en todo el Norte de Santander, por esto es necesario contar con un soporte efectivo para administrar la seguridad de la información que además de brindar facilidad y agilidad en estos procesos misionales, logre posicionar a la corporación como un sólido grupo de trabajo tecnológico que acata la normatividad nacional e internacional en cuanto a Seguridad de la Información.

1.5 HIPÓTESIS

Un Documento donde se formule la planeación del Sistema de Gestión de Seguridad de la Información ajustado a las necesidades específicas de la oficina de Control y Vigilancia de CORPONOR Ocaña, será considerado como un instrumento que permita efectivamente gestionar y mitigar al máximo los riesgos asociados al procesamiento y almacenamiento de la información; contribuyendo al soporte informático adecuado para el cumplimiento de los objetivos misionales.

1.6 DELIMITACIONES

Delimitación Geográfica: Oficinas de la Corporación Autónoma de la Frontera Nororiental ¨CORPONOR¨ territorial Ocaña.

Delimitación Conceptual: Los conceptos que se van a manejar en este proyecto se relacionan con la Seguridad Informática, Sistema de Gestión de Seguridad de la Información (SGSI), Políticas de Seguridad de la Información, Gestión de Riesgos.

Delimitación Temporal: El periodo de realización del estudio será de cinco meses a partir de la aprobación del proyecto

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

En la última década la preocupación por la seguridad de la información se ha tornado relevante para las organizaciones por el alto valor que tiene la información como activo, sin embargo, no ha sido algo del último tiempo solamente, el analista Luis Montenegro hace el siguiente análisis histórico de la seguridad de la información: "¿Y de donde nació este interés por la seguridad de la información? Para poder responder a esta pregunta, debemos mirar hacia atrás en la historia y analizar la evolución que ha sufrido el tratamiento de la información. Antes de la aparición de las primeras redes de computadores, prácticamente toda la información sensible de una organización se guardaba en un formato físico: Bodegas repletas de grandes archivadores y toneladas de papeles eran los encargados de guardar los datos de los clientes y la contabilidad de una empresa. Las principales amenazas a la seguridad de dicha información se podían encontrar en desastres naturales, y el robo de información era algo bastante más complejo que ahora (no cualquiera podía salir disimuladamente con los datos de 5000 clientes de una empresa). Pero con la aparición de la computación y el auge de las redes, la información comenzó a digitalizarse de una manera impresionante, y una bodega llena de archivadores con datos de una cartera de clientes ahora podía resumirse al contenido de un disco duro de un equipo que podría ocupar menos de un metro cuadrado de superficie. Este avance en la tecnología, aparte de las múltiples ventajas en el procesamiento y análisis de la información, trajo consigo un nuevo problema al mundo de la informática: La información en formato digital, es más fácil de transportar, por lo que las posibilidades de hurtarla o alterarla no son despreciables."

La seguridad de la información toma especial relevancia en el año 1980 en donde se fundamentan las bases de la seguridad de la información, en este año, James P. Anderson escribe un documento titulado 'Computer Security Threat Monitoring and Surveillance'. Lo más interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas.

En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término "virus" para describir un programa informático que se reproduce a sí mismo, en el año 1985 aparecieron los primeros Troyanos (caballo de Troya), escondidos como un programa de mejora de gráficos llamado EGABTR y un juego llamado NUKE-LA, en 1987 hace su aparición el virus Jerusalén o Viernes 13, que era

capaz de infectar archivos .EXE y .COM. Su primera aparición fue reportada desde la Universidad Hebrea de Jerusalén y ha llegado a ser uno de los virus más famosos de la historia. Robert Thomas Morris, el 3 de noviembre de 1988, equipos como VAX y SUN conectados al Internet se vieron afectados en su rendimiento y posteriormente se paralizaron. Se vieron afectados Bancos, Universidades e instituciones de gobierno, la causa fue un GUSANO, desarrollado por Morris, recién graduado en '*Computer Science*' en la Universidad de Cornell, en el año de 1994 se contempla la regulación de los virus (*computer contaminant*) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos. Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Fue durante el año 2004 cuando se informó de la existencia del primer código malicioso para plataformas móviles. Recordando el DISI 2006. A fondo: amenazas y vulnerabilidades Bajo este lema se celebró el Primer Día Internacional de Seguridad de la Información, que tuvo lugar en noviembre de 2006 en la Escuela Universitaria de Ingeniería Técnica de Telecomunicación EUITT de la Universidad Politécnica de Madrid, SEGURINFO Colombia 2011 XVI Congreso Interamericano de Seguridad de la Información El encuentro se realizó con el objetivo de informar y discutir sobre temas de actualidad en la materia para sustentar las decisiones gerenciales en el ámbito de la Seguridad en la Información.

La seguridad de la información es un tema que desde hace tiempo se ha puesto muy de moda, pero no solo por moda si no que en la actualidad es una necesidad prioritaria que toda empresa debe tener establecida por lo menos políticas de seguridad de la información, ya que la información en muchas casos al día de hoy se convierte en un activo mucha importante que el dinero mismo. Ya que la evidencia con la que cuenta un empresa para poder enfrentarse a entidades de control en cuanto a demandas y procesos judiciales se refiere es la información, lo que se encuentra escrito y firmado tiene mucho valor al instante de refutar o afrontar situaciones que tengan que ver con dinero de por medio, por esto los sistemas de gestión de seguridad de la información en la empresas es un costo que se debe asumir con demasiada seriedad y responsabilidad ya que muchas empresas viven de la información de sus clientes para poder sostenerse y para poder tener evidencia y soporte ante cualquier situación que se presente.

Al momento de hablar de la seguridad de la información obligatoriamente debemos tocar temas como los virus informáticos, en ocasiones es complicado saber cómo nos enfrentamos a estos riesgos y cuáles son sus consecuencias, por ejemplo en el tema de los virus informáticos las consecuencias pueden ser la perdida de la información y en algunos

de los casos el daño físico del equipo o suplantación de identidad. Los virus pueden presentarse de muchas maneras los cuales son:

- **Virus de sector de arranque**: aplicado a la información de inicio de los sistemas operativos actuales.
- **Hijacker** (secuestradores de navegador): redirecciona al usuario del navegador a páginas con publicidad.
- **Virus de Acción Directa**: se encuentra en un archivo ejecutable o reside en otro archivo y se activa cuando es ejecutado.
- **Phage Virus o Virus Fago**: Modifica y altera otros programas y bases de datos, infecta todos estos archivos.
- **Virus Polimórfico**: Estos cambian su forma para no ser detectados. Estos tipos de virus atacan el sistema, desplegando un mensaje en la computadora y borrando archivos en el sistema.
- **Retrovirus**: Los retrovirus atacan o eluden el software antivirus instalado en el sistema, pueden atacar directamente el software de antivirus del usuario, potencialmente destruyendo el archivo que contiene las firmas del mismo. Destruir esta información sin el conocimiento del usuario le dejaría al mismo una falsa sensación de seguridad.
- **Worm:** Los worms (gusanos) pueden ser interpretados como un tipo de virus más inteligente que los demás. La principal diferencia entre ellos es la forma de propagación: los worms pueden propagarse rápidamente hacia otros ordenadores, sea por Internet o por medio de una red local. Generalmente, la contaminación ocurre de una manera discreta y el usuario sólo nota el problema cuando el ordenador presenta alguna anormalidad. El worm puede capturar direcciones de e-mail, usar servicios de SMTP (sistema de envío de e-mails) propios o cualquiera otro medio que permita la contaminación de ordenadores (normalmente miles) en poco tiempo.

2.2 MARCO CONTEXTUAL

2.2.1Línea de Investigación: Gobernabilidad de TI. La línea de investigación es la enmarcada en Gobernabilidad de TI, la cual tiene establecido un macro proyecto titulado: "Establecimiento de un marco conceptual de gobernabilidad de TI para las empresas colombianas", el cual se está trabajando para el contexto de Norte de Santander, en su parte inicial la Provincia de Ocaña, por sectores de empresas. Se requiere de la concepción y creación del mencionado marco conceptual, y de la realización de un proceso minucioso de validación del marco propuesto. Para la aplicación del marco conceptual se utiliza una metodología de investigación evaluativa, donde los instrumentos representan un insumo muy importante. Se definen una serie de etapas en el proceso investigativo como son: la

recolección de información, diagnóstico, desarrollo de un plan de mejora y la socialización de resultados.

Durante muchos años la gobernabilidad ha sido vista como el futuro de las tecnologías de la información y la comunicación, a pesar del manejo de diferentes criterios de calidad en gobernabilidad de TI. El proceso de gobernabilidad de una empresa[1]se refiere al conjunto de responsabilidades y prácticas ejecutadas por el comité directivo de la misma, con el objetivo de proveer dirección estratégica a la compañía, asegurando que los objetivos definidos sean alcanzados, verificando que los riesgos sean administrados apropiadamente y que los recursos utilizados sean utilizados responsablemente. La gobernabilidad de TI es parte integral de la gobernabilidad de la empresa, y comprende el liderazgo, las estructuras organizacionales y los procesos que aseguran que la organización de TI sostenga y extienda las estrategias y objetivos de la organización, siendo responsabilidad del comité directivo de la empresa y del comité ejecutivo de TI.

Inspirados en diversos elementos como: el modelo inter-empresa de Santana[2], los conceptos de madurez y los objetivos de control de COBIT[3], se diseñó un marco conceptual de Gobernabilidad de TI[4], donde se identifican los principales componentes de la organización y las maneras en que estos componentes trabajan juntos con el fin de alcanzar los objetivos del negocio. Los componentes o niveles, comprenden procesos de modelado de negocios, arquitectura de SI/TI, Aplicativos de apoyo, y Tecnologías de Información y Comunicación (Ver Figura 1).

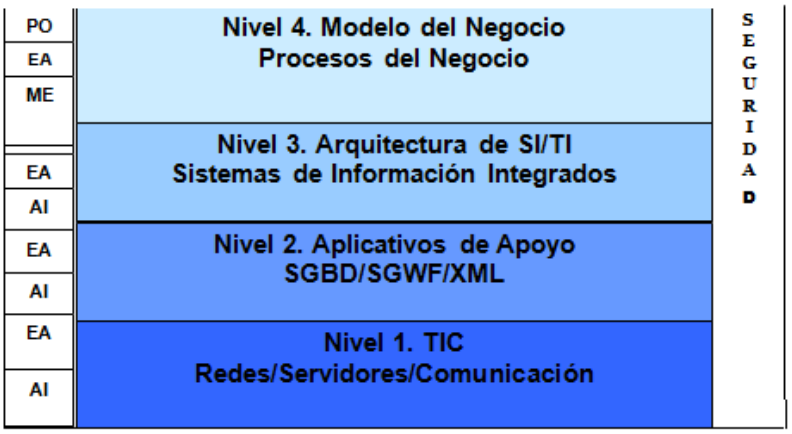
[1] COBIT, GovernanceInstitute Modelo ExecutiveSummary. [Versión electrónica] Extraído el 20 de Diciembre, 2008, desde http://www.isaca.org/cobit.html, 2003.

[2] M. **SANTANA**. *Developing an inter-enterprise alignment maturity model: research challenges and solutions*.Technical Report TR-CTIT-07-29, Centre for Telematics and Information Technology, University of Twente, Enschede.Extraído.

[3]**COBIT 4.0**, *Governance IT*. Extraído el 3 de Enero, 2009 del sitio Web del Institute, Borrad briefingon TI governance:
http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/ContentManagement/ContentDisplay.cfm, 2006.

[4]T, **VELASQUEZ**, Establecimiento De Criterios De Gobernabilidad De TI En Las Empresas Colombianas. Universidad de los Andes. Mérida. Venezuela. 2010.

Figura 1: Marco conceptual de Gobernabilidad de TI:



Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

Nivel 4: Modelado del negocio. Involucra la descripción de la estructura organizacional, procesos de negocios, sistemas de planeación y control, mecanismos de gobierno y administración, políticas y procedimientos de la empresa. Cada uno de estos componentes interactúa y contribuye a alcanzar las metas y objetivos del negocio y provee la base para identificar los requerimientos de los Sistemas de Información (SI) que soportan las actividades del negocio.

Nivel 3: La arquitectura de los sistemas de información. Esta arquitectura provee un modelo para el desarrollo e implementación de aplicaciones individuales, mapas de negocios y requerimientos funcionales de las aplicaciones, y muestra la interrelación entre aplicaciones. Las Aplicaciones Emergentes de Arquitectura están normalmente "orientadas al servicio". Los servicios pueden ser vistos como bloques de construcción que pueden ser ensamblados y re-ensamblados para lograr los cambios en los requerimientos del negocio, en una aproximación que maximice el re-uso y ayude a mantener la flexibilidad en las políticas de servicio para adaptarse a los cambios.

Nivel 2: Aplicativos de apoyo. Son todas las aplicaciones de apoyo a la arquitectura de aplicación como los sistemas de gestión de bases de datos (que ayudan a los procesos básicos de mantenimiento de la base de datos), la administración de los recursos de datos (esto muestra como los recursos de información están siendo administrados y compartidos en beneficio de la empresa). La Arquitectura de Información/Datos incluirá consideraciones de tecnología de almacenaje y administración del conocimiento que faciliten la explotación de la información corporativa, esto incrementará la cobertura y el contenido de la

administración de datos y facilitará el acceso a la información por múltiples canales y otras herramientas como XML y SGWF. Incluye los siguientes procesos dentro de los objetivos de control.

Nivel 1: Tecnología de información y comunicación (TIC). Describe la estructura, funcionalidad y la distribución del hardware, software y los componentes de comunicación que mantienen y soportan la Arquitectura de SI/TI, conjuntamente con los estándares técnicos aplicados a ellos. Estos componentes comprenden toda la "infraestructura de TIC" de la organización. El desarrollo, documentación y mantenimiento de la arquitectura de SI del negocio, debe formar parte del proceso de pensamiento estratégico que se debe desarrollar en la organización. Incluye los siguientes procesos dentro de los objetivos de control.

Se toman de referencia los objetivos del modelo de COBIT para definir las variables del modelo propuesto para las empresas colombianas como son:

- Planificación y Organización PO
- Adquisición e Instrumentos AI
- Entrega y Apoyo DS
- Monitoreo y Evaluación ME

En cada nivel se identifican las variables encontradas de acuerdo a los controles presentes en cada objetivo (Ver Tabla 1).

Tabla 1: Objetivos de Control presentados en cada Nivel

	TIC	Aplicativos de apoyo	Arquitectura de SI/TI	Modelo de Negocio
Planificación y Organización			**X**	**X**
Adquisición e Instrumentos	**X**	**X**	**X**	
Entrega y Apoyo	**X**	**X**	**X**	**X**
Monitoreo y Evaluación			**X**	**X**

Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

Evaluación del Nivel de Madurez. En[5] se muestra un modelo de madurez basado en valores para la alineación de TI en el negocio llamado el VITALMM, el cual cubre todos los sistemas de información que en la organización se empleen, en colaboraciones de inter-empresa, así como la infraestructura tecnológica y las facilidades de soporte necesarios para ellos, identificando valores para la alineación de TI en el negocio se toma como referencia la clasificación de 0 – Inexistente, 1 – Inicial, 2 – Repetible, 3 – Definido, 4 – Manejado y 5- Optimizado.

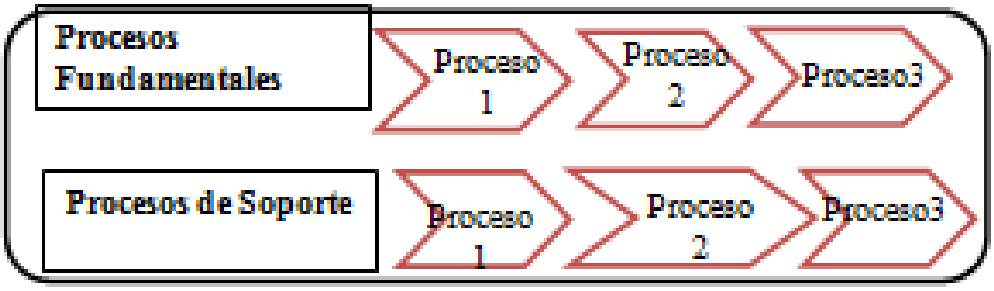
Se elabora una guía para la aplicación del modelo conceptual en la que se define: El reconocimiento del marco conceptual de gobernabilidad de TI, reconocimiento de la empresa, diseño y aplicación de los instrumentos de medición, análisis de la información recogida con la elaboración del diagnóstico situacional, realizar o seleccionar los formatos requeridos dentro de la empresa, creando el marco de referencia y la Implementación de los lineamientos definidos.

Reconocimiento del marco conceptual de gobernabilidad de TI. En este punto se toma la información suministrada anteriormente.

Reconocimiento de la dependencia tecnológica. Incluye una breve historia o reconocimiento de la dependencia desarrolladora del proyecto informático, los Objetivos general y específicos, la Misión y visión de la empresa. Se determina el Diagrama de proceso: procesos fundamentales y procesos de soporte (Ver Figura 2), la Estructura orgánica de la dependencia tecnológica y la Identificación de los perfiles del personal a cargo de los procesos de la TIC como son: Director ejecutivo (CEO), Director financiero (CFO), Ejecutivos del negocio, Director de información (CIO), Propietario del proceso de negocio, jefe de operaciones, Arquitecto en jefe, Jefe de desarrollo, Jefe de administración de TI, La oficina o función de administración de proyectos (PMO) y el cumplimiento, auditoría, riesgo y seguridad.

[5] M. **SANTANA**. *Developing an inter-enterprise alignment maturity model: research challenges and solutions*.Technical Report TR-CTIT-07-29, Centre for Telematics and Information Technology, University of Twente, Enschede.Extraído el 7 de mayo de 2007 desde http://eprints.eemcs.utwente.nl/9780/01/Research_challenges_(REPORT).pdf

Figura 2: Diagrama de Procesos



Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

Diseño y aplicación de los instrumentos de medición. Se necesita medir los tipos de escenarios, las variables determinadas para ser evaluadas que permitan medir el nivel de madurez en sus procesos se establecen de acuerdo al cargo desempeñado dentro de la dependencia, a través de preguntas correspondientes con su función, la existencia de un plan estratégico, la misión, visión y objetivos del proyecto, los recursos, la forma de seguimiento a los procesos, herramientas de medición, gestión y planificación.

Se revisa el nivel de madurez teniendo en cuenta las definiciones establecidas (Ver Tabla 2).

Tabla 2: Valores del Modelo de madurez

0	**No existe:** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
1	**Inicial:** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.
2	**Repetible pero intuitiva:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.
3	**Proceso definido:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4	**Administrado y medible:** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.
5	**Optimizado:** Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

Fuente. COBIT 4.0

Análisis de la información recogida con la elaboración del diagnóstico situacional. Se analiza la información de los instrumentos aplicados como entrevista y la validación de los mismos con la observación o validación respectiva, construyendo la tabla respectiva por cada nivel del modelo y los objetivos de control incluidos tomando como valor válido el observado.
A continuación se representa en una tabla el impacto de los objetivos de control de COBIT 4.1 sobre los criterios y recursos de TI.

La nomenclatura utilizada en los criterios de información para esta tabla es la siguiente: (P), cuando el objetivo de control tiene un impacto directo al requerimiento, (S), cuando el objetivo de control tiene un impacto indirecto es decir no completo sobre el requerimiento, y finalmente ( ) vacío, cuando el objetivo de control no ejerce ningún impacto sobre el requerimiento, en cambio cuando se encuentra con (X) significa que los objetivos de control tienen impacto en los recursos, y cuando se encuentra en blanco ( ), es que los objetivos de control no tienen ningún impacto con los recursos.

Tabla 3: Objetivos de Control de COBIT

Objetivos de Control de COBIT	**Criterios de Información de COBIT**							**Recursos de TI de COBIT**			
	Efectividad	**Eficiencia**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Cumplimiento**	**Confiabilidad**	**Personas**	**Información**	**Aplicación**	**Infraestructura**
Planear y Organizar											

PO1 Definir un plan estratégico de TI	**P**	**S**						**X**	**X**	**X**	**X**
PO2 Definir la arquitectura de la información	**S**	**P**	**S**	**P**					**X**	**X**	
PO3 Definir la dirección tecnológica	**P**	**P**								**X**	**X**
PO4 Definir los procesos, organización y relaciones de TI	**P**	**P**						**X**			
PO5 Administrar la inversión en TI	**P**	**P**					**S**	**X**		**X**	**X**
PO6 Comunicar las metas y la dirección de la gerencia	**P**					**S**		**X**	**X**		
PO7 Administrar los recursos humanos de TI	**P**	**P**						**X**			
PO8 Administrar la calidad	**P**	**P**		**S**			**S**	**X**	**X**	**X**	**X**
PO9 Evaluar y administrar los riegos de TI	**S**	**S**	**P**	**P**	**P**	**S**	**S**	**X**	**X**	**X**	**X**
PO10 Administrar los proyectos	**P**	**P**						**X**		**X**	**X**
Adquirir e Implementar											
AI1 Identificar las soluciones automatizadas	**P**	**S**								**X**	**X**
AI2 Adquirir y mantener software aplicativo	**P**	**P**		**S**			**S**			**X**	
AI3 Adquirir y mantener la infraestructura tecnológica	**S**	**P**		**S**	**S**						**X**
AI4 Facilitar la operación y el uso	**P**	**P**		**S**	**S**	**S**	**S**	**X**		**X**	**X**
AI5 Procurar recursos de TI	**S**	**P**				**S**		**X**	**X**	**X**	**X**
AI6 Administrar los cambios	**P**	**P**		**P**	**P**		**S**	**X**	**X**	**X**	**X**
AI7 Instalar y acreditar soluciones y cambios	**P**	**S**		**S**	**S**			**X**	**X**	**X**	**X**
Entregar y Dar Soporte											
DS1 Definir y administrar los niveles de servicio	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
DS2 Administrar los servicios de terceros	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
DS3 Administrar el desempeño y capacidad	**P**	**P**			**S**					**X**	**X**
DS4 Asegurar el servicio continuo	**P**	**S**			**P**			**X**	**X**	**X**	**X**
DS5 Garantizar la seguridad de los sistemas			**P**	**P**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
DS6 Identificar y asignar costos		**P**					**P**	**X**	**X**	**X**	**X**
DS7 Educar y entrenar a los usuarios	**P**	**S**						**X**			
DS8 Administrar la mesa de servicio y los incidentes	**P**	**P**						**X**		**X**	
DS9 Administrar la configuración	**P**	**S**			**S**		**S**		**X**	**X**	**X**
DS10 Administrar los problemas	**P**	**P**			**S**			**X**	**X**	**X**	**X**

DS11 Administrar los datos				**P**			**P**		**X**		
DS12 Administrar el ambiente físico				**P**	**P**						**X**
DS13 Administrar las operaciones	**P**	**P**		**S**	**S**			**X**	**X**	**X**	**X**
Monitorear y Evaluar											
ME1 Monitorear y evaluar el desempeño de TI	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
ME2 Monitorear y evaluar el control interno	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**
ME3 Garantizar el cumplimiento regulatorio						**P**	**S**	**X**	**X**	**X**	**X**
ME4 Proporcionar gobierno de TI	**P**	**P**	**S**	**S**	**S**	**S**	**S**	**X**	**X**	**X**	**X**

Fuente. Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas

2.3 MARCO CONCEPTUAL

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Apropiación: Las apropiaciones son autorizaciones máximas de gasto que el Congreso de la República aprueba para ser comprometidas durante la vigencia fiscal respectiva. Después del 31 de diciembre de cada año estas autorizaciones expiran y en consecuencia no podrán comprometerse, adicionarse, transferirse.

Auditoría: Puede definirse como el proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso.

Otro concepto de auditoría definido por Echenique es, "un examen crítico que se realiza con el objeto de evaluar la eficiencia y eficacia de una sección o un organismo y determinar cursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos. El encargado de realizar las auditorias es el auditor, un auditor es la persona que evalúa la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de

cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación"[6].

Auditoría Informática: Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientes los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicional de la auditoría.

Bitácora: Libro donde se registran las observaciones de un evento.

Contraseña: Conjunto de caracteres que permite el ingreso a un recurso informático.

Control: Cualquier medido que tome la dirección, el Consejo y otros, para mejorar la gestión de riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas.

Control interno: Todas las medidas utilizadas por una empresa para protegerse contra errores, desperdicios o fraudes y para asegurar la confiabilidad de los datos. Está diseñado para ayudar a la operación eficiente de una empresa y para asegurar el cumplimiento de las políticas de la empresa.

Control Interno Informático: Sistemas Integral al proceso administrativo, en la planeación, organización, dirección y control de las operaciones con el objeto de asegurar la protección de todos los recursos informáticos y mejorar los índices de economía, eficiencia y efectividad de los procesos operativos automatizados.

Cortafuegos: Parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

[6] ECHENIQUE GARCÍA, José Antonio. Auditoría en informática. 2 edición. Bogotá: McGraw Hill, 2004. 300p.

Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Evaluación del riesgo: Proceso global de estimar la magnitud de los riesgos y decidir si un riesgo es o no tolerable.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación del peligro: Proceso que permite reconocer que un peligro existe y que a la vez permite definir sus características.

Identificación del riesgo: Proceso para determinar lo que puede suceder, por qué y cómo.

Impacto: Daño potencial sobre un sistema cuando una amenaza se presenta.

Incidente de seguridad: Es cualquier evento que pueda o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

ISO (Organización Internacional de Normalización): Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

Log de auditoría: Término usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para una aplicación.

Plan de continuidad del negocio: Estrategia planificada constituida por: un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

Riesgo: Se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños.

Sistema de información: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

Tratamiento del riesgo: Selección e implementación de las opciones apropiadas para ocuparse del riesgo.

Valoración del riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Vulnerabilidad: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

2.4 MARCO TEÓRICO

2.4.1 ISO/IEC 27001:20057

Publicada el 15 de octubre de 2005, es la norma principal de la familia de la ISO27000, y contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. A pesar de no ser obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados. Recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI.

2.4.2 ISO/IEC 27002:2005

Describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, mencionados en el anexo A de la ISO 27001, 39 objetivos de control y 133 controles.

Los dominios a tratar son los siguientes:

- **Políticas de Seguridad:** Busca establecer reglas para proporcionar la dirección gerencial y el soporte para la seguridad de la información. Es la base del SGSI.

[7] INTERNATIONAL ORGANIZATION FOR STANDARIZATION ISO/IEC 27000. www.iso27000.es. 2008

- **Organización de la seguridad de la información:** Busca administrar la seguridad dentro de la compañía, así como mantener la seguridad de la infraestructura de procesamiento de la información y de los activos que son accedidos por terceros.

- **Gestión de activos:** Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos. Trata que cuenten con un nivel adecuado de seguridad.

- **Seguridad de los recursos humanos:** Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información. Busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

- **Seguridad física y ambiental:** Trata principalmente de prevenir el acceso no autorizado a las instalaciones para prevenir daños o pérdidas de activos o hurto de información.

- **Gestión de comunicaciones y operaciones:** Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

- **Control de accesos:** El objetivo de esta sección es básicamente controlar el acceso a la información, así como el acceso no autorizado a los sistemas de información y computadoras. De igual forma, detecta actividades no autorizadas.

- **Sistemas de información, adquisición, desarrollo y mantenimiento:** Básicamente busca garantizar la seguridad de los sistemas operativos, garantizar que los proyectos de TI y el soporte se den de manera segura y mantener la seguridad de las aplicaciones y la información que se maneja en ellas.

- **Gestión de incidentes de seguridad de la información:** Tiene que ver con todo lo relativo a incidentes de seguridad. Busca que se disponga de una metodología de administración de incidentes, que es básicamente definir de forma clara pasos, acciones, responsabilidades, funciones y medidas correctas.

- **Gestión de continuidad del negocio:** Lo que considera este control es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio. Busca a su vez, contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencias de fallas o desastres.

- **Cumplimiento:** Busca que las empresa cumpla estrictamente con las bases legales del país, evitando cualquier incumplimiento de alguna ley civil o penal, alguna obligación reguladora o requerimiento de seguridad. A su vez, asegura la conformidad de los sistemas con políticas de seguridad y estándares de la organización.

2.4.3 COBIT 4.1

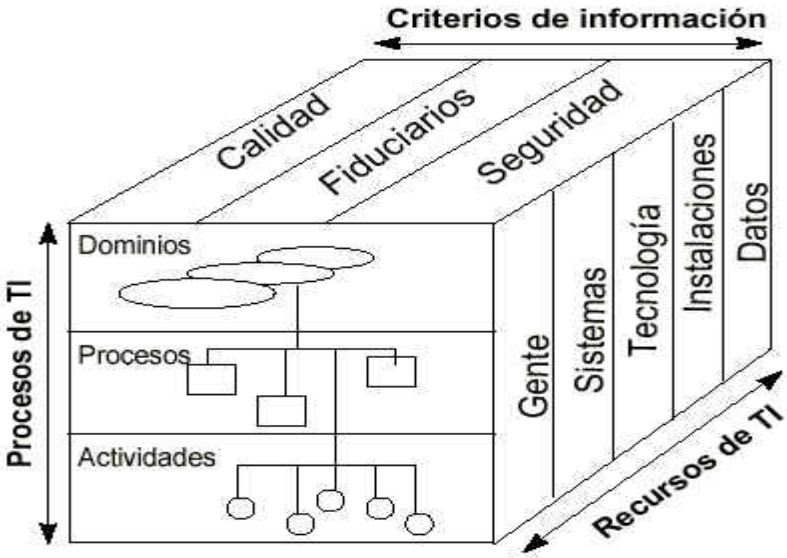
COBIT es un framework (también llamado marco de trabajo) de Gobierno de TI y un conjunto de herramientas de soporte para el gobierno de TI que les permite a los gerentes cubrir la brecha entre los requerimientos de control, los aspectos técnicos y riesgos de negocio.

Describe como los procesos de TI entregan la información que el negocio necesita para lograr sus objetivos. Para controlar la entrega, COBIT provee tres componentes claves, cada uno formando una dimensión del cubo COBIT, que se puede apreciar en la Figura 2.

Como un framework de gobierno y control de TI, COBIT se enfoca en dos áreas claves:

- Proveer la información requerida para soportar los objetivos y requerimientos del negocio.
- Tratamiento de información como resultado de la aplicación combinada de recursos de TI que necesita ser administrada por los procesos de TI.

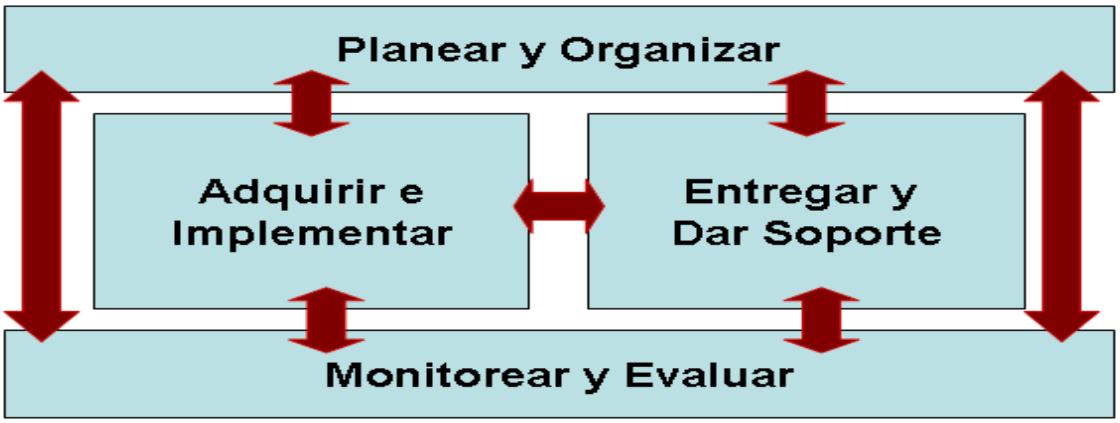
Figura 3: Componentes de COBIT 4.1



Fuente: COBIT 4.1, www.isaca.org

Tiene 34 procesos de alto nivel clasificados en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y, Monitorear y Evaluar, tal y como se puede apreciar en la Figura 3.

Figura 4. Dominios de COBIT



Fuente: COBIT 4.1, www.isaca.org

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores."

COBIT brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica, y están más enfocadas al control y mucho menos en la ejecución. El modelo COBIT cuenta con 4 dominios, 34 procesos de TI, 210 objetivos de control y 40 guías de auditoría. Los 4 dominios de COBIT son:

- **Planear y Organizar:** Este dominio cubre las estrategias y se refiere a la forma en que la tecnología de información puede contribuir a que se cumplan los objetivos del negocio. Busca establecer una organización y una infraestructura tecnológica apropiadas. Los procesos de TI con los que cuenta este dominio son:

- Definir un Plan Estratégico de TI
- Definir la Arquitectura de la Información
- Determinar la Dirección Tecnológica
- Definir los Procesos, Organización y Relaciones de TI
- Administrar la Inversión en TI
- Comunicar las Aspiraciones y la Dirección de la Gerencia
- Administrar Recursos Humanos de TI
- Administrar la Calidad
- Evaluar y Administrar los Riesgos de TI
- Administrar Proyectos

- **Adquirir e Implementar:** Las soluciones deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio para llevar a cabo la estrategia de TI.

Este dominio cubre los cambios y el mantenimiento realizado a sistemas existentes. Los procesos de TI con los que cuenta este dominio son:

- Identificar soluciones automatizadas.
- Adquirir y mantener software aplicativo.
- Adquirir y mantener infraestructura tecnológica.
- Facilitar la operación y el uso.
- Adquirir recursos de TI.
- Administrar cambios.
- Instalar y acreditar soluciones y cambios.

- **Entregar y Dar Soporte:** Este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el

entrenamiento, seguridad y continuidad. Incluye el procesamiento de los datos por sistemas de aplicación, clasificados frecuentemente como controles de aplicación. Los procesos de TI con los que cuenta este dominio son:

- Definir y administrar los niveles de servicio.
- Administrar los servicios de terceros.
- Administrar el desempeño y la capacidad.
- Garantizar la continuidad del servicio.
- Garantizar la seguridad de los sistemas.
- Identificar y asignar costos.
- Educar y entrenar a los usuarios.
- Administrar la mesa de servicio y los incidentes.
- Administrar la configuración.
- Administrar los problemas.
- Administrar los datos.
- Administrar el ambiente físico.
- Administrar las operaciones.

- **Monitorear y Evaluar:** Este dominio hace hincapié a que los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Los procesos de TI con los que cuenta este dominio son:

- Monitorear y evaluar el desempeño de TI.
- Monitorear y evaluar el Control interno.
- Garantizar el cumplimiento regulatorio.
- Proporcionar el gobierno de TI.

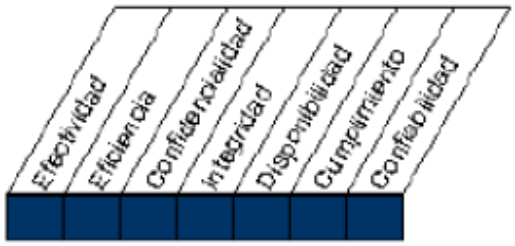
COBIT a su vez, tiene 7 criterios de información, agrupados en 3 requerimientos (calidad, fiduciarios y seguridad) con los que clasifica a cada uno de los 34 procesos de TI, según el enfoque que tenga el proceso. Estos criterios son:

- Efectividad: Se refiere a la información cuando es entregada de manera correcta, oportuna, consistente y usable.
- Eficiencia: Se refiere a la provisión de información a través de la utilización óptima de los recursos.

- Confidencialidad: Se refiere a la protección de la información sensible de su revelación no autorizada. Tiene que ver que con la información enviada a una persona debe ser vista solo por esa persona y no por terceros.
- Integridad: Se refiere a que la información no haya sufrido cambios no autorizados.
- Disponibilidad: Se refiere a que la información debe estar disponible para aquellas personas que deban acceder a ella, cuando sea requerida.
- Cumplimiento: Se refiere a cumplir con las leyes, regulaciones y acuerdos contractuales a los que la compañía se encuentra ligada.
- Confiabilidad: Se refiere a la provisión de la información apropiada a la alta gerencia que apoyen a la toma de decisiones.

En todos los procesos de TI del COBIT se puede saber a qué enfoque está orientado. Puede ser que abarque todos los enfoques, o que sólo abarque algunos, y para todos los controles se indicará si el enfoque es primario (P) o secundario (S).

Figura 5. Enfoque de procesos de TI de COBIT



Fuente: COBIT 4.1, www.isaca.org

Con respecto a los recursos de TI mencionados en la otra dimensión del cubo, se definen de la siguiente manera:

- Aplicaciones: Son procedimientos manuales y sistemas de usuarios automatizados que procesan información.
- Información: Es data que son ingresada, procesada y obtenida de los sistemas de información en cualquier formato usado por el negocio.
- Infraestructura: Incluye la tecnología y facilidades tales como: hardware, sistemas operativos y redes que permiten el procesamiento de las aplicaciones.

- Personas: Son requeridos para planificar, organizar, adquirir, implantar, entregar, soportar, monitorear y evaluar los servicios y sistemas de información. Ellos podrían ser internos, *outsourcing* o contratado

2.5 MARCO LEGAL

Tabla 4: Normativa

NORMA	DESCRIPCIÓN
Artículos 209 y 269, Constitución Política de Colombia de 1991.	En los artículos 209 y 269 se fundamenta el sistema de control interno en el Estado Colombiano, el primero establece: "La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley" y en el 269, se soporta el diseño del sistema: "En las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley, la cual podrá establecer excepciones y autorizar la contratación de dichos servicios con empresas privadas colombianas".
Ley 1273 de 2009	Se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.
Ley 1341 de 2009	Se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro.
Constitución/1991	Reitera el principio fundamental de competencia abierta., permite la inversión extranjera en el sector, y establece el carácter público del espectro electromagnético encargándole al Estado su control.
Decreto 2122/1992	Modifica algunos artículos del Decreto 1901 asignándole nuevas funciones al Ministerio de Comunicaciones y creando nuevas dependencias, entre las cuales se encuentra la Comisión de regulación de Telecomunicaciones como una Unidad Administrativa

	Especial.
Ley 335/1996	Modifica aspectos fundamentales de la normatividad en materia de televisión la cual estaba contenida en la Ley 14 de 1991 y en la Ley 182de1995.Por medio de esta Ley se permite una mayor participación del sector privado en la prestación del servicio de televisión.
Ley 689/2001	Modificó parcialmente la ley 142 de 1994 de servicios públicos domiciliarios en lo relacionado a los numerales 14.15 y 14.24 del artículo 14.
Decreto 575/2002	Mediante este decreto se reglamenta la prestación de los servicios de comunicación personal (PCS), fue modificado en el artículo 59 por decreto 576 de 2002.
Decreto 1686/2002	Se reglamenta el artículo 36 de la ley 80 de 1993, el cual establece que el término de duración de las concesiones para la prestación de los servicios y actividades de telecomunicaciones no podrá exceder de diez años, prorrogable automáticamente por un lapso igual.
Decreto 600/2003	Por medio del decreto 600 de 2003se expiden normas sobre los servicios de Valor Agregado y Telemáticos, y se reglamenta el decreto ley 1900 de 1990.
Decreto 0020/2003	En el decreto 0020 de 2003 se establece el procedimiento a seguir por el Ministerio de Comunicaciones para la fijación de las condiciones de administración del dominio.
Decreto 3055/2003	Por medio del cual se modifica el decreto 600 de 2003.
Decreto 195/2005	Por la cual se adoptan límites de exposición de las personas a campos electromagnéticos, se adecúan procedimientos para la instalación de estaciones radioeléctricas y se dictan otras disposiciones.
Decreto 075/2006	Interceptación de servicios de telecomunicaciones. Operadores de servicio móvil celular y PCS.
Decreto 1928/2006	Espectro electromagnético.

3. DISEÑO METODOLÓGICO

3.1 DISEÑO METODOLÓGICO

La presente investigación demostró que el diseño de un Sistema de Gestión de la Seguridad de la Información, ayudará a mejorar la gestión de los riesgos asociados con la información, para tal efecto se hace uso de una investigación cuantitativa ya que el objetivo es adquirir conocimientos fundamentales mediante una medición objetiva, demostración de la causalidad y la generación de resultados de la investigación, que nos permita conocer la realidad de una manera más imparcial; esta investigación tiene un enfoque descriptivo, permitiendo comprobar sistemática y progresivamente las características de la solución al problema planteado en la empresa objeto de estudio.

3.2 POBLACIÓN Y MUESTRA

La población para la realización de la investigación está conformada por los integrantes del área de Control y Vigilancia de la territorial Ocaña, Ingeniero de Sistemas de la territorial, responsable de la oficina de archivo, Coordinador de la oficina de control y vigilancia y el director territorial de Ocaña.

Para efectos de esta investigación se tomará como muestra al total de la población dado que todos conforman el grupo de trabajo del área de control y vigilancia, y la cantidad a evaluar es fácilmente abarcable.

3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Se desarrollarán herramientas para ser utilizadas para la ejecución del proceso de investigación con el fin de obtener conocimientos de la dependencia y evidencias claras y suficientes del problema de investigación, estas herramientas son las siguientes:

Observación directa: Esta será una herramienta de trabajo en donde se evaluará los procesos desde la propia dependencia a fin de recopilar evidencias suficientes para detectar riesgos en el manejo de la información y tecnologías de TI.

Encuesta: El propósito de esta herramienta es realizar una comunicación interpersonal entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a los interrogantes planteados sobre el problema propuesto.

3.4 SEGUIMIENTO METODOLÓGICO A LAS ACTIVIDADES

Tabla 5: Seguimiento de las Actividades

Objetivos Específicos	Actividades	Resultado/Entregable
Elaborar un estudio para diagnosticar los elementos del proceso de control y vigilancia que se desarrolla en la territorial de Ocaña con el fin de identificar riesgos de TI/SI	1. Hacer el levantamiento de la información como: misión, visión, objetivos, procesos entre otros 2. Diseñar una encuesta para ser aplicada al área de sistemas 3. Aplicar la encuesta diseñada	Direccionamiento estratégico de la empresa
Identificar los elementos que conforman el SGSI – Sistema de Gestión de Seguridad de la Información para la oficina de control y vigilancia en la corporación	1. Consultar los elementos que estructuran un Sistema de Gestión de Seguridad de la Información 2. Adaptar al contexto de la oficina de control y vigilancia los dominios de seguridad física y lógica	Documentos del Marco Referencial.
Documentar formalmente las actividades y políticas requeridas para gestionar adecuadamente la seguridad de la información en la oficina de control y vigilancia en la corporación	1. Estudiar la información que describe la empresa para conocer sus procesos, necesidades y requerimientos 2. Crear la guía con políticas, estándares y procedimientos para la gestión de la seguridad de la información.	Documento guía para la aplicación de políticas y estándares de seguridad informática

4. PRESENTACIÓN DE RESULTADOS

4.1 DIAGNÓSTICO DEL PROCESO DE CONTROL Y VIGILANCIA QUE SE DESARROLLA EN LA TERRITORIAL DE OCAÑA CON EL FIN DE IDENTIFICAR RIESGOS DE TI/SI

4.1.1 Modelado del Negocio

LA CORPORACIÓN AUTÓNOMA REGIONAL DE LA FRONTERA NORORIENTAL (**CORPONOR)** fue creada mediante decreto 3450 del 17 de Diciembre del año 1983, durante el gobierno de Belisario Betancourt, como corporación de desarrollo cuyo objetivo principal era encausar, fomentar, coordinar, ejecutar y consolidar el desarrollo económico y social de la región comprendida dentro de su jurisdicción y con algunas funciones de administración de los recursos naturales y del Medio Ambiente.

MISION
Ejercer la autoridad ambiental propendiendo por el desarrollo humano sostenible, promoviendo la gestión ambiental colectiva y participativa en el departamento Norte de Santander.

VISION
Ser en el 2019 la entidad reconocida, respetada y de referencia obligatoria para la toma de decisiones que orienten el desarrollo humano sostenible del departamento Norte de Santander.

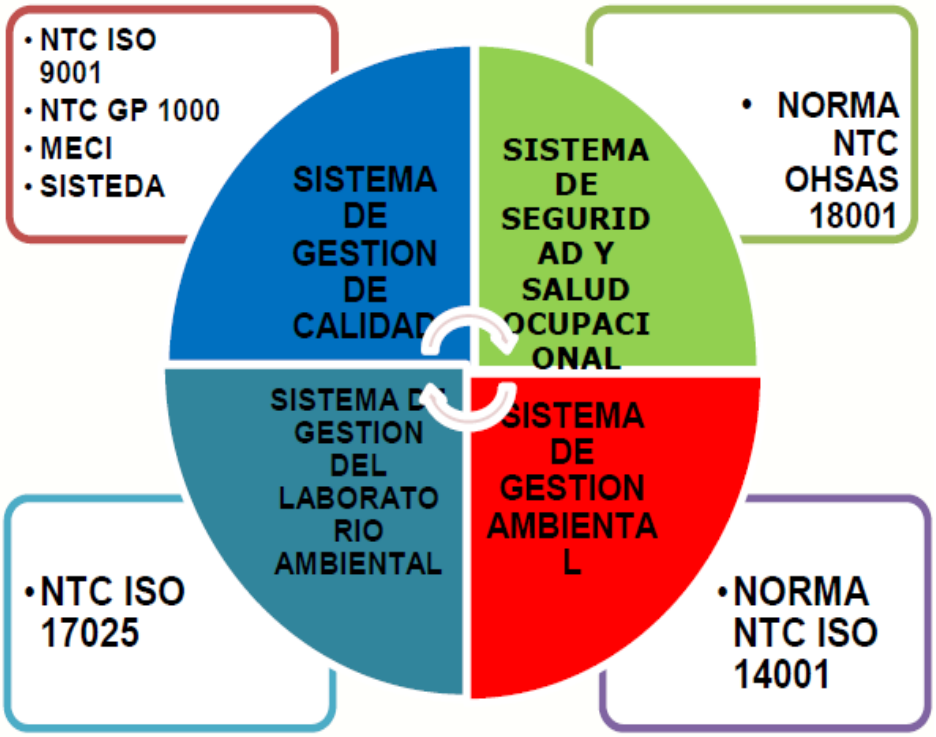
POLITICA DE GESTION INTEGRAL HSEQ
En la CORPORACIÓN AUTÓNOMA REGIONAL DE LA FRONTERA NORORIENTAL CORPONOR, promovemos la gestión ambiental colectiva y participativa, contando con un equipo humano competente y comprometido a:
- Ejercer la Autoridad Ambiental, con el fin de satisfacer las necesidades y expectativas de las partes interesadas, enmarcado en la eficiencia, eficacia y efectividad.
- Prevenir y mitigar el impacto ambiental negativo generado en el desarrollo de nuestras actividades.
- Implementar actividades de promoción y prevención en salud dirigidas a nuestros funcionarios y de Seguridad para nuestros colaboradores y visitantes.
- Prestar servicios de caracterización de aguas, con resultados confiables, oportunos, imparciales e independientes.

- Cumplir con la legislación aplicable y los acuerdos suscritos por la Entidad.

- Mejorar continuamente el Sistema de Gestión Integral HSEQ, siguiendo los parámetros y documentación establecida.

A través de la aplicación de esta política nos consolidaremos como la entidad reconocida, respetada y de referencia obligatoria para la toma de decisiones que orienten el desarrollo humano sostenible en el Departamento Norte de Santander.

Figura 6. Sistemas Actuales en CORPONOR



Fuente: CORPONOR

OBJETIVOS CORPORATIVOS

CORPONOR tiene por objeto ejercer la máxima autoridad ambiental en la zona de su jurisdicción a través de la administración del Medio Ambiente y los Recursos Naturales Renovables, con el fin de propender al desarrollo sostenible de los mismos

VALORES CORPORATIVOS:

- **CALIDAD:** actuación oportuna, responsable y eficiente en el cumplimiento de las funciones corporativas.
- **CREATIVIDAD:** Búsqueda permanente de motivaciones y alternativas que orienten al crecimiento y desarrollo continuo.

- **TRABAJO EN EQUIPO:** Es la unión de esfuerzos y saberes para lograr un propósito común.

- **GESTIÓN HUMANA:** Capacidad permanente de identificar y aprovechar al máximo el potencial del personal en función de su propio crecimiento y de la entidad.

- **INTEGRIDAD:** Actuar con conocimiento, respeto y ética en el cumplimientos de las funciones.

- **CONFIDENCIALIDAD:** Ser responsable y prudente en el uso de la información.

- **COMPROMISO:** Estar dispuesto de manera permanente en el cumplimiento de la Misión de la Entidad.

- **TRANSPARENCIA:** Actuar con equidad, independencia e imparcialidad, respetando los derechos de los ciudadanos y los demás grupos de interés.

- **AUSTERIDAD:** Dar uso eficiente y eficaz a los recursos asignados, ajustados a las normas de la moral.

VALORES ÉTICOS:

- **HONESTIDAD:** Calidad humana que determina a la persona actuar en verdad y justicia, expresa respeto por uno mismo y por los demás.

- **TOLERANCIA:** Virtud que se adquiere como proceso de aceptar la igualdad de derechos humanos respetando las diferencias para mantener mejores relaciones personales.

- **JUSTICIA:** Reconocemos los derechos y distribuimos con criterio de equidad los recursos públicos. Actuar en forma equitativa y racional, cada uno de los recursos naturales renovables que requieran nuestros usuarios para vivir mejor y sus familias,

siempre y cuando hagan uso con sentido de responsabilidad frente a las futuras generaciones.

- **PERTENENCIA:** Considerar cada uno de los miembros la Corporación como propia y por lo tanto asumir y afrontar sus éxitos y adversidades como un compromiso personal de satisfacción y mejora continua. La Pertenencia no se razona, se siente.

- **SOLIDARIDAD:** Trabajar en equipo en un ambiente de respeto y colaboración, asociados por la protección del medio ambiente, la Solidaridad es una característica de la sociabilidad que inclina al hombre a sentirse unido a sus semejantes y a la cooperación con ellos.

- **LEALTAD:** Compromiso implícito de actuación solidaria y comprometida en la búsqueda de objetivos comunes, que conllevan a vivir en armonía con el medio ambiente. Lealtad aparece cuando las interacciones entre comunidad-usuario han sido satisfactorias, sobre todo para este último. Ser leal implica compromiso y eso sólo se obtiene cuando el valor obtenido por el usuario es alto, o bien difícil de sustituir.

- **SINCERIDAD:** La Sinceridad es un valor que caracteriza a las personas por la actitud congruente que mantienen en todo momento, basada en la veracidad de sus palabras y acciones. Es un valor que produce plenitud personal y se define como expresión plena del ser miso, de actuar y relacionarse transparentemente en el marco de la verdad.

- **HUMILDAD:** Humildad es aceptar las cualidades con las que nacemos o desarrollamos, desde el cuerpo hasta las posesiones más preciadas. Por tanto, debemos utilizar estos recursos de forma valiente y benevolente. Ser humilde es dejar hacer y dejar ser, si aprendemos a eliminar la arrogancia, reconocemos las capacidades físicas, intelectuales y emocionales de los demás.

- **RESPONSABILIDAD:** La responsabilidad es un valor, porque gracias a ella podemos convivir en sociedad de una manera pacífica y equitativa. La responsabilidad en su nivel más elemental es cumplir con lo que se ha comprometido, o la ley hará que se cumpla. Pero hay una responsabilidad mucho más sutil (y difícil de vivir), que es la del plano moral.

- **RESPETO:** Es el reconocimiento del valor inherente y de los derechos innatos de individuos y de la sociedad. Si aprendemos a respetar el medio ambiente y administrar bien los recursos que nos regala la naturaleza, se evitarán catástrofes presentes y futuras; todos disfrutemos de un lugar más próspero para vivir como Dios quiere.

DESCRIPCIÓN DE LA ESTRUCTURA ORGANIZACIONAL

El Organigrama funcional de la Corporación Autónoma Regional de la Frontera Nororiental está conformado por la Asamblea Corporativa, como primer órgano de Dirección de la Corporación, seguida de un Consejo Directivo como órgano de administración, La Dirección General articulada con una Secretaría General, cuatro Subdirecciones de Apoyo, cuatro Oficinas y tres Direcciones Territoriales con sedes en Ocaña, Pamplona y Tibú.[8]

ORGANIGRAMA GENERAL:

Figura 7. Estructura Organizacional

[8] Fuente: CORPONOR. Plan de Acción 2012-2015[online]. Ocaña (Colombia). [Citado el 22 de Agosto de 2013]. Disponible en: http://www.corponor.gov.co/index.php?option=com_content&view=article&id=1259&Iteìte=299.

Fuente: CORPONOR

4.1.2 Descripción de procedimientos de auditorías y hallazgos encontrados

En este documento, se describen los resultados de la auditoría realizada a la seguridad física y ambiental en el área de control y vigilancia de la Corporación Autónoma Regional de la Frontera Nororiental "CORPONOR" territorial Ocaña, realizada del 20 de septiembre al 11 de octubre de 2013.
Para el desarrollo de esta auditoría se tuvieron en cuenta los siguientes lineamientos acordados con la dirección general:

- Acceso físico al cuarto de telecomunicaciones
- Aspectos relacionados con el Hardware
- Existencia de Plan de desastres o políticas de seguridad
- Estado de las instalaciones eléctricas y cableado
- Aspectos generales en cuanto a seguridad física

Durante la auditoría se realizó una investigación preliminar, con el fin de conocer la Corporación y los procesos que se llevan a cabo.

Todo el trabajo de auditoría se adelantó de acuerdo a la planeación, teniendo como referencia el programa y la guía de auditoría, entre las actividades que se contemplaban en los mismos estaba la recolección de la información, para ello fue indispensable la utilización de instrumentos como cuestionarios y listas de chequeo y la aplicación de técnicas como observación directa, revisión documental, solicitud de documentos (manuales) y entrevistas.

De los resultados obtenidos en la evaluación, me permito informarle a usted lo siguiente:

- Las condiciones ambientales del área, en lo referente a la iluminación y ventilación no son las adecuadas.

- El acceso al área de control y vigilancia, no está protegido por controles de ingreso apropiados.

- El cableado estructurado del lugar no cumple con los estándares.

- Son precarias las condiciones de orden y de saneamiento del lugar.

De acuerdo con las pruebas realizadas para verificar los controles existentes, en cuanto a la **seguridad física** del área, me permito dictaminar lo siguiente:

- Las condiciones ambientales del área de control y vigilancia, no son idóneas debido a que carece de un sistema de enfriamiento o aire acondicionado, lo cual hace que la temperatura no esté controlada, ocasionando calor excesivo y por ende se puede presentar un sobrecalentamiento en los equipos y dispositivos de cómputos que se encuentran en el lugar. Según el estándar ISO 17799, capítulo 9 que trata de la **seguridad física y del ambiente,** en el subíndice 9.2.1 **Ubicación y protección de los equipos de cómputo**, inciso f, se debe monitorear las condiciones ambientales, tales como temperatura y humedad; para evitar el calor excesivo en el lugar se recomienda la instalación de un aire acondicionado, que provea una temperatura adecuada para la protección de los equipos que allí reposan.

- El cuarto de telecomunicaciones se encuentra ubicado en el baño, haciéndolo vulnerable a riesgos naturales (Humedad excesiva, filtraciones de agua, entre otros), además la puerta no cuenta con una cerradura apropiada que le proporcione un nivel de seguridad, la cerradura con que cuenta actualmente es fácil de violar y a esto se suma el hecho que no hay vigilancia que controle el acceso al mismo, propiciando un escenario para el robo o el sabotaje de los equipos. Tomando como referencia el estándar ISO 17799, capítulo 9, subíndice 9.1.4 **Protección contra amenazas internas y externas,** inciso c, se deben asignar protecciones físicas contra daño o fuego, por tal razón se recomienda, reubicar el Rack e instalar un dispositivo que detecte humo y un extintor en el área que esté debidamente señalizado y visible. Además de esto se recomienda cambiar la cerradura de la puerta por una que ofrezca mayor seguridad ya que esto es considerado en el inciso 9.1.1 **Áreas seguras** como una barrera de protección.

- Es fácil acceder al área de control y vigilancia, ya que no existen mecanismos de control que regulen la entrada como la vigilancia y el personal no es registrado. Ya que a pesar de que se inscriben los visitantes en la portería, no hay acompañamiento hasta las proximidades de la oficina. Se recomienda según el estándar ISO 17799, capítulo 9, subíndice 9.1.2 **control de ingreso físico,** registrar la fecha y la hora de entrada y salida de los visitantes en una bitácora y es necesario en lo posible que estas visitas sean supervisadas y el acompañamiento de los visitantes hacia las instalaciones de la corporación.

- El cableado estructurado del lugar no cumple con los estándares, se observan tomas de datos y cajas sin tapas, interruptores sin la debida señalización, tuberías por donde pasan cables eléctricos expuestos. Se recomienda tomando como referencia el subíndice

9.2.3 **Seguridad del cableado,** proteger los cables, para ello es necesario colocar las tapas a las cajas y tomas que no los tenga, además se debe señalizar los interruptores y tapar la tubería de luz que está expuesta.

- Se observa desaseo en el área de control y vigilancia, hay gran cantidad de equipos obsoletos, a esto se suma que ingieren bebidas y alimentos. Teniendo como base el subíndice 9.1.3 y el 9.2.1 el estándar ISO 17799 se recomienda:

  Establecer lineamientos para la prohibición del consumo de alimentos, bebidas o fumar en el área de trabajo.

  Adquisición de equipos de punta con la suficiente robustez en hardware y software con las especificaciones técnicas idóneas para el manejo de las aplicaciones utilizadas en esta oficina.

De acuerdo a los dominios de COBIT se realizó una clasificación de las principales situaciones detectadas.

Tabla 6: Grados de Madurez

Dominio	**Análisis por dominios**	**Nivel de Madurez**
Planear y Organizar	• No se encuentran alineadas las estrategias de TI y del negocio. • Corponor Ocaña no está alcanzando el uso óptimo de los recursos ya que estos no son aprovechados al máximo, no se cuenta con los recursos necesarios para el desempeño de ciertas tareas.	**2**
Adquirir e Implementar	• Para que se cumplan la estrategia de TI, se debe identificar, desarrollar o adquirir las soluciones de TI, así como la implementación e integración en los procesos del negocio.	**2**
Entregar y Dar Soporte	• Los servicios de TI son medianamente entregados de acuerdo a las prioridades del negocio. • Los costos de TI no se encuentran totalmente optimizados puesto que no existe un plan de continuidad y no es implementada la disponibilidad de forma completa de los sistemas de TI.	**1**
Monitorear y	• La gerencia no monitorea ni evalúa el control	**0**

Evaluar	interno en Corponor Ocaña. • No existe vinculación en el desempeño de TI con las metas del negocio. • No existe una medición óptima de riesgos y el reporte de estos, así como el cumplimiento, desempeño y control.	

Fuente: COBIT 4.1

4.1.3 Análisis y evaluación de riesgos

Los riesgos son eventos negativos internos y externos que se pueden presentar afectando alcanzar los objetivos de la organización; su evaluación debe identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización y los resultados deben guiar y determinar la acción de gestión apropiada para implementar los controles seleccionados y proteger la información.

A continuación se describen las principales situaciones encontradas, las causas de las mismas, se hace una tabla donde se analizan los riesgos, su probabilidad de ocurrencia y el impacto para la organización en caso de que esto se materialice.

Tabla 7: Hallazgos

SITUACIONES	CAUSAS	SOLUCIÓN
Las condiciones ambientales del área, en lo referente a la luz y ventilación no son las adecuadas.	El área no posee unas condiciones adecuadas, para laborar.	Acondicionar el área de esta dependencia.
El acceso al área de control y vigilancia, no está protegido por controles de ingreso apropiados.	No existe un ingreso controlado de personas al área.	Implementar un registro de control para el personal, con la ayuda de una bitácora.
El cableado estructurado del lugar no cumple con los estándares.	El cableado en el área, se encuentra descubierto	Implementar una cubierta de seguridad para los cables, como las canaletas
Son precarias las condiciones de orden y de saneamiento del lugar. -	Se evidencian en el área cantidad de expedientes a campo abierto, lo que hacen que el área no sea una dependencia ordenada y aseada. Se evidencia el consumo de bebidas y alimentos dentro del área de control y vigilancia	Colocar unos estantes, para ordenar cada uno de los expedientes. Al igual implementar estrategias de saneamiento. Diseñar estrategias para evitar el consumo de bebidas y alimentos dentro del área de control y vigilancia.

Fuente: Autores del Proyecto

Tabla 8: Análisis de Riesgos

CORPONOR TERRITORIAL OCAÑA																			
Objetivo: Identificar y priorizar los riesgos en comparación con el nivel aceptable por la Corporación.																			
Identificación de Riesgos					Análisis Cualitativo de Riesgos														
Código Riesgo	Proceso	Riesgo	Causa	Descripción	Probabilidad					Impacto					Calificación Riesgo				
					Muy Probable	Bastante Probable	Probable	Poco Probable	Improbable	Muy Alto	Alto	Moderado	Bajo	Muy Bajo	Alto	Moderado	Bajo		
RO	Control y Vigilancia	Pérdida o daño en los activos asociados al procesamiento y almacenamiento de los datos	1. Las condiciones ambientales del área no son idóneas debido a que carece de un sistema de enfriamiento	Los activos como equipos de cómputo y equipos de comunicaciones podrían afectarse por las altas temperaturas	X					X					0.72				
RO	Control y Vigilancia	Pérdida, daño e interferencia de la operación por el acceso físico no autorizado.	1. No existen barreras que aseguren el área donde reposan los expedientes físicos. 2. Los equipos de comunicaciones no cuentan con restricciones de acceso.	Al no contar con perímetros de seguridad para proteger las áreas que contienen los expedientes se pueden presentar pérdida, daño o alteración de estos debido al ingreso de personal no autorizado.	X					X					0.72				
RT	Sistemas	Robo, pérdida o alteración de los datos contenidos en los sistemas de información	1. No existen controles anti malware. 2. El cableado instalado no cumple con la norma.	La falta de controles técnicos para defenderse del software malicioso expone los datos. No contar con un esquema de cableado estructurado implica que los datos puedan ser vulnerados.		X				X					0.56				

Código identificador del riesgo. Denota el tipo de riesgo a analizar, así:
RO - Riesgo Organizacional
RT - Riesgo Técnico
RA - Riesgo Administrativo
RE - Riesgo Externo

Tabla 9: Ayuda para interpretación de matriz de riesgo

PROBABILIDAD	**CUANTIFICACIÓN**	**DESCRIPCIÓN**	**FRECUENCIA**
Muy probable	0.9	Se espera que el evento ocurra en la mayoría de los casos.	Más de 1 vez al año.
Bastante Probable	0.7	El evento probablemente ocurrirá.	Al menos 1 vez en el último año.
Probable	0.5	El evento puede suceder eventualmente.	Al menos 1 vez en los últimos 2 años.
Poco Probable	0.3	El evento podría ocurrir en algún momento y se considera que es difícil que suceda.	Al menos 1 vez en los últimos 5 años.
Improbable	0.1	El evento ocurriría solamente en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.

Tabla 10: Calificación otorgada en la matriz de riesgo

IMPACTO	**CUANTIFICACIÓN**	**DESCRIPCIÓN**
Muy Alto	0.8	- Pérdida de la capacidad de operación que tiene efectos perjudiciales. - Enorme pérdida financiera. - Grave pérdida de imagen.
Alto	0.4	- Daños extensivos, pérdida de la capacidad de operación que no tienen efectos perjudiciales. - Pérdidas financieras mayores. - Pérdida de imagen.
Moderado	0.2	- Se necesita asistencia de un tercero para subsanar los daños. - La pérdida financiera es alta. - Podría existir pérdida de imagen.
Bajo	0.1	- Se puede subsanar los daños inmediatamente. - La pérdida financiera es media. - No hay pérdida de imagen.

Muy Bajo	0.05	- No hay daños o perjuicios. - La pérdida financiera es baja. - No hay pérdida de imagen.

Tabla 11: Evaluación, marcador de riesgo para un riesgo específico (PxI)

IMPACTO **PROBABILIDAD**	**Muy bajo 0.05**	**Bajo 0.1**	**Moderado 0.2**	**Alto 0.4**	**Muy Alto 0.8**
Muy Probable 0.9	**0.05**	**0.09**	**0.18**	**0.36**	**0.72**
Bastante Probable 0.7	**0.04**	**0.07**	**0.14**	**0.28**	**0.56**
Probable 0.5	**0.03**	**0.05**	**0.10**	**0.20**	**0.40**
Poco Probable 0.3	**0.02**	**0.03**	**0.06**	**0.12**	**0.24**
Improbable 0.1	**0.01**	**0.01**	**0.02**	**0.04**	**0.08**

Riesgo Bajo		Gestionar mediante procedimientos de rutina, es improbable que se necesite la aplicación específica de recursos.
Riesgo Moderado		Gestionar mediante procedimientos de monitoreo o respuesta específicas.
Riesgo Alto		Acción inmediata, especificar planes de acción y atención de la alta dirección.

4.2 IDENTIFICACIÓN DE ELEMENTOS DEL SGSI PARA LA OFICINA DE CONTROL Y VIGILANCIA DE CORPONOR OCAÑA

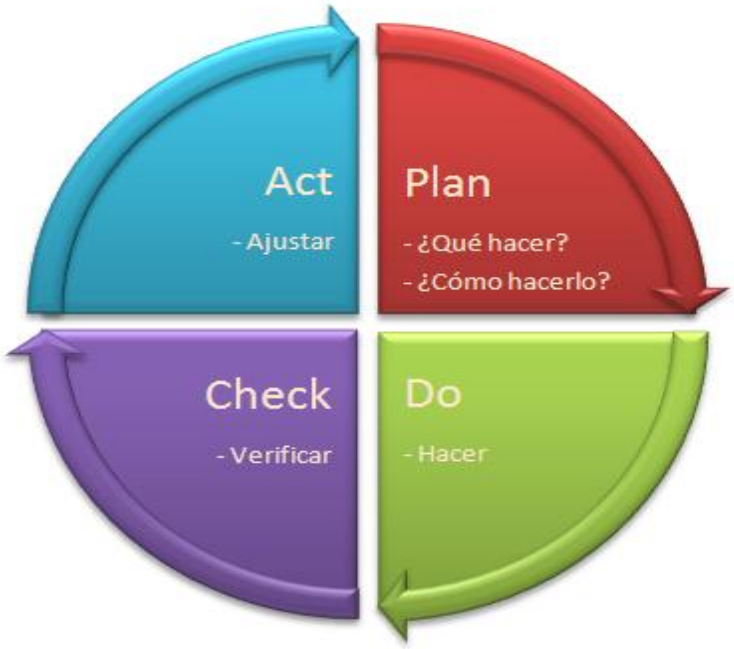
4.2.1 ISO/IEC 27001

Este estándar internacional ha sido preparado para proporcionar un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

El presente sistema de gestión de la seguridad de la información (SGSI) se basa en la norma ISO/IEC 27001:2005, la cual contiene los requisitos básicos que debe tener todo sistema de gestión de seguridad de la información y es la norma sobre la cual se certifican, por auditores externos, los SGSI de las organizaciones. Propone un sistema basado en el Ciclo de Deming: Plan, Do, Check, Act (Planear, Hacer, Verificar, Actuar) conocido como PDCA, el cual encamina a un sistema de mejora continua con capacidad de adaptase a cambios y necesidades de su entorno de desarrollo.

Figura 8. Ciclo de Deming



A continuación se hace una breve descripción de las actividades que se deben realizar en cada una de las 4 Fases del ciclo PDCA según el estándar internacional 27001[9].

[9] ISO/IEC. (2005). *Estandar Internacional 27001 - Primera edición .*

Planificar
En esta fase se define actividades susceptibles de mejora e identifican los objetivos a alcanzar, procesos y procedimientos del SGSI relevantes para mejorar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.

Hacer
En esta fase se debe implementar un plan de tratamiento de riesgos, operar políticas y controles, procesos y procedimientos y la definición de métricas que permitan evaluar la eficacia de los procesos implantados.

Comprobar
En el transcurso de esta fase se aplica diversos tipos de revisiones las cuales miden el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia.

Mejorar
Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna del SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo.

La norma ISO /IEC 27001 tiene 11 dominios de controles que cubre todos los rincones de una empresa donde debe existir seguridad de la información, los dominios están divididos en 39 objetivos de control que comprende 133 controles de seguridad.
Se seleccionan los controles para definir un SGSI que aplique a la corporación autónoma de la frontera nororiental "CORPONOR" territorial Ocaña los cuales se encuentran en el Anexo A de la norma ISO/IEC 27001.

Fases para un sistema de gestión de seguridad de la información[10]

- Requerimientos Generales
- Establecer y manejar el SGSI
- Implementar y operar el SGSI
- Monitorear y revisar el SGSI
- Mantener y mejor el SGSI

[10] ISO/IEC. (2005). *Estandar Internacional 27001 - Primera edición .*

Responsabilidad de la Gerencia

- Compromisos de la gerencia; Debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI.
- Gestión de recursos

Auditorías Internas SGSI

La organización debe realizar auditorías internas SGSI a intervalos planeados para determinar los objetivos de control, controles, procesos y procedimientos del SGSI que cumplan;

- Los requerimientos del estándar ISO/IEC 27001.
- Los requerimientos de seguridad de la información identificados.
- Se implementen y mantenga de manera efectiva.
- Se realice conforme a lo esperado.

Revisión gerencial del SGSI

- General: La gerencia debe revisar el SGSI de la organización a intervalos planeados (por lo menos 1 vez al año) para asegurarse de su continua idoneidad, conveniencia y efectividad.
- Insumos de la revisión.
- Resultados de la revisión.

Mejoramiento del SGSI

- Mejoramiento continúo.
- Acción correctiva.
- Acción preventiva.

4.2.2 ISO/IEC 27002

El ISO/IEC 27002, también conocido como ISO 17799, es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

El objetivo de la norma ISO/IEC 27002 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

Se trata de una norma no certificable, pero que recoge la relación de controles a aplicar para establecer un SGSI.

Para el desarrollo de la Política de Seguridad de la Información base del SGSI, se seleccionó la norma ISO/IEC 27002, porque es un marco de trabajo de mejores prácticas internacionales que establece las guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la organización. Sus objetivos de control y controles son recomendados para cubrir los requerimientos de seguridad que han salido de una evaluación de riesgos.

Estructura del estándar:

El ISO/IEC 27002 contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales. Se detallan las diferentes cláusulas con sus categorías y los objetivos que persiguen cada una de ellas:

1. Política de Seguridad
    - Política de seguridad de la información. Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

2. Organización de la Seguridad de la Información
    - Organización interna. Manejar la seguridad de la información dentro de la organización.
    - Grupos o personas externas. Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados o manejados por, grupos externos.

3. Gestión de Activos
    - Responsabilidad por los activos. Lograr y mantener una apropiada protección de los activos organizacionales.
    - Clasificación de la información. Asegurar que la información reciba un nivel de protección apropiado.

4. Seguridad de Recursos Humanos
    - Antes del empleo. Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, y reducir el riesgo de robo, fraude y mal uso de los medios.

- Durante el empleo. Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.
- Finalización o cambio de empleo. Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada.

5. Seguridad Física y Ambiental
- Áreas seguras. Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.
- Equipo de seguridad. Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

6. Gestión de Comunicaciones y Operaciones
- Procedimientos y responsabilidades operacionales. Asegurar la operación correcta y segura de los medios de procesamiento de la información.
- Gestión de la entrega del servicio de terceros. Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.
- Planificación y aceptación del sistema. Minimizar el riesgo de fallos en el sistema.
- Protección contra el código malicioso y móvil. Proteger la integridad del software y la integración.
- Copia de Seguridad. Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.
- Gestión de seguridad de la red. Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
- Gestión de medios. Evitar la divulgación no-autorizada, la modificación, eliminación o destrucción de activos y la interrupción de las actividades comerciales.
- Intercambio de información. Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa.
- Servicios de comercio electrónico. Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.
- Monitorización. Detectar las actividades de procesamiento de información no autorizadas.

7. Control de Acceso

- Requerimiento del negocio para el control del acceso. Controlar el acceso a la información.
- Gestión de acceso del usuario. Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.
- Responsabilidades del usuario. Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.
- Control de acceso a la red. Evitar el acceso no autorizado a los servicios de la red.
- Control del acceso al sistema operativo. Evitar el acceso no autorizado a los sistemas operativos.
- Control de acceso a la aplicación y la información. Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.
- Computación y tele-trabajo móvil. Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móvil.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- Requerimientos de seguridad de los sistemas de información. Garantizar que la seguridad sea una parte integral de los sistemas de información.
- Procesamiento correcto en las aplicaciones. Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.
- Controles criptográficos. Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.
- Seguridad de los archivos del sistema. Garantizar la seguridad de los archivos del sistema.
- Seguridad en los procesos de desarrollo y soporte. Mantener la seguridad del software y la información del sistema de aplicación.
- Gestión de la Vulnerabilidad Técnica. Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

9. Gestión de Incidentes de Seguridad de la Información

- Informe de los eventos y debilidades de la seguridad de la información. Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

- Gestión de los incidentes y mejoras en la seguridad de la información. Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

10. Gestión de la Continuidad Comercial
    - Aspectos de la seguridad de la información de la gestión de la continuidad del negocio. Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallos importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

11. Cumplimiento
    - Cumplimiento de los requerimientos legales. Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.
    - Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico. Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.
    - Consideraciones de auditoría de los sistemas de información. Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

4.3 DOCUMENTAR FORMALMENTE LAS ACTIVIDADES Y POLÍTICAS REQUERIDAS PARA GESTIONAR ADECUADAMENTE LA SEGURIDAD DE LA INFORMACIÓN EN LA OFICINA DE CONTROL Y VIGILANCIA EN LA CORPORACIÓN

Posterior a las fases de diagnóstico e identificación de los estándares pertinentes para la planeación del Sistema de Gestión de la Seguridad de la Información se procedió a documentar formalmente los elementos requeridos para condensar en una política el resultado de la presente propuesta. Dicho documento se encuentra como anexo al presente proyecto, y cuenta con la aprobación de la dirección territorial de la Corporación.

ALCANCE DEL SGSI

El Sistema de Gestión para la Seguridad de la Información para la Corporación autónoma de la frontera nororiental "CORPONOR" territorial Ocaña aplica a la oficina de control y vigilancia, y a todos sus trabajadores. La corporación reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la misma.

Se hace necesario el establecimiento de las políticas de seguridad de la información que protejan, preserven y administren correctamente la información de la oficina de Control y Vigilancia de CORPONOR Territorial Ocaña, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

CONCLUSIONES

Las niveles actuales de inseguridad informática en las organizaciones de carácter público y privado no son diferentes a los que se presenten en la corporación, lo cual pudo evidenciarse en una serie de auditorías realizadas durante el último año; dichas auditorías se realizaron tanto a las personas y procesos de gestión de la información, como a los componentes técnicos y tecnológicos involucrados en dicha gestión. Partiendo de los hallazgos de las auditorias se procedió a realizar una investigación que abordo la planeación de un Sistema para la Gestión de la Seguridad de la Información

La investigación realizada permitió construir un instrumento para contribuir en la preservación de la seguridad de la información gestionada al interior de la Corporación Autónoma de la frontera nororiental "CORPONOR" territorial Ocaña, para esto se propusieron tres fases. En la primera fase se pudo hacer un modelado del negocio y un diagnóstico real de los riesgos, las vulnerabilidades y las amenazas que afectan la infraestructura tecnológica y los sistemas de información con los que trabaja la corporación.

Para formular de adecuadamente un Sistema de Gestión de Seguridad de la Información (SGSI) se realizó un trabajo comparativo entre los dos estándares internacionales pertinentes: NTC-ISO/IEC 27001 y NTC-ISO/IEC 27002. Con esto se pudo determinar que la 27001 proporciona un modelo para establecer, implementar, operar, monitorear, revisar y mejorar un Sistema de Gestión de Seguridad de la Información, proporcionando adicionalmente, un anexo con el listado de los dominios, los objetivos de control y los controles; la 27002 ofrece un conjunto de recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. A partir de estos referentes y teniendo en cuenta el Ciclo de Deming, se trabajó en la Planeación del Sistema de Gestión de Seguridad de la Información para CORPONOR Ocaña, incluyendo la Política de Seguridad.

BIBLIOGRAFÍA

CORLETTI, ALEJANDRO. ISO/IEC 27001. Los Controles – 2006 [en línea]. http://www.kriptopolis.org/iso-27001-los-controles-parte-II

R. KAPLAN y D. NORTON. (2001). Cuadro de Mando Integral. Ed. Gestión 2000.

FRED R. DAVID, (2003). Conceptos de Administración Estratégica. Ed. Pearson Educación. México.

COBIT**,** *GovernanceInstitute Modelo ExecutiveSummary.* [Versión electrónica] Extraído el 20 de Diciembre, 2008, desde http://www.isaca.org/cobit.html, 2003.

COBIT 4.0, *Governance IT*. Extraído el 3 de Enero, 2009 del sitio Web del Institute, Borrad briefingon TI governance: http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/ContentManagement/ContentDisplay.cfm, 2006.

GESTIÓN DEL SGSI CON LA HERRAMIENTA – Soluciones de Seguridad [en línea]. http://www.siainternational.com/noticias/sgsi.pdf

INTERNATIONAL ORGANIZATIÓN FOR STANDARIZATION. ISO/IEC 27001:2005 [en línea]. http://www.iso.org/iso/home/search.htm?qt=iso+27001&published=on&active_tab=standards&sort_by=rel

M. SANTANA. *Developing an inter-enterprise alignment maturity model: research challenges and solutions*.Technical Report TR-CTIT-07-29, Centre for Telematics and Information Technology, University of Twente, Enschede.Extraído el 7 de mayo de 2007 desde http://eprints.eemcs.utwente.nl/9780/01/Research_challenges_(REPORT).pdf

T, VELASQUEZ, Establecimiento De Criterios De Gobernabilidad De Ti En Las Empresas Colombianas. Universidad de los Andes.Mérida. Venezuela. 2010.

ANEXOS

ANEXO A. HALLAZGOS PRODUCTO DE LAS AUDITORÍAS REALIZADAS EN SITIO.

AUDITOR	DESCRIPCIÓN
Auditor 1	Verificar controles que sirvan para la toma de decisiones
FACTOR	**SEGURIDAD FÍSICA**
SUBFACTOR	**ACCESO FÍSICO**
PRUEBAS	1. Acceso físico de personal no autorizado 2. Verificar que se lleve una Bitácora de control de acceso al cuarto de telecomunicaciones
TIPO DE PRUEBAS	Sustantivas
CONTROLES	- No existen avisos que indiquen que el acceso al cuarto es restringido. - No hay vigilancia que evite el acceso al cuarto.
HALLAZGOS	- El cuarto de telecomunicaciones no cuenta con ningún mecanismo de control que regule el acceso físico de los usuarios a las instalaciones del mismo. - La puerta del cuarto de telecomunicaciones no ofrece mayor seguridad ya que no posee un mecanismo de cierre seguro. - Se verificó la no existencia de una bitácora en la cuál se registre el personal que ingresa al cuarto de telecomunicaciones - La ubicación del cuarto de telecomunicaciones no es la adecuada, ya que está ubicada en el baño de la dirección territorial.
EVIDENCIA	EV_01 EV_02
RECOMENDACIONES	- Colocar avisos visibles lo cual indiquen que el acceso al

	cuarto es restringido o sólo puede pasar personal autorizado - Llevar una Bitácora en la cual se registre el personal que ingresa al área, la fecha, la hora y el motivo por el cual accede al cuarto. - Cambiar la cerradura a la puerta del cuarto por una que sea más segura. -Buscarle otra ubicación al cuarto de comunicaciones, ya que esta representa un peligro para los dispositivos que se encuentran en el cuarto de telecomunicaciones.

ANEXO B. ASIGNACIÓN DE PROYECTOS Y FUNCIONES DE LOS PARTICIPANTES

NOMBRE DEL PROYECTO	OBJETIVO DEL PROYECTO	ACTIVIDADES
Proyecto 2. **Control de la calidad del recurso hídrico** **GUSTAVO CASTILLA**	Controlar la calidad de agua de las fuentes hídricas del Departamento Norte de Santander, mediante el cumplimiento de los Objetivos de Calidad establecidos por la Corporación, el monitoreo del recurso y la inversión en proyectos de descontaminación hídrica.	Seguimiento de de los Planes de Saneamiento y Manejo de Vertimientos PSMV en cuanto al avance físico de las actividades e inversiones programadas dentro del mismo y la caracterización de Vertimientos y de la fuente receptora, para verificar la meta individual de reducción de la carga contaminante. Revisión de los Planes de Saneamiento y Manejo de Vertimientos PSMV
		Monitoreo de la calidad del recurso hídrico
		Evaluación y ejecución de proyectos de inversión en descontaminación hídrica
NOMBRE DEL PROYECTO	**OBJETIVO DEL PROYECTO**	**ACTIVIDADES**
Proyecto 4. **Control ambiental de residuos Sólidos** **GUSTAVO CASTILLA**	Realizar el seguimiento ambiental a la disposición final adecuada de los residuos sólidos de los municipios	Visitas de seguimiento ambiental elaboración de informes, sobre la disposición final de residuos sólidos en rellenos sanitarios con licencia ambiental.

		Administración, Construcción y producción de la información estadística e indicadores, de residuos sólidos dispuestos.
	Realizar el seguimiento a los PGIRS de los municipios.	Visitas de verificación y obtención de información y datos, así como la elaboración de informes sobre el desarrollo, avance y estado de los compromisos ambientales establecidos y acordados en los PGIRS.
	Realizar la identificación y registro de los generadores de residuos peligrosos, así como la captura, consolidación y manejo de la información de RESPEL.	Registro de generadores de RESPEL. Captura y consolidación de la información de residuos hospitalarios y similares. Construcción de un censo de generadores de RESPEL. Producción de la información estadística.
NOMBRE DEL PROYECTO	**OBJETIVO DEL PROYECTO**	**ACTIVIDADES**

Proyecto 22 **Evaluación, Control y seguimiento a licencias, permisos y autorizaciones ambientales** **GISELLE ECHAVEZ**	Dar cumplimiento a las funciones de seguimiento y control establecidas en la ley 99 de 1993 y decretos reglamentarios durante un periodo de tiempo especifico	Realizar el seguimiento a Licencias Ambientales, Permisos de Concesión de Aguas, Permisos de Ocupación de Cauce, Permisos de Vertimiento, registro de Guías Ambientales, registro de empresas e industrias forestales. Asimismo, verificar el cumplimiento de las obligaciones establecidas en los actos administrativos otorgados por la Corporación.
NOMBRE DEL PROYECTO	OBJETIVO DEL PROYECTO	**ACTIVIDADES**
Proyecto 9. Apoyo a la Gestión Integral del Riesgo en los entes territoriales y adaptación al cambio climático **JUAN CARLOS RODRIGUEZ OSORIO**	El proyecto consiste en la asesoría, apoyo y acompañamiento a los entes territoriales en la planificación territorial y gestión del riesgo de desastres	Cumplimiento a la Gestión integral del riesgo de desastres Ley 1523 de 2012. Art.31; Ley 99 de 1993, art. 31-numeral 23 y Art. 121 Ley 388 de 1997 y sus Decretos reglamentarios
Subproyecto 9.1. Apoyo a las labores de gestión del riesgo y ordenamiento territorial		Acompañamiento y apoyo a los Entes Territoriales en los procesos de Gestión Integral del Riesgo que corresponden a la sostenibilidad ambiental del territorio

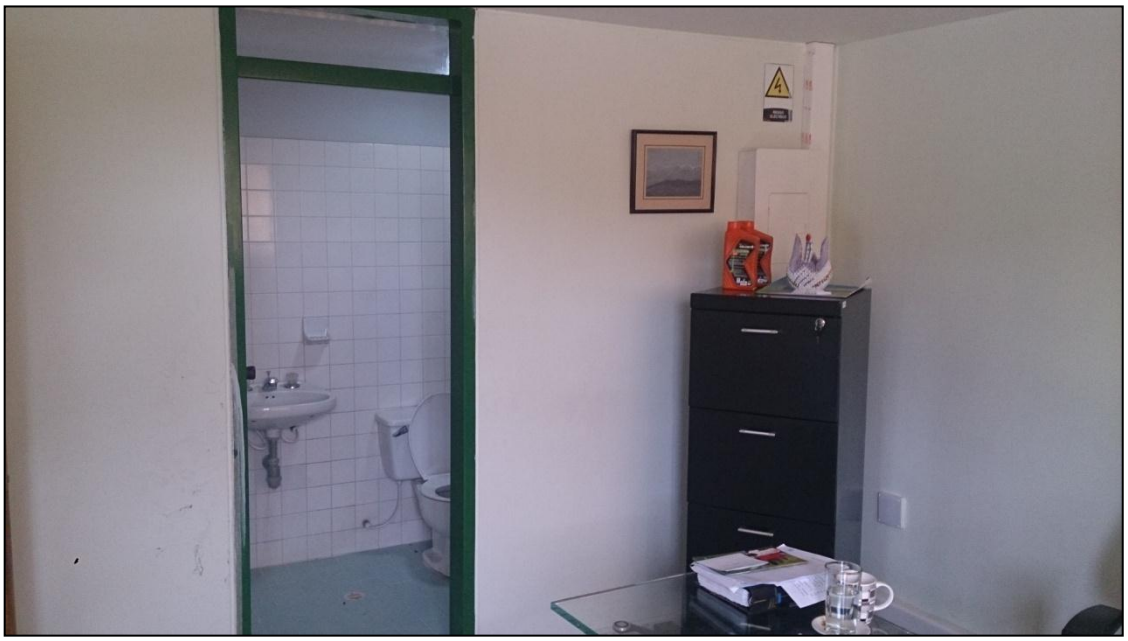
Subproyecto 9.3 Apoyo a las labores de gestión del riesgo en materia de incendios forestales		Revisar periódicamente el cumplimiento de los determinantes ambientales en los POTs y los programas asociados a la gestión del riesgo y del medioambiente
		Realización de eventos (Talleres, reuniones) Realizar visitas de seguimiento y acompañamiento.
		Implementación de medidas estructurales para la reducción del riesgo de desastres
		Acompañamiento a los entes municipales para la preparación y conformación de personal Voluntario especializado en la Prevención, control y mitigación de los Incendios Forestales. Coordinación con los municipios y los organismos de Socorro en caso de evento que se presenten.

		Atención a los eventos o incidentes, por atentado a la Infraestructura petrolera

ANEXO C. EVIDENCIA FOTOGRÁFICA RECOPILADA EN LAS AUDITORÍAS

EVIDENCIA 1. Seguridad acceso al cuarto

Entrada dirección territorial



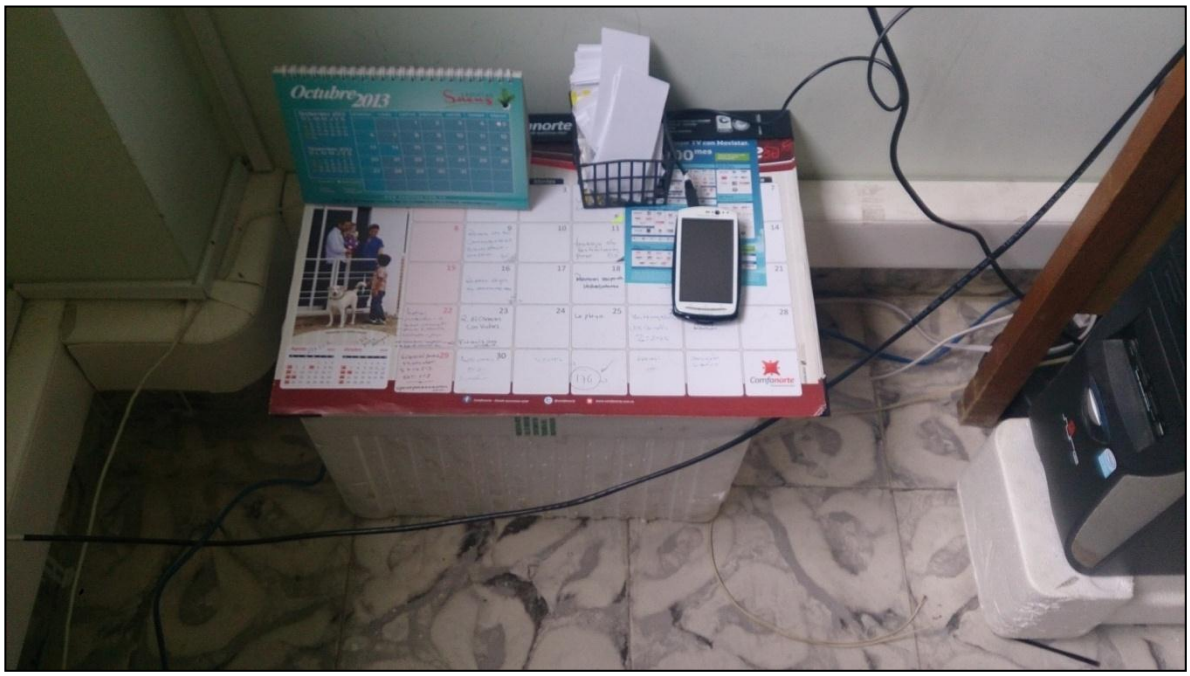
Entrada cuarto de comunicaciones

EVIDENCIA 2: Ubicación Equipos

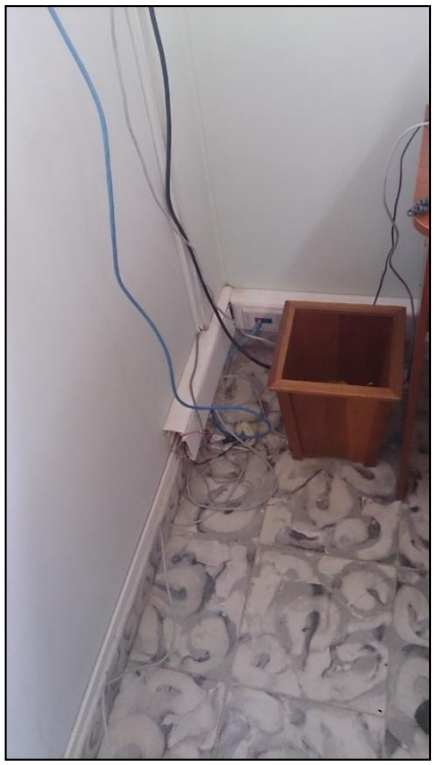
Ubicación Rack

EVIDENCIA 3. Acceso al cuarto de comunicaciones

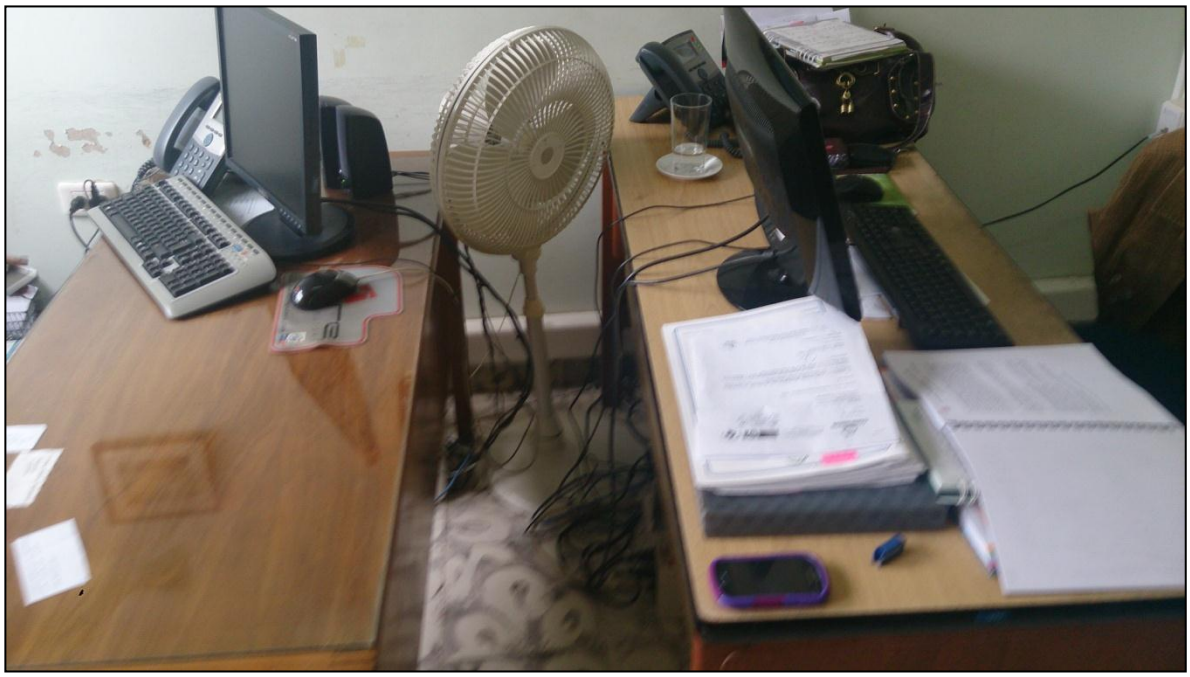
EVIDENCIA 4. Cableado expuesto



Cableado área control y vigilancia



EVIDENCIA 5. Orden y limpieza



Área de control y vigilancia

ANEXO D.

POLÍTICA PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA CORPORACIÓN AUTONOMA DE LA FRONTERA NORORIENTAL "CORPONOR" TERRITORIAL OCAÑA

TERMINOS Y CONDICIONES DE USO
VERSIÓN: 1.0
FECHA: Julio de 2014
Documento elaborado por:
Gustavo Castilla Vergel
Giselle Echavez Casadiegos
Juan Carlos Rodríguez Osorio
Diana Marcela Sandoval Sanjuán

1. INTRODUCCIÓN

1.1 GENERALIDADES

La Corporación ha experimentado un desarrollo en el ámbito tecnológico importante, razón por la cual se cuenta con sistemas de información que soportan de manera efectiva las actividades clave de los procesos misionales. La corporación es consciente de la importancia de la información, y por ello la reconoce como un activo muy valioso. El crecimiento en la infraestructura de TI/SI permite que se administre la información de dichos procesos de acuerdo a los requerimientos actuales de agilidad y precisión; por esta razón y teniendo en cuenta que en la actualidad existen múltiples vulnerabilidades y amenazas asociadas al almacenamiento y procesamiento de la información, se hace relevante contar con una política que establezca los principios que deben guiar a las personas que interactúan de todas las formas con la información de la Corporación.

1.2 ALCANCE DE LA POLÍTICA

La presente política se elaboró teniendo en cuenta un análisis de los riesgos a los que se encuentre expuesta la corporación. La dirección territorial acoge esta política como un aporte en materia de seguridad de la información, de acuerdo a su compromiso con la calidad y la mejora continua.

La corporación reconoce que la información es un activo valioso y que se requieren políticas adecuadas de seguridad. Esta política de Seguridad de la Información se formuló teniendo como base para la Corporación autónoma de la frontera nororiental "CORPONOR" territorial Ocaña aplica a la oficina de control y vigilancia, y a todos sus trabajadores.

Se hace necesario el establecimiento de las políticas de seguridad de la información que protejan, preserven y administren correctamente la información de la oficina de Control y Vigilancia de CORPONOR Territorial Ocaña, junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

2. CONCEPTUALIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como el aseguramiento y cumplimiento de las siguientes características de la información:

• **Confidencialidad**: los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.

• **Integridad**: El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones deben ser registradas asegurando su confiabilidad.

• **Disponibilidad**: Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios con los permisos adecuados.

Otras características también importantes son:

•**Autenticidad**: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.

• **Posibilidad de Auditoría**: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

• **No repudio**: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.

• **Confiabilidad**: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad y autenticidad.

3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El propósito es proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.

Teniendo esto en cuenta, el Comité de Seguridad de la Información de la oficina de Control y Vigilancia de CORPONOR Territorial Ocaña, estará integrado por:
- Director Territorial (Coordinador del Comité de Seguridad de la Información)
- Ingeniero de Sistemas (Responsable de los sistemas de información)
- Jefe del Área de Control y Vigilancia (Responsable de los procesos misionales)
- Asesor en Seguridad de la información (Encargado del control interno – auditoría de sistemas)

Los integrantes del Comité velarán por el cumplimiento de los siguientes objetivos de seguridad:

- Revisar el estado general de la seguridad de la información periódicamente.
- Inspeccionar y monitorear los incidentes de seguridad de la información.
- Dar cumplimiento a las políticas de seguridad que se hayan establecido.
- Revisar, analizar y aprobar los proyectos de seguridad de la información.
- Aprobar las modificaciones o nuevas políticas de seguridad de la información que se quieran implementar.
- Realizar análisis de riesgos a los sistemas de información que se manejan.
- Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.

3.1 ROLES: FUNCIONES Y RESPONSABILIDADES

A continuación se enumeran los roles que intervienen en el Comité de Seguridad de la Información del Área de Control y Vigilancia.

Coordinador del Comité de Seguridad de la Información. Será el responsable de coordinar las acciones del Comité así como de impulsar la implementación y cumplimiento de la presente Política. Este rol recae sobre el Director Territorial de la Corporación.

Responsable de Sistemas de Información.
Cumplirá funciones relativas a la seguridad de los sistemas de información utilizados, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios usados en ésta. Este rol es desempeñado por el Ingeniero de Sistemas.

Responsable de los procesos Misionales:
Garantizar que de acuerdo al presupuesto para la Corporación en las vigencias anuales, quede bien repartido entre los rubros presupuestales asignados en la institución, organiza los estados financieros de la Corporación y garantiza los estados de los resultados financieros. Este rol es desempeñado por el Jefe del Área de Control y Vigilancia.

Responsable del Área de Recursos Humanos.
Pertenece al Comité de Seguridad de la Información y cumplirá la función de implicar a todo el personal del Área de control y vigilancia de la corporación en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los empleados y de la capacitación continua de los mismos en materia de seguridad. Este rol es desempeñado por el Jefe de Recursos Humanos.

4. GESTIÓN DE ACTIVOS

Se debe lograr y mantener la protección apropiada de los activos organizacionales, para esto, cada área, bajo supervisión del Comité de Seguridad de la Información debe elaborar y mantener un inventario de los activos de información que poseen.

Controles:

- Se identificarán los activos importantes asociados al SISPRO, SIPJ, CID, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 2 meses.

- Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

- Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información: Copia, Almacenamiento, Transmisión por (correo, fax, correo electrónico), Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, entre otros).

5. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Orientadas a reducir los riesgos de error humano, comisión de ilícitos contra el Área de Control y Vigilancia de la Corporación uso inadecuado de instalaciones, el Comité de Seguridad documentará las funciones de seguridad de los empleados y las Responsabilidades con respecto a la seguridad de la información.

Controles:

- El Comité de Seguridad desarrollará planes de capacitación de Seguridad de la Información, los cuales se realizarán periódicamente, mínimo una capacitación por semestre.

- Cuando un empleado se retire del Área de Control y Vigilancia, el Ingeniero de Sistemas eliminará el usuario correspondiente a dicho empleado y debe hacer entrega del inventario de activos a su cargo.

- Como parte de sus términos y condiciones iniciales de empleo, los empleados firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del área de Control y Vigilancia.

- Todos los empleados del Área de Control y Vigilancia y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la misma, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimiento.

- Los empleados del Área de Control y Vigilancia, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Ingeniero de Sistemas.

6. SEGURIDAD FÍSICA Y DEL ENTORNO

Para el acceso a los sitios y áreas restringidas a la Corporación, debe notificarse para la autorización correspondiente, y así proteger la información y los bienes informáticos, muebles e inmuebles y demás elementos.

Controles:

- La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas al Área de Control y Vigilancia.

- Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Jefe del Área de Control y Vigilancia, a fin de permitir el acceso sólo al personal autorizado.

- Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad.

- Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, para el personal que trabaja en el Área de Control y Vigilancia, así como para las actividades de terceros que tengan lugar allí.

- El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

- El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

- El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

- Disponer de pólizas de protección de equipos actualizadas.

- El Comité de Seguridad, establecerá un plan de mantenimiento preventivo para los equipos y velará por el cumplimiento del mismo.

- El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Corporación será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Jefe del Área de Control y Vigilancia.

- La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento; medios de almacenamiento conteniendo material sensible.

- Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

- El equipamiento, la información y el software no serán retirados del Área sin autorización formal. Se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos.

7. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Los usuarios y funcionarios deben proteger la información utilizada en la infraestructura tecnológica del Área de Control y Vigilancia. De igual forma, deberán proteger la información reservada o confidencial que por necesidades de la empresa deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna a otras dependencias o redes externas como internet.

Controles:

- Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Ingeniero de Sistemas.

- El Ingeniero de Sistemas controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan.

- Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

- Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

- El Jefe del Área de Control y Vigilancia y el Ingeniero de Sistemas sugerirán criterios de aprobación de nuevos sistemas de información para el Área de Control y Vigilancia, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

- El Ingeniero de Sistemas o su delegado, instalará antivirus en equipos de procesamiento de información del Área de Control y Vigilancia para actualizaciones diarias.

- El Jefe del Área de Control y Vigilancia desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones del Área de Control y Vigilancia, que permita tomar medidas correctivas.

- El Ingeniero de Sistemas monitoreará permanentemente el tráfico de la red para detectar actividades inusuales o detrimento en el desempeño de la red.

- El Comité de Seguridad de la Información garantizará la comunicación del Área de Control y Vigilancia con las demás Áreas mediante la existencia de líneas de respaldo.

- El Jefe del Área de Control y Vigilancia, elaborará copias de seguridad diarias a los sistemas (SISPRO, SIPJ, CID) y las guardará en sitios bajo llave. Es recomendable que las copias de seguridad se almacenen también en un lugar externo a la Corporación para prevenir pérdida de datos en el caso de destrucción de la misma.

- El Jefe del Área de Control y Vigilancia o su delegado revisará semanalmente las copias de seguridad y llevará un registro de dicho procedimiento.

- Todo equipo de TI debe ser revisado, registrado y aprobado por el Ingeniero de Sistemas antes de conectarse a cualquier nodo de la red de comunicaciones, así mismo, desconectará aquellos dispositivos que no estén aprobados y reportar tal conexión como un incidente de seguridad a ser investigado.

- No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la ley 23 de 1982 y su modificación, la ley 44 de 1993 y la Decisión 351 de 1993. Ver la normatividad en la página:www.cecolda.org.co/index.php/derecho-de-autor/normas-y-jurisprudencia/normas-nacionales

- Las instalaciones de software deben ser aprobadas por el Ingeniero de Sistemas y en el caso de encontrarse software ilegal en el Área de Control y Vigilancia, será reportado como incidente de seguridad y posteriormente investigado.

- El Jefe del Área de Control y Vigilancia, con la asistencia del Ingeniero de Sistemas, implementará procedimientos para la administración de medios informáticos removibles, USB, CD´s, DVD e informes impresos y la eliminación segura de los mismos.

- Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

- El Comité de Seguridad Informática garantizará la protección contra la piratería y robo de información.

8. CONTROL DE ACCESO

En un sistema informático resulta de vital importancia, restringir los accesos y garantizar la adecuada utilización de los recursos informáticos.
Cada usuario y funcionario son responsables de los mecanismos de control de acceso que le sean proporcionados.

Controles:

- Corresponde al Ingeniero de Sistemas elaborar, mantener y publicar los documentos de servicios de red que ofrece la Corporación a todos los empleados y usuarios.

- El Ingeniero de Sistemas elaborará, mantendrá y publicará los procedimientos de administración de cuentas de usuario para el uso de servicios de la red.

- El Jefe de Recursos Humanos deberá comunicar al Ingeniero de Sistemas la relación de funcionarios públicos que hayan ingresado a laborar y de los que han dejado de hacerlo, para la activación o desactivación de los usuarios de los sistemas (SISPRO, SIPJ, CID) respectivas.

- El Ingeniero de Sistemas definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a los Sistemas (SISPRO, SIPJ, CID); se limitará y controlará la asignación y uso de privilegios.

- El Ingeniero de Sistemas o su delegado, configurará alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataque e intentos de intrusión.

- Las contraseñas serán cambiadas periódicamente y suministradas al Ingeniero de Sistemas, cada vez que se haga el cambio.

- Los empleados del Área de Control y Vigilancia deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

- El Ingeniero de Sistemas, conjuntamente con el Jefe del Área de Control y Vigilancia, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

- El Ingeniero de Sistemas debe coordinar con el Jefe de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas del Área de Control y Vigilancia, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

- Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto.

- El Ingeniero de Sistemas junto con el Jefe del Área de Control y Vigilancia realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

- Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

- Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los empleados del Área de Control y Vigilancia sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

- El proceso de autenticación al Software de la Corporación debe ser el adecuado, máximo tres intentos para una autenticación satisfactoria, después de éste número de intentos, se deshabilitará el ingreso de usuario.

- El acceso a los recursos de TI institucionales deben estar restringidos según los perfiles de usuario definidos por el Comité de Seguridad de la Información.

9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y Software de Base de Datos que integren el Área de Control y Vigilancia deben tener inmersos controles de seguridad de la información.

Controles:

- Las empresas con las cuales se realicen adquisiciones de software, deben tener reconocimiento a nivel nacional.

- Las aplicaciones contarán con el Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al Ingeniero de Sistemas, la revisión de incidentes en el manejo de las aplicaciones.

- Se debe llevar una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó.

- Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo: Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles; control de conciliación de cuentas para asegurar el procesamiento de todos los datos, provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información; procedimientos para responder a las pruebas de validación de salidas, definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

- Se garantizará que las actividades de soporte a los Sistemas SISPRO, SIPJ, CID se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

- Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

10. GESTIÓN DE INCIDENTES Y DE LA CONTINUIDAD DEL NEGOCIO

Una adecuada gestión de incidentes le permitirá al Área de Control y Vigilancia: responder a los incidentes de manera sistemática, eficiente y rápida; volver a la normalidad en poco tiempo, perder muy poca información; realizar continuamente mejoras en la gestión y tratamiento de incidentes; generar un Base de conocimientos sobre Incidentes; evitar en lo posible, incidentes repetitivos.

- El Ingeniero de Sistemas ante una incidencia, debe comunicarlo al Comité de Seguridad de la Información y diligenciará un formato donde quede consignados los datos de reporte del incidente y de la persona que reportó:

Reportes de Incidencias de seguridad informática.

REPORTE DE INCIDENTES
Datos del reporte de incidencia • Número • Fecha • Hora • Descripción del incidente • Efectos Producidos • Responsable del activo afectado • Causas del incidente (se diligencia, una vez se recupere la normalidad del proceso afectado)
Datos del reportante: • Nombre • Cargo • Dependencia • Correo

- Todos los empleados del Área de Control y Vigilancia, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos.

- Una vez verificada la incidencia, el Ingeniero de Sistemas recolectará la información que le permitirá determinar el alcance del incidente, qué redes y que sistemas y aplicaciones fueron afectados, y que fue lo que generó el incidente, como ocurrió o está ocurriendo, también nos permite saber que originó el hecho, cómo ocurrió y las herramientas utilizadas, qué vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la Corporación.

Para determinar el alcance, el Ingeniero de Sistemas puede hacerse las siguientes preguntas:

- ¿Cuántos equipos fueron comprometidos?
- ¿Cuántas redes se vieron envueltas?
- Hasta qué punto de la red logró penetrar el atacante?
- ¿Qué nivel de privilegio logró el atacante?
- ¿Qué es lo que está en riesgo?
- ¿Cómo impacta en las actividades de la Corporación y en particular el Área de Control y Vigilancia?
- ¿Se encuentran en riesgo aplicaciones críticas?

- ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
- ¿Hay otros equipos con la misma vulnerabilidad?

- Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información.

- Determinado el alcance del incidente de seguridad, el Ingeniero de Sistemas procederá a la contención, respuesta y puesta en marcha de las operaciones afectadas por el incidente.

La **contención,** evitará que el incidente siga produciendo daños. La **erradicación** eliminará la causa del incidente y todo rastro de los daños y la **recuperación**, consiste en volver el entorno afectado a su estado original.
Para llevar a cabo estas acciones, se tendrán que contar con estrategias que permitan realizar las operaciones de manera organizada, rápida y efectiva.

Para contar con una buena estrategia tengamos en cuenta estos agentes:

- Daño potencial de recursos a causa del incidente
- Necesidad de preservación de evidencia
- Tiempo y recursos necesarios para poner en práctica la estrategia
- Efectividad de la estrategia total o parcialmente
- Duración de las medidas a tomar
- Criticidad de los sistemas afectados
- Características de los posibles atacantes
- Si el incidente es de conocimiento público
- Pérdida económica
- Posibles implicancias legales
- Relación costo-beneficio de la estrategia
- Experiencias anteriores

- El Ingeniero de Sistemas, una vez neutralizado el incidente, procederá a investigar las causas de dicho incidente. Las causas se registrarán en el formato de reporte de incidentes.

La recolección de información cuando se investigan las causas debe respetar los siguientes puntos:
- **AUTENTICIDAD**: Quien haya recolectado la evidencia debe poder probar que es auténtica.
- **CADENA DE CUSTODIA**: Registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

- **VALIDACION**: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **CUMPLIMIENTO**

Todo uso y seguimiento de la seguridad de la información en el Área de Control y Vigilancia de la Corporación debe estar de acuerdo a las normas así como a la legislación nacional en la materia, incluido, pero no restringido a:

CONSTITUCIÓN POLÍTICA DE COLOMBIA:

Artículo. 61.- El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.
Ley 23 de 1982 Establece los derechos de autor.
Ley 1266 de 2008 (Habeas_Data)
Ley 1273 Delitos Informáticos
Ley 1581 Protección_Datos_Personales
Ley 488 de 1998 Se elimina el ajuste integral por inflación fiscal para los inventarios, ingresos, costos y gastos. Por expresa disposición del artículo 14 de la mencionada ley, estos cambios tienen efectos contables.
Plan único de cuentas
Decreto 2193 aplicativo SIHO
Normas de auditoría generalmente aceptadas NAGA
Decreto 2193 del MDPS
ISO 27002: Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable.