Capítulo 1 INTRODUCCIÓN

La Empresa Colombiana de Productos Veterinarios S.A. – VECOL S.A. (en adelante VECOL S.A. o la Empresa) tiene la responsabilidad de contar con un direccionamiento estratégico en materia de Seguridad de la Información. El desarrollo de este Manual de Seguridad y Privacidad de la Información le permitirá a la Empresa tomar decisiones más ágiles y acertadas frente a los riesgos y las regulaciones, permitiendo una gestión oportuna y efectiva aprovechando de la mejor forma los recursos con que cuenta.

La referencia principal para el desarrollo de este Manual de Seguridad y Privacidad de la Información es la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información, y la Guía Técnica Colombiana GTC-ISO-IEC 27002:2013, Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

1.1. CONTEXTO DE LA ORGANIZACIÓN.

1.1.1. CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO.

VECOL S.A., es una sociedad de economía mixta cuyo objeto es promover y estimular el incremento de la producción agropecuaria y sus insumos, así como el mejoramiento de la salud humana y animal, mediante la producción, venta, comercialización, importación, exportación e investigación científica de productos biotecnológicos, químicos, farmacéuticos, agrícolas e industriales.

MISIÓN

Somos una empresa con enfoque global, que brinda soluciones integrales para promover la sanidad animal y la productividad del sector agropecuario.

VISIÓN

Ser una empresa de clase mundial reconocida por ser el mejor aliado de nuestro campo.

1.1.2. COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS.

VECOL S.A. con el fin de dar cumplimiento a los lineamientos establecidos en la Política de Gobierno Digital, anteriormente llamada Estrategia de Gobierno en Línea, y atender estos nuevos requisitos, orientados a la prestación de servicios de calidad, que generen competitividad a la Empresa y que administren los riesgos cambiantes en el ámbito de la gestión de la información y de las nuevas tecnologías de información y comunicación, ha decidido establecer, implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), que busque mediante una mejora continua, preservar la Confidencialidad, Integridad y Disponibilidad de los activos de información en los procesos Estratégicos, Operacionales, de Apoyo y Control.

1.2. GENERALIDADES

1.2.1. PLANIFICACIÓN Y CONTROL OPERACIONAL

Para la planificación y control operacional del Sistema de Gestión de Seguridad de la Información (SGSI) se consideran los requisitos aplicables establecidos en la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información, y la Guía Técnica Colombiana GTC-ISO-IEC 27002:2013. Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.

Se desarrollan procedimientos, instructivos y controles de Seguridad de la Información basados en la NTC-ISO-IEC 27001:2013 y en la GTC-ISO-IEC 27002:2013.

Para cumplir los requisitos relativos a Planificación de cambios en el Sistema de Gestión de Seguridad de la Información (SGSI), la Empresa considera y aplica en caso necesario las actividades apropiadas dentro de la siguiente lista:

- Política General y específicas.
- Objetivo general y específicos.
- Alcance.
- Estructura de la organización.
- Sistematización.
- Adecuación de área físicas.
- Cambios tecnológicos.
- Controles requeridos por los clientes.
- Cambios en la reglamentación NTC-ISO-IEC 27001:2013 y GTC-ISO-IEC 27002:2013.
- Subcontratación de actividades y cualquier cambio que se considere impacte al SGSI.

Cualquier cambio que pueda tener impacto en el SGSI y sus anexos deben documentarse y controlarse según lo establece el PRO-GC1-024 “Planificación de cambios del Sistema de Gestión de Calidad”.

1.2.2. RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN.

Dentro de las tareas para el establecimiento e implementación del Sistema de Gestión de Seguridad de la Información (SGSI), VECOL S.A. hace una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades. En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

Para que VECOL S.A. pueda tomar decisiones sobre cómo actuar ante los diferentes riesgos de Seguridad de la Información, la Empresa hace una valoración de riesgos para determinar cuáles son los más críticos. Esta valoración se hace en términos de la probabilidad de ocurrencia del riesgo y del impacto que tenga la materialización del riesgo, finalmente la Empresa realiza el tratamiento del riesgo verificando si se debe evitar, reducir, compartir o transferir, o asumir, de acuerdo con su criticidad.

Con el fin de cumplir con el análisis de riesgo y una gestión continua, La Empresa define una metodología para la gestión de riesgos de Seguridad de la Información, mediante la construcción del documento **Anexo 1**. “Identificación, Análisis y Tratamiento de Riesgos de Seguridad de la Información”.

1.2.3. OBJETIVO GENERAL

Establecer lineamientos de seguridad de alto nivel que permitan que los activos de información de propiedad de VECOL S.A. sean accedidos sólo por las personas autorizadas que tienen necesidad legítima para la realización de las funciones propias del negocio (confidencialidad), que no se realicen modificaciones no autorizadas y salvaguardar su exactitud y completitud (integridad), y que estén disponibles cuando éstos sean requeridos para el desarrollo de las actividades propias del negocio (disponibilidad); alineados con la misión, visión, objetivos estratégicos y valores corporativos de la Empresa.

1.2.4. OBJETIVOS ESPECÍFICOS

- Establecer los fundamentos para el Sistema de Gestión de Seguridad de la Información (SGSI).
- Proteger la imagen, los intereses y el buen nombre de VECOL S.A.
- Reducir el nivel de riesgo en seguridad de la información.
- Implementar y ejecutar controles efectivos que velen por la Seguridad de la Información.
- Establecer los canales de comunicación que le permitan a la Presidencia de la Empresa mantenerse informada de los riesgos y uso inadecuado de los activos de información y las acciones tomadas para su mitigación y corrección.
- Promover una cultura organizacional orientada a la Seguridad de la Información.
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.
- Definir la conducta esperada en el acceso, uso y manejo de los activos de información.
- Propender por la disponibilidad de los activos de información, servicios e infraestructura tecnológica.
- Asegurar la continuidad de la Seguridad de la Información, permitiendo el cumplimiento de los objetivos estratégicos de la Empresa.
- Propender por el uso de las tecnologías de información y comunicación de manera segura.
- Fortalecer los controles que aseguren la Confidencialidad, Integridad y Disponibilidad de la información de la Empresa.
- Garantizar una adecuada y permanente gestión de riesgos del manejo en Seguridad de la Información.
- Fortalecer la cultura en Seguridad de la Información para los usuarios internos y externos, respecto al SGSI.

1.3. ALCANCE

“VECOL S.A. establece e implementa el Sistema de Gestión de Seguridad de la Información, el cual busca proteger la Confidencialidad, Integridad y Disponibilidad de los activos de información para los procesos: “Estratégicos, Operacionales, Apoyo y Control”, en la sede principal de Bogotá D.C. y las bodegas de despacho que VECOL S.A. administre, el cual exige el cumplimiento de la política general y políticas específicas de Seguridad de la Información, controles y procedimientos que aplican a todas las partes interesadas del SGSI. Cuenta con el apoyo de la Alta Gerencia para mantener y mejorar continuamente el SGSI, basado en la gestión de riesgos definida por la Empresa incluido dentro del contexto.”

1.4. NORMATIVIDAD APLICABLE

- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos, 2013-12-11, ICONTEC Internacional.
- Guía Técnica Colombiana GTC-ISO-IEC 27002:2013, Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información, ICONTEC Internacional.

1.5. DEFINICIONES

Activo: Se denomina activo a aquel conjunto de bienes tangibles o intangibles que posee la Empresa. Así mismo, se considera activos a aquellos bienes que en el futuro tienen una importante probabilidad de convertirse en un real beneficio económico, la información es el activo más valioso de la Empresa.

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Empresa y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Documento en el que los trabajadores de VECOL S.A. o terceros se obligan a mantener la confidencialidad de la información, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Alta Gerencia: La Alta Gerencia está conformada por todos los reportes directos al Presidente de la sociedad. Son el soporte del Presidente y se encargan de liderar y direccionar la sociedad con el fin de asegurar su sostenibilidad, rentabilidad y viabilizar el cumplimiento de la estrategia.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de Confidencialidad, Integridad y Disponibilidad de la información.

Áreas seguras: Son sitios en los que se maneja información sensible o valiosos equipos informáticos refugio y el personal para conseguir los objetivos de negocio. En el contexto de la seguridad física, el término “sitio” significa edificios, habitaciones u oficinas que albergan todos los servicios e instalaciones. La función principal de la seguridad física es proteger los activos de información de amenazas físicas: el acceso no autorizado, las indisponibilidades y los perjuicios causados por la acción humana, además de eventos ambientales perjudiciales.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autenticación Fuerte: Es una manera de asegurar que la persona que se identifica en un sistema es realmente quien dice ser comprobando su identidad.

Centro de cómputo: Es el espacio físico donde están alojados los equipos de datos y comunicaciones, al igual desde donde se inicia la distribución del cableado a las distintas oficinas. Deben cumplir requisitos adecuados de acceso físico, pisos, techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Código Malicioso: Es código informático que provoca infracciones de seguridad para dañar un sistema informático. Se trata de un tipo de amenaza que no siempre puede bloquearse con un software antivirus por sí solo.

Confidencialidad de la Información: Acceso a la información por parte únicamente de quienes estén autorizados. Es una característica o propiedad por la que la información no está disponible o revelada a individuos, empresas, o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de un software, una obra literaria, artística o científica, publicada o que todavía no se haya publicado.

Disponibilidad de la Información: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una empresa autorizada.

Dispositivos de almacenamiento externo: Cualquier formato de almacenamiento de datos que no está fijo de modo permanente dentro del equipo. Las ventajas residen en su facilidad de transporte derivadas de su rápido acceso, larga vida útil, poco tamaño y peso. Algunos ejemplos son Disco Duro externo, memorias USB, entre otros.

Dueño de la información: Es el responsable de la información que genera o utiliza en las actividades de su proceso.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Estudio de Confiabilidad y Credibilidad: Es una herramienta para la mitigación de riesgos que permite complementar los resultados de los procesos de selección de personal que se realizan al interior de cada empresa. Así mismo, puede ser utilizado para complementar investigaciones en casos de robos, fraude, extorsión, contaminación de mercancías y otros hechos delictivos. El Estudio de Confiabilidad Personal consta de varios servicios de análisis. Se recomienda su uso completo, aunque cada servicio también puede ser utilizado individualmente. Ejemplos: Verificación de Referencias Laborales, Visitas Domiciliarias, entre otros.

Etiquetado: Identificación del tipo de calificación que se le da a la información, en dado caso que la información no esté etiquetado se entiende que es información pública.

Evento de Seguridad: Ocurrencia de una situación que indica una posible violación a las políticas de seguridad de la información o fallas en los controles que no genere un impacto en el desarrollo de las operaciones de la Empresa y que puede ser controlado rápidamente.

Factor de Autenticación: Se trata de una medida de seguridad. Cuando se habla de autenticación multifactor combina dos o más credenciales independientes: lo que sabe el usuario (contraseña), lo que tiene el usuario (token de seguridad) y lo que es el usuario (verificación biométrica).

Firewall Personal: Es un programa que funciona en su computador de forma permanente. El programa monitoriza las conexiones que entran y salen de su computador y es capaz de distinguir las que son legítimas de las realizadas por atacantes. En este segundo caso, las bloquea y notifica al usuario del computador.

Gabinete: Armario metálico cerrado donde se encuentra ubicado todo lo referente a telecomunicaciones switch, Modem, hubs entre otros, de allí se envía el cableado al resto de la estructura para crear los puntos de trabajo.

GEL: Gobierno en Línea.

Hacking ético: Conjunto de actividades para ingresar a las redes de datos y voz de la Empresa con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intención maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: Ocurrencia de un acto intencional o no intencional que tiene una alta probabilidad de afectar el buen funcionamiento de los sistemas de información, que a causa de este acto se vea afectada la operación de la Empresa y que por lo tanto amenaza la seguridad de la información.

Ingeniería Social: Se refiere al arte de manipular personas para eludir los sistemas de seguridad. Esta técnica consiste en obtener información de los usuarios por teléfono, correo electrónico, correo tradicional o contacto directo. Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador, entre otros.

Integridad de la Información: Propiedad que busca mantener los datos libres de modificaciones no autorizadas y salvaguardar la exactitud y completitud de los activos.

Licencia de software: Contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluye cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

No Repudio: Sirve a los emisores o a los receptores para no poder negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

Perfiles de usuario: Grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Privacidad: El derecho de individuos y organizaciones para controlar la recolección, almacenamiento y diseminación de información acerca de ellos mismos.

Procedimientos: Documentos que contienen las instrucciones detalladas y las responsabilidades de las personas involucradas en la realización de operaciones o actividades y pueden generar registros que se utilizan como complemento de la documentación.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Rack: Es un término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico. Se trata de un armazón metálico que, de acuerdo a sus características, sirve para alojar una computadora, un router u otra clase de equipo.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red) estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de VECOL S.A.

Registros de Auditoría: Archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Empresa. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Requisitos de Seguridad: Lineamientos que debe cumplir a nivel de seguridad de la información o seguridad informática, algún producto, sistema de información o servicio.

Responsable por el activo de información: Es la persona o grupo de personas encargadas de velar por la Confidencialidad, la Integridad y Disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una

pérdida o daño en un activo de información.

Sanitización: En el manejo de información confidencial o sensible, es el proceso lógico y/o físico mediante el cual se remueve información considerada sensible o confidencial de un medio ya sea físico o magnético, ya sea con el objeto de desclasificarlo, reutilizar el medio o destruir el medio en el cual se encuentra.

Seguridad de la Información: Tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada, sin importar en el medio o formato en el que se encuentren.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por VECOL S.A. o de origen externo, ya sea adquirido por la Empresa como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Teletrabajo: Actividad laboral que se desarrolla fuera de las instalaciones de la Empresa, apelando a las tecnologías de la información y de la comunicación para el desarrollo de las actividades propias de la Empresa. Por lo tanto, el teletrabajo es el trabajo que se realiza a distancia equipado con un computador con conexión a Internet. Para el caso del presente manual el concepto Teletrabajo no tiene el alcance completo definido en la Ley 1221 de 2008 que incluye trabajo desde el hogar del trabajador ni de la ley 2088 de 2021 que regula el trabajo en casa.

Usuarios: Incluye tanto internos como externos y otros grupos, donde los usuarios externos se refieren a clientes mayoristas, clientes minoristas, gremios y asociaciones, usuario final, Entidades del Estado Nacionales e Internacionales, accionistas, y proveedores. Mientras que los usuarios internos se refieren a trabajadores activos, temporales, practicantes del SENA y Universitarios, trabajadores pensionados y retirados, así como de cualquier otro que por su actividad tenga acceso a información de la compañía. También otros grupos como accionistas y proveedores.

Vulnerabilidades: Son las debilidades, huecos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la empresa (amenazas), las cuales se constituyen en fuentes de riesgo.

1.6. PRINCIPIOS

A continuación, se establecen los principios de Seguridad de la Información que soportan el SGSI de VECOL S.A.:

- Las responsabilidades frente a la Seguridad de la Información son definidas, compartidas,

publicadas por la Alta Gerencia, y aceptadas por cada uno de los usuarios internos y externos.

- VECOL S.A. protege:
  - ✔ Que la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a cada uno de los usuarios internos y externos.
  - ✔ Que la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso indebido de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
  - ✔ Que las instalaciones de procesamiento de información y la infraestructura tecnológica que soporta sus procesos críticos estén actualizados.
- VECOL S.A. procurará mantener la plataforma tecnológica actualizada según la planeación estratégica de la Empresa.
- VECOL S.A. deberá implementar controles de acceso a los activos de información.
- VECOL S.A. incorpora la seguridad como parte integral del ciclo de vida de los sistemas de información, a través de una adecuada gestión de riesgos.
- VECOL S.A. propende:
  - ✔ Por la disponibilidad de sus procesos de negocio y la continuidad de sus servicios, con base en el impacto que pueden generar los incidentes de seguridad de la información.
  - ✔ Por el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

COMPROMISO DE LA ALTA GERENCIA

La Alta Gerencia de VECOL S.A., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Empresa y el fortalecimiento de los procesos Estratégicos, Operacionales y de Apoyo y Control.

La Alta Gerencia de VECOL S.A. está comprometida con el desarrollo y la implementación de políticas de Seguridad de la Información, así como de su mejora continua, mediante:

- La autorización para la implementación de Políticas de Seguridad de la Información en VECOL S.A.
- La aprobación de Políticas de Seguridad de la Información.
- El suministro de los recursos necesarios para una adecuada implementación de Políticas de Seguridad de la Información y el SGSI.
- La comunicación a los usuarios internos y externos de la importancia de las Políticas de Seguridad de la Información para el logro de los objetivos de Seguridad de la Información.

Este Manual de Seguridad y Privacidad de la Información está fundamentado en la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información, y la Guía Técnica Colombiana GTC-ISO-IEC 27002:2013, Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información, que recopila las mejores prácticas, para suministrar lineamientos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Sistema de Gestión de Seguridad de

la Información (SGSI), y este es influenciado por las necesidades y objetivos, los requisitos de seguridad, los procesos y el tamaño y estructura de la Empresa, además persigue preservar la Confidencialidad, Integridad, Disponibilidad y privacidad de la información, brindando confianza a las partes interesadas acerca de la adecuada gestión de la Información de la Empresa.

Todas las actividades realizadas por usuarios internos y externos de VECOL S.A. están bajo el control del Sistema de Gestión de Seguridad de la Información (SGSI), que se somete de forma regular y sistemática a auditorías internas al Sistema de Gestión, con el fin de asegurar su eficacia.

El presente Manual de Seguridad y Privacidad de la Información está a disposición de todos los usuarios internos y externos de la Empresa para servir de guía en las actividades referentes a la Seguridad de la Información.

La Presidencia aprueba el contenido de este Manual y lo declara de obligatorio cumplimiento en todos los procesos de la Empresa.

1.7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de Seguridad de la Información entre los usuarios internos y externos de VECOL S.A. Por tal razón, es necesario que las violaciones al Sistema de Gestión de Seguridad de la Información (SGSI), se analicen teniendo en cuenta las diferentes disposiciones legales que apliquen en la materia, con el objetivo de aplicar las medidas correctivas que legalmente procedan y así mitigar posibles afectaciones contra la Seguridad de la Información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

1.8. REVISIÓN POR LA DIRECCIÓN.

El Comité Institucional de Gestión y Desempeño revisa anualmente el desempeño, eficacia y eficiencia del Sistema de Gestión de Seguridad de la Información (SGSI), así como el cumplimiento de las políticas y objetivos de Seguridad de la Información, según lo establece el procedimiento de “Revisión del sistema de gestión de calidad”, PRO-PO0-002. Para efectuar dichas revisiones, el Comité Institucional de Gestión y Desempeño cuenta con la asistencia del Director del Departamento de T.I., quien es el responsable de la preparación de los elementos de entrada necesarios para efectuar la revisión y se definió la siguiente información:

- **a.** Estado de las acciones con relación a las revisiones previas por la Dirección.
- **b.** Los cambios que podrían afectar al Sistemas de Gestión de Seguridad de la Información (SGSI).
- **c.** Desempeño de la Seguridad de la Información referente a:
  - No conformidades y acciones correctivas.
  - Seguimiento y resultados de las mediciones.
  - Resultados de auditorías internas y externas del SGSI.
  - Cumplimiento de la Política General y los objetivos específicos de Seguridad de la Información.
- **d.** Resultados de la valoración de riesgos y el estado del plan de tratamiento de riesgos.
- **e.** Oportunidades de mejora continua.

Los resultados de la revisión por la dirección se documentan y registran en un acta FVC-PO0-420 “Acta revisión por la dirección”. El Comité Institucional de Gestión y Desempeño delega en el Director de Aseguramiento de Calidad y Jefe de sección de Aseguramiento de Calidad, el seguimiento de las acciones correctivas y preventivas, oportunidades de mejora continua y cualquier necesidad de cambio en el SGSI, requeridas como resultado de la revisión por la dirección para garantizar que el Sistema de Gestión de Seguridad de la Información esté funcionando acorde con las Políticas y Objetivos de Seguridad de la Información de la Empresa.

1.9. MEJORA.

1.9.1. NO CONFORMIDADES Y ACCIONES CORRECTIVAS.

VECOL S.A., cuando ocurra una no conformidad:

- **a.** Toma acciones para controlarla y corregirla
- **b.** Evalúa la necesidad de acciones para eliminar las causas de la no conformidad, de tal manera que no vuelva a ocurrir.
  - Identifica la no conformidad
  - Hace una revisión de la no conformidad
  - Realiza la determinación de las causas de la no conformidad
  - Realiza la determinación de si existen no conformidades
- **c.** Implementa acciones necesarias
- **d.** Revisa la eficacia de las acciones tomadas
- **e.** Hace cambios al SGSI si es necesario
- **f.** Documenta la información relacionada con las causas y las acciones realizadas de la no conformidad.

Con el fin de garantizar la solución y evitar la recurrencia o prevenir las no conformidades, se procede de acuerdo con lo descrito en el PRO-GC1-014 “Acciones correctivas y preventivas”.

1.9.2. MEJORA CONTINUA.

VECOL S.A. debe mejorar continuamente la conveniencia, adecuación y eficacia del SGSI. Se realizan capacitaciones a todo el personal para garantizar la actualización en el desarrollo del talento humano en temas de Seguridad de la Información, y mantiene un seguimiento permanente a las acciones correctivas y preventivas.

Capítulo 2 GESTIÓN DEL MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1. PRESENTACIÓN DEL MANUAL

El Manual de Seguridad y Privacidad de la Información de VECOL S.A. establece las buenas prácticas en materia de Seguridad de la Información, con el fin de dar cumplimiento a la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información. Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, y la Guía Técnica Colombiana GTC-ISO-IEC 27002:2013, Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información, y está constituido por cuatro capítulos de los cuales el primero hace referencia a las generalidades, el segundo hace referencia a la gestión del manual, el tercero hace referencia a la organización interna y el cuarto hace referencia a la política general y políticas específicas de Seguridad de la Información.

El Manual de Seguridad y Privacidad de la Información, aplica a todos los procesos Estratégicos, Operacionales y los de Apoyo y Control de la Empresa y por lo tanto es de obligatorio cumplimiento por todos los colaboradores.

2.2. ELABORACIÓN, REVISIÓN Y APROBACIÓN

La elaboración del Manual de Seguridad y Privacidad de la Información está a cargo del Departamento de Tecnologías de Información (TI). Como evidencia firma el Director de T.I. (Tecnologías de la Información).

El Manual de Seguridad y Privacidad de la Información se elabora siguiendo los lineamientos que se encuentran en el PRO-GC1-001 “Clasificación y Presentación de Documentos”

La revisión del Manual de Seguridad y Privacidad de la Información se hace por parte del Comité Institucional de Gestión y Desempeño, la firma de revisión será por parte del líder de éste. La revisión del Manual de Seguridad y Privacidad de la Información es llevada a cabo para verificar que haya consistencia entre lo descrito en este y lo que se hace.

Es responsabilidad del Presidente de VECOL S.A. aprobar el Manual de Seguridad y Privacidad de la Información.

1.1. DISTRIBUCIÓN

El jefe de sección de Aseguramiento de Calidad es el responsable de la generación y distribución de las copias electrónicas y/o digitales del Manual de Seguridad y Privacidad de la Información. Estas copias se encuentran en las áreas de la dirección de Aseguramiento de Calidad, Presidencia e Informática, el original es conservado en la Jefatura de Aseguramiento de Calidad.

También se puede consultar en el sitio dispuesto del Sistema de Gestión de Calidad.

1.2. CONTROL DE CAMBIOS

Para asegurar la continua adecuación del Manual de Seguridad y Privacidad de la Información este se revisa y/o modifica, según se requiera o si no se han suscitado cambios, se revisa completamente cada 3 años.
Los cambios en el Manual de Seguridad y Privacidad de la Información pueden ser generados por modificaciones significativas en la organización, cambio del reglamento interno o de sus estatutos generales que pueden ser aplicables para el desarrollo de sus actividades o por el cambio del modelo referencial, implantación de nuevas normas o requisitos, cambios en el Sistema de Gestión de Seguridad de la Información (SGSI) tales como el alcance.

Todo usuario que desee introducir cambios en el Manual de Seguridad y Privacidad de la Información debe comunicar al Comité Institucional de Gestión y Desempeño o el que haga sus funciones, para analizar conjuntamente la magnitud o trascendencia del cambio. Para registrar los cambios generados al Manual de Seguridad y Privacidad de la Información, deberá presentar la solicitud al Grupo de Trabajo de Arquitectura Empresarial mediante la Mesa de Ayuda Técnica del Departamento de T.I.

Capítulo 3 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

3.1. ORGANIZACIÓN INTERNA

A nivel interno, se tiene estructurada la organización que permite iniciar y controlar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en VECOL S.A., esto es posible estableciendo una adecuada comunicación para que el Presidente pueda aprobar los lineamientos de Seguridad de la Información, asignando responsabilidades y coordinando la implementación de la seguridad en todos los niveles de la Empresa.

Es por esto que se definen los roles y responsabilidades que deben participar en la oportuna y efectiva gestión del SGSI, los cuales se describen a continuación, así:

ALTA GERENCIA: Es responsabilidad:

- Designar al Líder de Seguridad de la Información de la Empresa.
- Revisar el Sistema de Gestión de Seguridad de la Información (SGSI) de la Empresa.

COMITÉ INSTITUCIONAL DE GESTIÒN Y DESEMPEÑO: Este comité es responsable del liderazgo, planeación e impulso de la política de Gobierno Digital en la Empresa y conforme al Manual de Gobierno Corporativo de la Empresa será creado mediante Resolución de Presidencia.

El Comité Institucional de Gestión y Desempeño dentro de sus responsabilidades incluye los siguientes referentes al Sistema de Gestión de Seguridad de la Información (SGSI), así:

- Definir los lineamientos y las estrategias de Seguridad de la Información en función de la misión y visión de la Empresa.
- Revisar las Políticas de Seguridad de la Información de la Empresa.
- Revisar el Plan de Acción del proceso de Gestión de Seguridad de la Información de la Empresa.
- Revisar las estrategias del Programa de Concientización en Seguridad de la Información.
- Fomentar el desarrollo de la Seguridad de la Información en la Empresa.
- Velar por un seguimiento y que se cumplan los lineamientos de Seguridad de la Información.
- Ejercer un control gerencial del plan de Seguridad de la Información y tomar las acciones correctivas respecto a aquellos que no estén acordes con el Plan de Seguridad de la Información.
- Verificar la efectividad de los Programas de Seguridad de la Información en la Empresa.
- Velar que el Líder de Seguridad de la Información o quien haga sus veces diseñe, desarrolle, ejecute y controle un Programa de Seguridad de la Información ajustado a la Empresa.

LÍDER DE SEGURIDAD DE LA INFORMACIÓN (o quien haga sus veces): Corresponde al líder del Grupo de Trabajo de Arquitectura Empresarial. Es responsable del diseño, desarrollo, implantación, mantenimiento y verificación del correcto funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI), en línea con los requerimientos del negocio y bajo las directrices del Comité Institucional de Gestión y Desempeño, entre sus responsabilidades de seguridad de la información, están:

- Verificar que todos los riesgos a los que pudiera estar sometida la información en la Empresa estén identificados, evaluados, actualizados y mitigados.
- Verificar el crecimiento del nivel de Seguridad de la Información por medio del análisis de los indicadores de gestión del proceso de seguridad de la Información, así como tomar acciones correctivas en caso de ser requerido.
- Analizar integralmente los riesgos de la información de la Empresa
- Mantener informado al dueño de la Información de los riesgos de Seguridad de la Información identificados en su área, así como diseñar los planes de acción para mitigarlos.
- Diseñar, desarrollar, implantar y controlar el proceso de Seguridad de la Información con indicadores de gestión claros, objetivos y verificables.
- Implantar los lineamientos de Seguridad de la Información definidos por medio del diseño, desarrollo, implantación, mantenimiento y control de un Sistema de Gestión de Seguridad de la Información.
- Someter a revisión y socialización ante el Comité Institucional de Gestión y Desempeño, el Plan de proyectos y el Programa que implementa el Sistema de Gestión de Seguridad de la Información (SGSI) en la Empresa.
- Definir la Arquitectura de Seguridad de Información en línea con la arquitectura de tecnología de la Empresa.
- Desarrollar, implantar y controlar el procedimiento de gestión de Incidentes de Seguridad de Información.
- Definir los lineamientos y las directrices de Seguridad de la Información a ser incluidas en el Plan de Contingencias.
- Proveer asesoría en materia de Seguridad de la Información al Comité Institucional de Gestión y Desempeño y a las distintas unidades funcionales de la Empresa.
- Verificar que el Sistema de Gestión de Seguridad de la Información (SGSI) esté incluido en el ciclo de vida de una aplicación o sistema.
- Ponderar la relación costo-beneficio entre la implantación de Proyectos de Seguridad de la Información y el riesgo asumido.
- Impulsar el mejoramiento continuo del Proceso de Seguridad de la Información en la Empresa.
- Desarrollar, implantar y controlar el programa de clasificación de la información para la Empresa.

ADMINISTRADOR DE SEGURIDAD INFORMÁTICA: Corresponde al Departamento de Tecnologías de la Información (T.I.). Se encargará de toda la gestión de infraestructura de seguridad informática y demás temas que tengan relación con el Departamento de T.I. (Tecnologías Información) , así:

- Administrar las herramientas de Seguridad de la Información de su plataforma de responsabilidad.
- Administrar el nivel de seguridad de las aplicaciones basado en el nivel de acceso que identifique el Responsable de la Información.
- Aplicar los controles de seguridad a los recursos informáticos.
- Monitorear, registrar, resolver e informar los eventos de intrusión o uso malicioso de los recursos informáticos de su responsabilidad y reportarlos al Responsable de la Información y al Líder de Seguridad de la Información.
- Revisar y reportar al Líder de Seguridad de la Información respecto al nivel y consistencia de la seguridad de los recursos informáticos de su responsabilidad.
- Evaluar sus activos de información en términos de riesgo y mantener los estándares de Seguridad de la Información para minimizar dichos riesgos.

- Proveer al Líder de Seguridad de la Información, los datos obtenidos durante el monitoreo de la infraestructura de seguridad.
- Facilitar información que permita resolver incidentes que involucren los recursos informáticos de su responsabilidad.
- Aplicar y mantener los estándares de seguridad de la plataforma tecnológica de la información de la Empresa.
- Apoyar las actividades planteadas en el Plan de Concientización que ayuden a incrementar el nivel de conciencia sobre la importancia de la Seguridad de la Información.
- Suministrar información que permita verificar el cumplimiento de los estándares de configuración.

GERENTE DE RECURSOS HUMANOS: Es responsable de facilitar los mecanismos necesarios para la creación de una cultura organizacional en Seguridad de la Información, entre sus responsabilidades de seguridad de la información, están:

- Implementar el Programa de Concientización.
- Apoyar al Líder de Seguridad de la Información en cuanto a la concientización en el reporte de eventos o incidentes de Seguridad de la Información y evaluación de riesgos.
- Participar en la investigación de las personas que tengan acceso a información crítica sin estar autorizados.
- Fomentar el cumplimiento de las Políticas y procedimientos de Seguridad de la Información en la Empresa.
- Incluir responsabilidades tanto directas como indirectas en cuanto a Seguridad de la Información en los manuales de funciones de los cargos.
- Desarrollar el plan de capacitación del área de Seguridad de la Información.
- Apoyo en la conformación de la organización de Seguridad de la Información de la Empresa.
- Asegurar que en los contratos de trabajo y en el reglamento interno de trabajo, se incluyan responsabilidades de Seguridad de la Información.

SECRETARÍA GENERAL: Es responsable de brindar apoyo y asesoramiento para que el Sistema de Gestión de Seguridad de la Información de la Empresa esté dentro del marco legal correspondiente y cuente con el sustento legal que formalice y haga viable su aplicación. El dueño de la Información y/o el líder de Seguridad deben informar a Secretaría General cuando se presenten incidentes de Seguridad de la Información que puedan resultar en litigios.

Entre sus responsabilidades de seguridad de la información, están:

- Verificar que el Sistema de Gestión de Seguridad de la Información (SGSI) emitido por la Empresa cuente con el sustento legal que permita su formalización, aplicación y obligatorio cumplimiento previa publicación y difusión.
- Asesorar a la Empresa en el cumplimiento de las normas legales locales y/o internacionales de Seguridad de la Información que afecten a la Empresa.
- Atender y resolver las consultas legales que el Líder de Seguridad de la Información, el Comité Institucional de Gestión y Desempeño o el Gerente de Recursos Humanos pudieran hacer en cuanto al proceso de emisión, ajuste y formalización del Sistema de Gestión de Seguridad de Información (SGSI) de la Empresa.
- Alertar al Líder de Seguridad de la Información de la Empresa cuando cambios en la legislación afecten la vigencia o haga necesarios ajustes al Sistema de Gestión de Seguridad de la Información (SGSI) de la Empresa.

- Asesorar al líder de Seguridad de la Información y Auditoría Interna, cuando en una investigación aparezcan situaciones que puedan resultar en un litigio que la comprometa.

USUARIOS INTERNOS Y EXTERNOS DE LA EMPRESA: Son responsables de poner en práctica las políticas, procedimientos y programas oficializados por el proceso de Seguridad de la Información que garanticen la protección de la información del negocio. Entre sus responsabilidades de seguridad de la información, están:

- Identificar los activos de información que sean críticos para el negocio.
- Identificar los problemas y posibles riesgos de la información e informar a los dueños de la información y/o al líder de Seguridad de la información.
- Cumplir las políticas de Seguridad de la Información.
- Clasificar y manejar la información generada de acuerdo con la criticidad definida en el Sistema de Gestión de Seguridad de la Información (SGSI).
- Brindar información y participar en las labores de investigación de incidentes de seguridad de la información.
- Ser agentes de cambio en el proceso de Concientización sobre la importancia de la Seguridad de la Información.
- Generar sugerencias para mejorar el Sistema de Gestión de Seguridad de la Información (SGSI).
- Reportar eventos o incidentes que afecten la seguridad de la información.

DUEÑO DE LA INFORMACIÓN: Debe identificar claramente el valor de su información, conocer los riesgos a que podría estar expuesta y velar porque se provean los mecanismos necesarios para que los riesgos se mitiguen a niveles aceptables considerando la relación costo-beneficio para su área de negocio. Entre sus responsabilidades de Seguridad de la Información, están:

- Identificar los activos de información con sus requerimientos de seguridad.
- Identificar, definir y evaluar los riesgos a que pudiera estar expuesta su información, solicitando asesoría al Líder de Seguridad de la Información.
- Aprobar los riesgos de su información.
- Definir los controles de negocio a implantar para cada riesgo identificado.
- Recomendar posibles ajustes al Sistema de Gestión de Seguridad de la Información (SGSI).
- Apoyar al Equipo Operativo de Trabajo en Seguridad de la Información en la definición de los requerimientos de Seguridad de la Información.
- Mantener un nivel adecuado de conocimiento y conciencia en cuanto a la Seguridad de la Información en su área de negocio.
- Definir los perfiles de los usuarios de los Sistemas de Información, los respectivos privilegios y justificación de negocio para su acceso y uso, e informar al Departamento de T.I. para su implantación.
- Informar sobre los incidentes de Seguridad de la Información que ocurran en su área al líder de Seguridad de la Información.
- Mantener un registro que incluya todo lo referente a riesgos, clasificación de los activos, lista de usuarios e incidentes y acciones correctivas ejecutadas.
- Ejecutar y participar activamente en las actividades planteadas en el plan de Concientización.
- Cumplir con las políticas y procedimientos de Seguridad de la Información.
- Participar en las Auditorias del Sistema de Gestión de Seguridad de la información (SGSI).

Capítulo 4 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

4.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La siguiente es la Política de Seguridad de la Información establecida para VECOL S.A., así:

"La Empresa Colombiana de Productos Veterinarios S.A. – VECOL S.A. reconoce la importancia de identificar y proteger sus activos de información, asegurando su Confidencialidad, Integridad y Disponibilidad, dependiendo su nivel de clasificación, comprometiéndose a establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI)."

Así mismo, VECOL S.A. como Empresa de economía mixta cuyo objeto es promover y estimular el incremento de la producción agropecuaria y sus insumos, así como el mejoramiento de la salud humana y animal, mediante la producción, venta, comercialización, importación, exportación e investigación científica de productos biotecnológicos, químicos, farmacéuticos, agrícolas e industriales, en aras de propender por la seguridad de la información, tiene como finalidad permitir que los activos de información de propiedad de VECOL S.A. reciban los niveles de protección adecuados de acuerdo a su Confidencialidad, Integridad y Disponibilidad.

La Presidencia de VECOL S.A., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos; alineado con el ordenamiento jurídico y normativo en concordancia con la misión, visión, objetivos estratégicos y valores corporativos de la Empresa.

Para VECOL S.A., la protección de la información busca la disminución del impacto generado sobre los activos de información por los riesgos identificados de manera sistemática; con el propósito de mantener un nivel aceptable de exposición que permita responder por la Confidencialidad, Integridad y Disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados. A continuación, se relacionan las políticas específicas que soportan la política general de Seguridad de la Información.

4.2. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

4.2.1. POLÍTICA PARA DISPOSITIVOS MÓVILES

El uso de dispositivos móviles, tales como computadores portátiles (notebooks y laptops), tabletas electrónicas, teléfonos inteligentes - smartphones, unidades de almacenamiento externo y teléfonos móviles, que contengan información de VECOL S.A. y que a su vez se utilicen para el manejo de esta información, deben ser integrados y controlados por una plataforma de administración del Departamento de T.I. de VECOL S.A. para mitigar el impacto a que se expone la información como su pérdida, alteración y divulgación no autorizada. Con el fin de garantizar el cumplimiento de esta política, se establecen los siguientes lineamientos:

4.2.1.1. El Departamento de T.I. debe contar con un inventario actualizado de dispositivos móviles utilizados para almacenar o transmitir información de VECOL S.A.

4.2.1.2. El Departamento de T.I. se reserva el derecho a bloquear de manera temporal o indefinida los servicios instalados en los dispositivos móviles (teléfonos, laptops, tabletas) de los contratistas o trabajadores que utilicen la red de datos y/o servicios corporativos siempre y cuando considere que son un riesgo para los activos de información.

4.2.1.3. Los contratistas y trabajadores que utilicen la red de datos de la Empresa aceptan los parámetros de seguridad corporativos.

4.2.1.4. En los dispositivos móviles que exista información de VECOL S.A., se restringe su conexión a otras redes o servicios que no sean explícitamente autorizados por VECOL S.A.

4.2.1.5. En caso de tener un dispositivo móvil asignado por la Compañía y que tenga fines de traslado, deberá usar la plataforma de almacenamiento en nube que disponga VECOL S.A. en la cuenta asignada para tal fin.

4.2.1.6. Si desde el dispositivo móvil se procesa información, se debe contar con un software instalado y actualizado contra códigos maliciosos, firewall personal y para prevenir intrusos.

4.2.1.7. Estos dispositivos deben contar con un mecanismo de autenticación.

4.2.1.8. La dirección de Comunicaciones debe generar recomendaciones del uso y cuidado de tipo físico, cuando el dispositivo se encuentre fuera de las instalaciones de la Empresa.

4.2.1.9. Cuando desde los dispositivos móviles no se estén usando servicios de conexión inalámbrica se desactivan los protocolos de comunicación mientras no los esté usando.

4.2.1.10. Si desde el equipo móvil se requiere conexión remota a los servicios de información de la red de VECOL S.A., se valida previamente que el dispositivo esté libre de infección y cumple con los demás controles de seguridad activos y actualizados.

4.2.1.11. Los dispositivos móviles que se conecten a la red de la infraestructura tecnológica de VECOL S.A. deben ser previamente autorizados por el Departamento de T.I.

4.2.1.12. Se prohíbe el uso de dispositivos móviles personales que no estén autorizados por el Departamento de T.I. para el manejo, transporte y transmisión de información de la Compañía.

4.2.1.13. Se configuran los dispositivos móviles de tal manera que cualquier aplicación incluyendo los mecanismos de software de seguridad, permanezcan actualizados sin que dependan de conexión directa a la infraestructura tecnológica de VECOL S.A.

4.2.1.14. Los dispositivos móviles cuentan con mecanismos de autenticación para desbloquear el equipo y poder tener acceso a su información y servicios.

4.2.1.15. Periódicamente se deberán realizar copias de respaldo a la información de VECOL S.A. y almacenarla en la nube que la empresa disponga; es responsabilidad de cada usuario la realización de las copias de respaldo, mínimo una vez por semana.

4.2.1.16. En caso de robo o extravío, el Departamento de T.I. debe contar con mecanismos que permitan eliminar el usuario e información remotamente, poder localizar, recuperar o borrar datos que almacenaron en la nube que la Compañía.

4.2.1.17. Al realizar la disposición final o reasignación del dispositivo móvil a otra área con un propósito diferente para el cual estaba designado, se realiza un borrado seguro de toda la información allí almacenada.

4.2.1.18. El acceso al computador portátil estará protegido por una contraseña del dominio de Vecol S.A.

4.2.1.19. Si el usuario no está presente en el dispositivo, éste deberá estar bloqueado o apagado.

4.2.1.20. El computador portátil tiene un mecanismo de anclaje con clave y/o llave que permita asegurarlo a otro elemento fijo de tal manera que no pueda ser hurtado del lugar conectado.

4.2.1.21. Los dispositivos deberán tener solo software legal y autorizado por el Departamento de T.I.

4.2.1.22. Está prohibido tener dispositivos móviles que utilicen la red de datos y/o servicios de Vecol con software de análisis y penetración de redes. Los equipos que usen este tipo de software sin autorización de la Empresa, serán bloqueados por el Departamento de T.I. y los usuarios podrían llegar a tener sanciones contractuales.

4.2.1.23. En cualquier momento el Departamento de T.I. podrá hacer revisión del cumplimiento de la política directamente en los dispositivos móviles, sin previo aviso.

4.2.1.24. Todo equipo móvil que se compre y/o se renueve, deberá contar con el aval técnico obligatorio del Departamento de T.I.

4.2.1.25. Evitar el uso de dispositivos móviles cuyo software (Sistema Operativo) ha sido modificado (jailbreak, rooted, WGA y WAT).

4.2.2. POLÍTICA DE SEGURIDAD DEL TRABAJO EN CASA.

La Empresa protege la información clasificada según lo establecido en sus políticas de “Inventario, Clasificación y Valoración de activos de Información”, a la que tienen acceso los trabajadores desde lugares remotos, por razón y motivo de su cargo, por lo tanto, el acceso a la información fuera de la oficina puede ser permitida si se demuestra que la información requerida es necesaria para el cumplimiento de sus funciones, y que existe un control de acceso dado con autorización previa y controlado por VECOL S.A. Con el fin de garantizar el cumplimiento de esta política, se establecen los siguientes lineamientos.

4.2.2.1. El acceso remoto se puede realizar desde equipos de propiedad de VECOL S.A. y de equipos de propiedad de los trabajadores debidamente autorizados y configurados por el Departamento de T.I., que cumplan con niveles de seguridad aceptables (como mínimo: Sistema Operativo actualizado, con firewall y antivirus actualizado), antes de permitir la conexión remota a los servicios o recursos de la infraestructura tecnológica de VECOL S.A.

4.2.2.2. El Departamento de Tecnologías de la Información (T.I.) debe contar con la administración y control del dispositivo del cual se procesa la información, para evitar accesos no autorizados por personas ajenas a VECOL S.A.

4.2.2.3. Los equipos en los que se realiza trabajo en casa, deben tener protección contra software malicioso, antivirus, cliente de VPN y demás que el Departamento de T.I. establezca como necesario.

4.2.2.4. EL usuario deberá usar su cuenta de las herramientas colaborativas para asegurar toda información en la nube, garantizando el acceso en cualquier momento de la información. Si es indispensable tener una única copia en el dispositivo, deberá garantizar la copia regular a la nube por parte del usuario y así dar la continuidad de las funciones realizadas.

4.2.2.5. Cualquier usuario que requiera conexión remota a los servicios o información de VECOL S.A., deberá ser previamente autorizado por el Departamento de T.I. y avalado por la Dirección de RRHH.

4.2.2.6. La conexión remota a servicios o información de VECOL S.A. se realiza a través de canales de comunicación seguros como redes privadas virtuales (VPN).

4.2.2.7. La administración remota de la infraestructura tecnológica de VECOL S.A. desde equipos conectados a Internet no está permitida, salvo que se cuente con la autorización debidamente sustentada mediante documento escrito y con un mecanismo de control de acceso seguro autorizado por el Director de T.I. o el Jefe de Desarrollo y Nuevas Tecnologías de VECOL S.A.

4.2.2.8. En el esquema de trabajo en casa no se permite almacenar información clasificada ni de uso del cargo en servicios en la nube públicos o híbridos de cuentas personales, deben usarse los mecanismos y servicios que VECOL S.A ponga a disposición del usuario previamente administrados por el Departamento de T.I.

4.2.2.9. El propietario del activo, con el apoyo del Departamento de Tecnologías de la Información (TI), identificará los riesgos potenciales que puede generar el retiro del equipo o medios de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.

4.2.2.10. En caso de pérdida, suplantación o robo de un equipo portátil se debe reportar inmediatamente al Departamento de T.I. para realizar la gestión necesaria y se deberá poner la denuncia ante la autoridad competente, si aplica.

4.2.3. POLÍTICA DE CONTROL DE ACCESO LÓGICO Y FÍSICO

El acceso lógico y físico a los activos de información de VECOL S.A. está restringido de acuerdo a los niveles de clasificación definidos para proteger la información de accesos no autorizados; para esto, la Empresa tiene en cuenta los requisitos de seguridad de los sistemas de información, y la autorización del acceso a la misma, con base en los perfiles y roles definidos. Además, el Departamento de T.I. debe tener implementados controles para las diferentes actividades cuando se requiere: dar acceso a los activos de información, implementar derechos de acceso, cambiar roles o funciones o deshabilitar accesos; así mismo, se debe contar con mecanismos que permiten mantener actualizados los permisos garantizando los mínimos privilegios para el desarrollo de las funciones para todos los usuarios. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.3.1. Dependiendo del nivel de clasificación y criticidad de los activos de información a los cuales se va a brindar acceso, se establecen mecanismos de autenticación de uno, dos o tres factores.

4.2.3.2. Cuando se solicite tener acceso a algún recurso o servicio informático de VECOL S.A., el Departamento de T.I. realizará el correspondiente análisis con el fin de determinar los privilegios a otorgar y definir los mecanismos necesarios para su protección según matrices de acceso y privilegios.

4.2.3.3. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones, o a centros de procesamiento de información crítica, si previamente no han sido autorizados por el Director de T.I. o el Jefe de Desarrollo y Nuevas Tecnologías junto con los dueños del activo.

4.2.3.4. La creación, modificación y baja de usuarios en la infraestructura de procesamiento de información, comunicaciones y seguridad deberá ser solicitada por la mesa de ayuda del Departamento de Tecnologías de la Información (TI) y autorizada por la Dirección de RRHH para poder ser ejecutada según los parámetros de la solicitud.

4.2.3.5. Las asignaciones de privilegios en las aplicaciones para los diferentes usuarios estarán determinadas por la matriz de roles y perfiles de la Gerencia de RRHH.

4.2.3.6. Los cambios a las cuentas privilegiadas como la matriz de roles y perfiles se deben revisar en la Gerencia de RRHH previo informe que enviará el Director de TI.

4.2.3.7. Se cuenta con la separación de las funciones de solicitud, autorización y administración del acceso que deben ser desarrolladas por personas diferentes.

4.2.3.8. Cada Dirección que interviene en el proceso debe contar con los requisitos para la autorización formal de las solicitudes, así como para la revisión periódica de los controles y el retiro de los derechos de acceso a los usuarios.

4.2.3.9. Se establece la regla basada en la premisa "En general, todo está prohibido, a menos que esté expresamente permitido".

4.2.3.10. Se usa una única identificación de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones.

4.2.3.11. Se verifica que el usuario tenga autorización del propietario del sistema para el uso del sistema o servicio de información.

4.2.3.12. Se verifica que el nivel de acceso otorgado sea adecuado para los propósitos y limitado exclusivamente a la información que está autorizado a acceder, y no poner en riesgo la segregación de funciones.

4.2.3.13. Dar a los usuarios una declaración escrita de sus derechos de acceso la cual debe firmar, que indique que ellos conocen, entienden y aceptan cumplir las condiciones del acceso.

4.2.3.14. Se retira o bloquea inmediatamente los derechos de acceso a los usuarios que han dejado de ser parte de VECOL S.A. o modificarlos para aquellos que han cambiado de función.

4.2.3.15. Se incluyen cláusulas en los contratos del personal y de los servicios, que especifiquen las sanciones del personal o los proveedores del servicio, que intenten ingresar a accesos no autorizados.

4.2.3.16. Los privilegios de administración de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red), son asignados exclusivamente a los administradores del sistema designados por el Departamento de Tecnologías de la Información (TI) de VECOL S.A.

4.2.3.17. Los privilegios de administración se asignan a un identificador de usuario (ID) diferente a los utilizados para el uso normal del sistema.

4.2.3.18. Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les suministra de manera segura una contraseña temporal, la cual se forzará a cambiar inmediatamente realice el siguiente ingreso al sistema.

4.2.3.19. Las contraseñas nunca se deben almacenar en sistemas de computador o en otro medio en un formato no protegido.

4.2.3.20. Las contraseñas predeterminadas por el vendedor se cambiarán inmediatamente después de la instalación de los sistemas o del software.

4.2.3.21. Se revisan las autorizaciones para derechos de acceso privilegiado, a intervalos frecuentes, para garantizar que no se tengan privilegios no autorizados o que no correspondan a las funciones del usuario.

4.2.3.22. Recursos Humanos informa a las direcciones y jefaturas que administren accesos físicos y lógicos, de la ausencia de los trabajadores debido a vacaciones, licencias o

incapacidad, para que se les modifique su usuario de manera temporal, mientras no estén ejerciendo sus funciones, a partir de la cantidad de días que determine VECOL S.A.

4.2.3.23. Toda contraseña es personal e intransferible, y cada usuario es responsable de las acciones que se ejecuten con el usuario que se le ha asignado.

4.2.3.24. En caso de que exista sospecha o certeza de que alguna contraseña se ha comprometido, ésta debe ser cambiada de manera inmediata.

4.2.3.25. De acuerdo con los parámetros que están fijados en la documentación de cada sistema de información, todos los usuarios deben cumplir los lineamientos para la construcción de sus contraseñas. Deben estar compuestas de acuerdo a los lineamientos establecidos en el Anexo 2. “Gestión de Acceso”.

4.2.3.26. La protección física se lleva a cabo mediante la creación de diversas barreras o medidas de control físicas, alrededor de las instalaciones de VECOL S.A. y de las instalaciones de procesamiento de información.

4.2.3.27. Para la selección de controles de las áreas protegidas 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.

4.2.3.28. El cableado de energía eléctrica y comunicaciones que transportan voz y datos que brinda apoyo a los servicios de información, deben protegerse contra intercepción o daños.

4.2.3.29. Se garantiza la seguridad física del Centro de Cómputo incluyendo, entre otros, el sistema eléctrico, el control de acceso, el sistema de protección contra incendios y el control de temperatura.

4.2.3.30. Todas las puertas que utilicen sistema de control de acceso, deben permanecer cerradas, y es responsabilidad de todos los empleados y terceros autorizados evitar que las puertas se dejen abiertas.

4.2.3.31. Se exige a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado en cada una de las áreas de VECOL S.A., mientras permanezcan dentro de sus instalaciones.

4.2.3.32. Los visitantes permanecen acompañados de un empleado cuando se encuentren dentro de alguna de las áreas seguras de VECOL S.A.

4.2.3.33. Es responsabilidad de todos los usuarios internos y externos acatar las normas de seguridad y mecanismos de control de acceso a las instalaciones de las áreas de VECOL S.A.

4.2.3.34. Todas las áreas que se hayan definido como protegidas y activos de información que la componen, están protegidas de acceso no autorizado mediante controles y tecnologías de autenticación fuerte.

4.2.3.35. Se mantiene un sistema de información de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y/o servicios.

4.2.3.36. Todo acceso físico a las áreas protegidas, debe estar manejado según los lineamientos definidos por la jefatura de la Sección de Seguridad Industrial y Salud Ocupacional.

4.2.3.37. En las áreas seguras donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:

- 4.2.3.37.1. No se deben consumir alimentos ni bebidas.
- 4.2.3.37.2. No se deben ingresar elementos inflamables.
- 4.2.3.37.3. No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.

4.2.3.37.4. No se permiten tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.

4.2.3.37.5. No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores, a menos que haya una justificación para esto.

4.2.4.POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS.

La política de Seguridad de Controles Criptográficos utiliza controles encaminados a la protección de la información de VECOL S.A. soportado en la realización del análisis de riesgos donde se identifica la información sensible para aplicar estos controles y así garantizar una adecuada protección de la Confidencialidad, Integridad y Disponibilidad de la información. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.4.1. La información digital catalogada como pública reservada y pública clasificada, se debe almacenar y/o transmitir bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad, no obstante, en caso de no poderse aplicar un mecanismo criptográfico, se deberá asignar clave de apertura a los archivos digitales que contengan este tipo de información.

4.2.4.2. Se verifica que todo sistema de información o aplicativo que requiera realizar transmisión de información pública reservada o pública clasificada, cuente con mecanismos de cifrado de datos.

4.2.4.3. Se verifican, desarrollan y establecen mecanismos para el manejo y la administración de llaves de cifrado y estándares para la aplicación de controles criptográficos.

4.2.4.4. Se implementan controles respecto de la administración de claves, recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y reemplazo de las claves de cifrado.

4.2.4.5. Se debe llevar a cabo un análisis y evaluación de riesgos entre el propietario de la Información y el responsable de la Seguridad de la Información.

4.2.4.6. Se utilizan algoritmos de cifrado y tamaños de clave que se consideren seguros. Se verifica esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

4.2.4.7. Se tiene en cuenta los controles aplicables al cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes a criptografía.

4.2.4.8. Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos, estas pueden aplicarse a cualquier tipo de documento que se procesa electrónicamente.

4.2.4.9. Al utilizar firmas y certificados digitales, se debe considerar la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.

4.2.4.10. Todas las claves son protegidas contra modificación y destrucción; y las claves secretas o privadas serán protegidas contra copia o divulgación no autorizada.

4.2.4.11. Se proporcionará una protección adecuada a la infraestructura utilizada para generar, almacenar y archivar claves, considerándola crítica o de alto riesgo.

4.2.4.12. Cuando las claves son comprometidas o cuando un empleado se desvincula de VECOL S.A. se revocan los certificados o firmas digitales.

4.2.4.13. Se registra y audita las actividades relativas a la administración de claves.

4.2.4.14. A fin de reducir la probabilidad de compromiso, las claves tienen fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por un lapso de tiempo definido, no mayor a 12 meses.

4.2.5. POLÍTICA DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN, ESCRITORIO LIMPIO, Y PANTALLA LIMPIA.

La política de Capacitación y Sensibilización en Seguridad de la Información, Escritorio Limpio, y Pantalla Limpia, se centra en formar y dar a conocer a los trabajadores temas relacionados con la Seguridad de la Información, cuya finalidad es que puedan identificar y reportar de manera oportuna los incidentes de seguridad de la información y disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano. Esta gestión está a cargo de la Gerencia de Recursos Humanos. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.5.1. Se provee al personal activo las habilidades requeridas a través de entrenamientos para proteger los sistemas y cumplir con las responsabilidades de administrar de manera oportuna y correcta los dispositivos de seguridad de la información.

4.2.5.2. Se tiene una cultura que promueve la Seguridad de la Información donde todos los trabajadores apliquen los controles de Seguridad de la Información y prevengan que la información sensible de VECOL S.A. se vea comprometida.

4.2.5.3. A partir de los resultados de pruebas de ingeniería social y de análisis de riesgo se debe determinar los temas y las estrategias de sensibilización para reforzar el nivel de conocimiento en temas de Seguridad de la Información para todos los trabajadores.

4.2.5.4. Se tiene definido un mecanismo de inducción en Seguridad de la Información para todos los trabajadores que sean destinados a recibir un nuevo cargo, bien sea por nombramiento, traslado o por disposiciones internas de la Empresa.

4.2.5.5. Se tiene definido un programa de capacitación y sensibilización que de manera periódica refuerzan los conceptos y amenazas de seguridad de la información para que los trabajadores cuenten con información actualizada y sepan cómo actuar ante incidentes y cómo reportarlos.

4.2.5.6. VECOL S.A. destina los recursos suficientes para desarrollar los programas de capacitación y sensibilización.

4.2.5.7. La asistencia a las sesiones de capacitación y sensibilización en seguridad de la información son de carácter obligatorio.

4.2.5.8. Los mensajes de sensibilización de las políticas de Seguridad de la Información, se dan a conocer y entender de manera fácil.

4.2.5.9. Se evalúa a todos los empleados de manera periódica, los niveles de sensibilización en temas de Seguridad de la Información.

4.2.5.10. En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar los medios que contengan información crítica protegida bajo llave.

4.2.5.11. Los usuarios deben guardar bajo llave información crítica cada vez que se retiren de su puesto de trabajo, de tal manera que no quede expuesta y se pueda comprometer su disponibilidad o confidencialidad.

4.2.5.12. Todas las estaciones de trabajo usan únicamente el papel tapiz y el protector de pantalla establecido por VECOL S.A.

4.2.5.13. Al retirarse del puesto de trabajo, los usuarios deben bloquear el equipo de cómputo, para evitar que otras personas puedan acceder a la información:

- Debe pulsar simultáneamente (tecla Windows + la tecla L) para bloquear el equipo o bloqueo de pantalla.
- Pulsar (Ctrl + alt + supr) y seleccionar la opción bloquear equipo.

4.2.5.14. Los empleados son responsables por la custodia y las acciones que se realicen sobre los activos informáticos que le han asignado. Por lo tanto, deben estar presentes en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de software de dichos activos. Cuando se requiera trasladar el equipo informático a otro sitio, se deberá hacer previa autorización del responsable del activo informático.

4.2.5.15. Se definen compromisos y obligaciones por parte del personal que es capacitado en temas de Seguridad de la Información.

4.2.5.16. No se deben dejar en las impresoras documentos expuestos que contengan información sensible, ya que se puede comprometer su confidencialidad.

4.2.5.17. Los usuarios y claves son personales e intransferibles en ese sentido no se pueden “prestar” o facilitar entre compañeros de trabajo, el hacerlo se considera como una falta grave a las obligaciones contractuales.

4.2.6. POLÍTICA DE COPIAS DE RESPALDO.

VECOL S.A. realizará copias de respaldo de la información dando prioridad a la clasificada con mayores niveles de importancia y criticidad basados en lo definido en el Anexo 3. “Inventario, Clasificación y Valoración de activos de Información”. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.6.1. Todo usuario y/o empleado de VECOL S.A. será responsable de tener copia de respaldo de su información, en la herramienta de almacenamiento que se disponga para el alojamiento de la información; dicha copia de respaldo deberá realizarse por lo menos 1 vez cada 15 días.

4.2.6.2. Los usuarios que no tengan conexión y/o entrada a la herramienta nombrada en el ítem anterior, deberán entregar en la misma periodicidad y en medio digital (USB, CD, DD, DVD, etc.) al Departamento de T.I., el backup correspondiente y el Departamento de T.I. realizará el respectivo almacenamiento de la información en la herramienta dispuesta para ello.

4.2.6.3. Cuando se trate de información de respaldo identificada como pública reservada y pública clasificada, debe estar cifrada.

4.2.6.4. Los medios de copias se almacenarán en custodia externa, nube, o cualquier otro que el Departamento de T.I. considere, asegurando disponibilidad y que tenga implementado mecanismos de protección ambiental como detección de humo, fuego, humedad, así como mecanismos de control de acceso físico.

4.2.6.5. Se realizan pruebas de restauración de la información contenida en las copias de respaldo, de acuerdo a un plan de restauración para asegurar que se puede depender de ellas en caso de emergencia si es necesario.

4.2.6.6. Se definen los tiempos de retención de las copias de respaldo, permitiendo minimizar el impacto de la operación de VECOL S.A., en caso de presentarse una falla o desastre y poder contar con la información necesaria en el momento oportuno para responder con los tiempos de restauración de los servicios.

4.2.6.7. Se define la frecuencia y tipo de copias de respaldo a realizar.

4.2.6.8. El Departamento de T.I. garantizará las copias de respaldo de los Servidores asignados al Departamento de T.I.

4.2.7.POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN.

VECOL S.A. Implementa mecanismos y los debidos controles que permitan establecer una comunicación segura en la transferencia de la información evitando la interceptación que pueda copiar, modificar, o eliminar la información por parte de terceros. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.7.1. Todo trabajador de la Empresa con autoridad, que desee conceder permisos de transferencia de información, debe solicitar la autorización al Departamento de Tecnologías de la Información a través de un correo electrónico dirigido al Director del Departamento T.I. con copia al Jefe de Desarrollo y Nuevas Tecnologías. La persona que realiza la solicitud es responsable de la Confidencialidad e Integridad de la misma.

4.2.7.2. Toda información requerida por un área o un tercero, debe ser solicitada directamente al responsable de la misma, siguiendo los conductos regulares, previa autorización de la Secretaría General.

4.2.7.3. Se usan técnicas de cifrado a información sensible para garantizar la Confidencialidad, Integridad y Disponibilidad de la información durante la transferencia de la información.

4.2.7.4. Únicamente se entrega información a receptores autorizados por la Secretaria General, quienes garanticen por escrito la reserva legal y protección de la información que se les vaya a suministrar.

4.2.7.5. Se deberán suscribir Acuerdos de Confidencialidad con los terceros que van a acceder a la información. Para el efecto, el interesado deberá realizar la correspondiente solicitud formal a la Secretaría General para la elaboración o revisión, según sea el caso, del respectivo Acuerdo de Confidencialidad.

4.2.7.6. Cuando proceda, la oficina responsable de dar respuesta legal a un requerimiento de información clasificada, deberá verificar previamente entre otros temas y sin limitarse a:

- 4.2.7.6.1. La solicitud se ajuste a la normatividad aplicable vigente.
- 4.2.7.6.2. La respuesta identifique el nivel de clasificación correspondiente a la naturaleza del documento o la información que se ponga en conocimiento de la autoridad competente.
- 4.2.7.6.3. La respuesta refleja adecuadamente la valoración de la información, el uso de términos condicionales y dubitativos, que garantice entre otros la reserva, el debido proceso, el buen nombre y el derecho a la intimidad.
- 4.2.7.6.4. La respuesta cumple con los protocolos de seguridad, acceso y reserva.
- 4.2.7.6.5. La respuesta con la información suministrada no pone en peligro o riesgo la Seguridad de VECOL S.A.
- 4.2.7.6.6. La respuesta no da a conocer capacidades, procedimientos, métodos, medios, elementos técnicos, operaciones o actividades que comprometan la seguridad de VECOL S.A.
- 4.2.7.6.7. La respuesta queda debidamente registrada para tener la trazabilidad de la misma. En el documento de respuesta se debe trasladar a las autoridades competentes o receptores autorizados la reserva legal de la información y especificar las prohibiciones o restricciones de su difusión, alertando sobre las acciones penales y

disciplinarias que acarrea la no observancia de lo consagrado en la ley.

4.2.7.6.8. Se da cumplimiento a lo establecido en el Anexo 3. "Inventario, Clasificación y Valoración de activos de Información".

4.2.8. POLÍTICA DE DESARROLLO SEGURO.

VECOL S.A. crea y mantiene mecanismos que incluyan los requerimientos de seguridad en todo el ciclo de vida de desarrollo y mantenimiento seguro de las aplicaciones, los responsables revisan y determinan la acción a seguir para el tratamiento de las vulnerabilidades, para evitar que tengan brechas de seguridad, esto aplica para los desarrollos realizados al interior de VECOL S.A. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.8.1. Se identifican y establecen los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software, y se justifica, acuerda y documenta.
4.2.8.2. Se incluyen puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.
4.2.8.3. El cambio de versión de las aplicaciones implementadas en el ambiente de producción deben contar con controles de seguridad, para esto se hace una copia de respaldo en caso que se deba realizar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.
4.2.8.4. Se realizan pruebas de seguridad en un ambiente controlado con el fin de identificar vulnerabilidades, las cuales son resueltas antes del paso a producción.
4.2.8.5. El Departamento de Tecnologías de la Información (TI) deberá contar con los ambientes de Desarrollo, Pruebas y Producción, los cuales deberán estar separados.
4.2.8.6. El ambiente de prueba es simular el ambiente de producción.
4.2.8.7. Cuando se contraten desarrollos por terceros, VECOL S.A. valida el cumplimiento de requerimientos de seguridad.

4.2.9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES.

VECOL S.A. identifica requisitos de seguridad para proteger la información, e incluirlos dentro de los acuerdos con proveedores, por medio de un análisis que permita identificar riesgos asociados para implementar planes de acción dependiendo de las actividades a realizar. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.9.1. Se tiene en cuenta la documentación relacionada con los servicios, infraestructura de TI, sistemas de información y activos a los cuales tendrán acceso los proveedores, esto es controlado teniendo en cuenta los permisos de acuerdo al trabajo a realizar y los acuerdos firmados, los cuales tienen requisitos mínimos de seguridad, que se cumplen haciendo seguimiento por medio de mecanismos establecidos.
4.2.9.2. VECOL S.A. incluye dentro de los acuerdos a firmar con el proveedor, todos los controles de seguridad aplicables.
4.2.9.3. Cuando exista la necesidad de otorgar acceso de terceras partes a los diferentes sistemas de información, se realiza siempre con la participación del propietario de la

información una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta entre otros los siguientes aspectos:

4.2.9.3.1. El tipo de acceso requerido (físico, lógico y a qué recurso).
4.2.9.3.2. Los motivos para los cuales solicita el acceso.
4.2.9.3.3. El valor de la información del área que lo solicita.
4.2.9.3.4. Los controles empleados por la tercera parte.

4.2.9.4. En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y firmado un contrato o acuerdo que definan las condiciones para la conexión o el acceso.

4.2.9.5. El acceso de los terceros a la información o a cualquier elemento de la infraestructura tecnológica es solicitado por el supervisor, o persona a cargo del tercero, al propietario de dicho activo, éste junto con los encargados de la infraestructura tecnológica, aprueban y autorizan el acceso y uso de la información.

4.2.9.6. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de computadores, contemplarán como mínimo los siguientes aspectos:

4.2.9.6.1. Forma en los que se cumplirán los requisitos legales aplicables
4.2.9.6.2. Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conocen sus responsabilidades en materia de seguridad.
4.2.9.6.3. Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
4.2.9.6.4. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
4.2.9.6.5. Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
4.2.9.6.6. Niveles de seguridad física que se asignará al equipamiento tercerizado.
4.2.9.6.7. Derecho a la auditoría por parte de VECOL S.A.

4.2.9.7. Todos los proveedores firman la cláusula y/o acuerdo de confidencialidad que es parte integral de los contratos, utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplica para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos a personas o entidades externas.

4.2.9.8. Se formalizan los Acuerdos de Niveles de Servicio y los acuerdos de intercambio de información con cada proveedor dentro del contrato realizado, de acuerdo a los lineamientos establecidos por VECOL S.A.

4.2.9.9. Se definen las cláusulas por incumplimiento en los contratos de los proveedores, para establecer las situaciones que puedan generar multas o penalizaciones, dentro de los cuales se contempla los acuerdos de confidencialidad y no divulgación de la información.

4.2.9.10. Los procesos de selección, evaluación y adjudicación del contratista o proveedor están enmarcados en la normatividad vigente aplicable y las políticas internas de VECOL S.A.

4.2.9.11. El seguimiento y control de ejecución de los contratos es ejercido por los supervisores que designe VECOL S.A.

4.2.9.12. Los encargados de la infraestructura tecnológica verifican las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros.

4.2.9.13. Los supervisores de contratos con terceros administran los cambios en el suministro de servicios por parte de terceros, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

4.2.10. POLÍTICA DE GESTIÓN DE ACTIVOS.

VECOL S.A. identifica todos los activos de información y mantiene un inventario actualizado, exacto, consistente y documentado con todos los aspectos relevantes de cada uno, clasificándolos de acuerdo a la Confidencialidad, Integridad y Disponibilidad de la información, para identificar su valor y criticidad. Además, cada activo debe tener un propietario que garantice los niveles de seguridad que correspondan según sea el caso. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.10.1. Los equipos de terceros que requieran acceder a las redes de datos de VECOL S.A. deben cumplir con mecanismos de sanitización informática antes de concederles dicho acceso.
4.2.10.2. VECOL S.A., garantizará que el Departamento de Tecnologías de la Información (TI) tenga los recursos para una correcta gestión de Activos de la Información.
4.2.10.3. Todos los activos de información adquiridos y dados de baja, deben ser reportados por el responsable del mismo mediante la Mesa de Ayuda Técnica con el fin de ser actualizado el inventario.
4.2.10.4. Cuando un activo de información es reasignado a otra persona, se debe informar por la Mesa de Ayuda Técnica, con el fin de ser actualizado el inventario.
4.2.10.5. Los equipos de terceros que hayan sido autorizados para acceder de forma permanente a las redes de datos de VECOL S.A. sólo podrán hacerlo una vez se haya efectuado un análisis de software malicioso por parte del Departamento de Tecnologías de la Información (TI).
4.2.10.6. Los trabajadores de VECOL S.A. se comprometen a identificar, clasificar, etiquetar, disponer, devolver y gestionar los activos de información establecidos como tal, de acuerdo a la presente política y al Anexo 3. “Inventario, Clasificación y Valoración de activos de Información”.
4.2.10.7. La identificación, clasificación y valoración de los activos de información se realiza de acuerdo al Anexo 3. “Inventario, Clasificación y Valoración de activos de Información”.
4.2.10.8. Se mantiene un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, de acuerdo al Sistema o Herramienta que el Departamento de Tecnologías de la Información (TI) disponga para el Inventario, Clasificación y Valoración de activos de Información.
4.2.10.9. Todos los activos de información tienen asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.
4.2.10.10. Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.
4.2.10.11. Los documentos, información o material de VECOL S.A. se enmarcan dentro de los niveles de clasificación de seguridad de la información, de acuerdo a lo establecido en el Anexo 3. “Inventario, Clasificación y Valoración de activos de Información”.

4.2.10.12. Los documentos de VECOL S.A. que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.

4.2.10.13. La información con mayor nivel de clasificación de seguridad, tiene mayores restricciones y controles para el acceso a la misma por parte de los receptores, las autoridades, los empleados y asesores que deban conocer de ella.

4.2.10.14. Los trabajadores de VECOL S. A. deben seguir los siguientes lineamientos:

4.2.10.14.1. Se encuentra restringida la conexión no autorizada de cualquier elemento de almacenamiento de acuerdo con la Política de Dispositivos Móviles que hace parte del presente manual.

4.2.10.14.2. El uso de medios removibles de almacenamiento solamente es autorizado a los trabajadores, contratistas y demás terceros con el aval del Jefe de cada una de las oficinas quienes informan por medio de correo electrónico al Director de Informática.

4.2.10.14.3. Los medios de almacenamiento removibles como cintas, discos duros removibles, y dispositivos USB, que contengan información corporativa de Vecol, deben ser controlados y físicamente protegidos por el funcionario responsable de la información.

4.2.10.14.4. La información que es almacenada en medios removibles y que debe estar disponible por largo tiempo, debe ser protegida y controlada adecuadamente por cada Jefe o Director responsable para evitar que ésta se vea afectada por el tiempo de vida útil del medio.

4.2.10.14.5. La responsabilidad de la información contenida en los medios removibles es del trabajador que está a cargo del mismo, con la autorización del Jefe o Director.

4.2.10.14.6. De acuerdo con buenas prácticas en seguridad de la información, se debe evitar el almacenamiento o transporte de este tipo de información en medios removibles no controlados o autorizados. Sólo se deben habilitar unidades de medios removibles cifrados si hay una razón de la operación para hacerlo. Se deben aplicar los siguientes controles:

- Se utilizan mecanismos de cifrado fuertes sobre la información y/o medio removible.
- Los medios removibles sobre los cuales se pueda tener control, se almacenan en un ambiente protegido y seguro.
- Para mitigar el riesgo de degradación de los medios que contienen los datos almacenados, éstos se transfieren a medios nuevos antes de que se vuelvan ilegibles luego de cumplir un tiempo el cual es definido por la Empresa.
- En caso de necesitar retirar de Vecol un medio removible, se debe realizar con la autorización del Director o Jefe directo.

4.2.10.14.7. En caso de ser necesario, el Director o Jefe responsable de los medios debe realizar una copia de respaldo de la información que se encuentra en el medio removible antes de ejecutar cualquier acción de disposición segura o reasignación del mismo.

4.2.10.14.8. El responsable de un medio que se reasigne o que se requiera para otra tarea y deba realizar un borrado total del mismo, debe solicitar al Director del Departamento de Tecnologías de la Información (TI)

realizar el borrado seguro del contenido del medio removible, para esto se utiliza el método Peter Gutmann (35 pasadas).

4.2.10.14.9. Cuando un medio removible se deba destruir, el responsable del mismo debe realizar la disposición segura del medio utilizando alguna de las siguientes técnicas: Desintegrar, Pulverizar, Fundir o Incinerar. Adicionalmente, para los discos ópticos (CD, DVD, Blu-ray) se utiliza la técnica de triturar, haciendo uso de máquinas trituradoras de papel o específicas para esta labor.

4.2.10.15. Los activos de información deben tener un uso aceptable siguiendo las indicaciones definidas en el Anexo 3. "Inventario, Clasificación y Valoración de activos de Información".

4.2.10.16. El desarrollo de contratos de mantenimiento de equipos informáticos cuentan con la asignación de un supervisor permanente, encargado de controlar que se cumplan los estándares de seguridad tanto en la parte física como lógica de los sistemas.

4.2.10.17. VECOL S.A. deberá garantizar al Departamento de Tecnologías de la Información (TI), contar con un área física de mantenimiento de equipos, la cual garantizará que los equipos que son llevados a mantenimiento y que contenga información pública reservada y pública clasificada, estarán contenidos y supervisados.

4.2.10.18. Los discos duros o sistemas de almacenamiento que requieran mantenimiento y en los cuales se haya grabado en algún momento información pública reservada y pública clasificada, no podrán ser retirados de las instalaciones donde estén asignados por aspectos de seguridad. Si el dispositivo requiere reemplazo, en ningún caso podrá ser entregado para su cambio al proveedor o fabricante. Esta disposición deberá quedar registrada y acordada en todos los contratos y garantías. En caso de una garantía, se debe proceder a borrar en forma segura, para lo cual VECOL S.A. garantizará al Departamento de T.I. que tenga la herramienta necesaria para dicha labor.

4.2.11. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

VECOL S.A. Promueve para usuarios internos y externos el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.11.1. Se deben reportar a la Mesa de Ayuda Técnica los incidentes de seguridad de la información, la cual tendrá la responsabilidad de investigar y solucionar junto con el Departamento de T.I., los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

4.2.11.2. Los propietarios de los activos de información, trabajadores y terceros deben informar los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización, mediante la Mesa de Ayuda Técnica MAT de Vecol S.A.

4.2.11.3. Se documentan y clasifican los incidentes de seguridad de la información de acuerdo con las indicaciones especificadas en la Mesa de Ayuda Técnica MAT de Vecol S.A.

4.2.11.4. Se analizan los incidentes de seguridad de la Información para identificar cuáles serán escalados y proceder a realizar el contacto con las autoridades, cuando se estime necesario.

4.2.11.5. Todo aquel evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la Confidencialidad, Integridad y Disponibilidad de la infraestructura tecnológica, será reportado en la Mesa de Ayuda Técnica MAT de Vecol S.A.

4.2.11.6. En los casos que sea necesario realizar recolección y preservación de la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información, será reportado a la Mesa de Ayuda Técnica de Vecol S.A. y el comité TIC deberá generar el plan de recolección de evidencia a ser ejecutado.

4.2.12. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

VECOL S.A. estructura una organización donde se instituyen unos roles y responsabilidades de Seguridad de la Información, los cuales ejecutan actividades de administración, operación y gestión de la Seguridad de la Información. Esto es posible estableciendo una adecuada comunicación para que la Empresa pueda aprobar los lineamientos de Seguridad de la Información y coordinar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en todos los procesos de la Empresa. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.12.1. Los diferentes roles y sus responsabilidades del Sistema de Gestión de Seguridad de la Información (SGSI) están definidos en el Capítulo 3 del presente Manual.

4.2.12.2. La estructura de organización de Seguridad de la Información debe ser pública y clara en sus responsabilidades para cada uno de los roles definidos.

4.2.12.3. Se debe nombrar a quien lidera y asume la responsabilidad total por el desarrollo e implementación de la Seguridad de la Información y que apoye la identificación de los controles.

4.2.12.4. Cada activo o proceso de Seguridad de la Información tiene asignado un responsable y están documentados los detalles de esta responsabilidad.

4.2.12.5. Para tener la capacidad de cumplir las responsabilidades en el área de Seguridad de la Información, los trabajadores nombrados deben ser competentes en el área y se les debe brindar oportunidades de mantenerse actualizados con los avances en este tema.

4.2.12.6. Se definen las responsabilidades para las actividades de gestión del riesgo de la Seguridad de la Información, de acuerdo al Anexo 1. “Identificación, Análisis y Tratamiento de Riesgos de Seguridad de la Información”.

4.2.13. POLÍTICA DE NO REPUDIO.

La política de No Repudio comprende la capacidad de definir diferentes mecanismos o estrategias que están encaminadas a que un empleado o tercero evite negar que hayan realizado alguna acción. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.13.1. Para los procesos que se consideren, se deben implementar mecanismos en los que no exista la posibilidad de desafiar su validez de una acción por parte de quien la generó.

4.2.13.2. Algunos mecanismos a implementar deberán contar con un tercero, quien permita avalar la integridad y origen de los datos.

4.2.13.3. Se cuentan con registros que permitan hacer trazabilidad de las acciones de creación, origen, recepción, entrega de información y otros, que servirán de evidencia para poder garantizar el no repudio.

4.2.13.4. Estos registros se protegen contra la pérdida o modificación de tal manera que se garantice su disponibilidad e integridad.

4.2.13.5. Se pueden realizar auditorías continuas a los mecanismos de control y a los procesos, para asegurarse que las partes implicadas nieguen haber realizado una acción.

4.2.13.6. Los servicios de intercambio electrónico de información incorporan mecanismos que sean garantía de no repudio.

4.2.14. POLÍTICA DE PRIVACIDAD Y CONFIDENCIALIDAD.

La Política de Privacidad y Confidencialidad determina los lineamientos de tratamiento y protección sobre los datos personales y sobre la información considerada como sensible según la Ley 1581 de 2012 y las que apliquen. Se implementan controles de acuerdo a su nivel de clasificación. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.14.1. VECOL S.A. Realiza las verificaciones de antecedentes a todos los candidatos a un empleo de acuerdo a los lineamientos de la Gerencia de Recursos Humanos.

4.2.14.2. Todos los usuarios internos y externos de VECOL S.A. firman un acuerdo de confidencialidad, el cual contiene el compromiso de no divulgar la información interna y externa que conozca como parte del desarrollo de las funciones que desempeña o de su vinculación con la Empresa. La firma del acuerdo implica que la información conocida por todo usuario interno y externo, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización escrita por la Empresa.

4.2.14.3. El acuerdo de confidencialidad indica la vigencia del mismo, el cual debe mantenerse por el tiempo adicional que considere VECOL S.A. luego de terminada la vinculación con la Empresa. Este acuerdo debe ser comunicado al usuario interno y externo, según los lineamientos del Departamento de Recursos Humanos.

4.2.14.4. El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.

4.2.14.5. El tratamiento de datos personales, está sujeto a lo establecido en la “Política de tratamiento de datos personales” de VECOL S.A.

4.2.15. POLÍTICA DE INTEGRIDAD.

La política de Integridad se refiere a la protección de la exactitud y completitud de la información tanto interna como externa, conocida o administrada por usuarios internos y externos relacionados con VECOL S.A. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.15.1. Toda la información verbal, física o electrónica, es adoptada, procesada y entregada o transmitida integral, coherente y en forma exclusiva a las personas autorizadas a través de los medios correspondientes, sin modificaciones ni alteraciones.

4.2.15.2. En el caso de vinculación contractual, el compromiso de administración y manejo integro de la información interna y externa es parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información.

4.2.15.3. Para la información que se clasifique como pública reservada, pública clasificada y pública, y requiera ser transmitida a través de canales de comunicación, se utilizan mecanismos que permitan garantizar que la información mantiene su integridad mientras es transmitida por la red, es decir, que la información es completa y exacta de punto a punto en la transmisión.

4.2.16.POLÍTICA DE DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN.

VECOL S.A., proporciona los recursos suficientes y desarrolla esfuerzos tendientes a garantizar la continuidad de las operaciones para sus procesos con el fin brindar la disponibilidad de los servicios; así mismo, responde de manera efectiva ante eventos adversos según la dimensión y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la Seguridad de la Información durante dichos eventos, de igual manera se mantienen canales de comunicación adecuados hacia los trabajadores y demás partes interesadas.

Para esto VECOL S.A. evalúa el impacto de eventos que afectan los procesos de la Empresa y que tienen soporte en la infraestructura tecnológica y en la prestación de terceros. Igualmente, desarrolla planes de continuidad para aquellos servicios que son críticos y misionales de VECOL S.A., dichos planes cuentan con medidas tanto técnicas como administrativas y se prueban y revisan de manera periódica. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos:

4.2.16.1. La Empresa debe contar con un Plan de Continuidad de Seguridad de la Información que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales.
4.2.16.2. El responsable de la Continuidad de Seguridad de la Información es el encargado de mantener documentado y actualizado el Plan de Continuidad de Seguridad de la Información e informar cualquier cambio a todos los interesados.
4.2.16.3. Todos los sistemas de información que soportan las funciones críticas de VECOL S.A., cuentan con un plan de recuperación de T.I. que le permita garantizar una respuesta efectiva y eficiente ante eventos de desastre o interrupciones mayores, el cual está a cargo del Departamento de T.I.
4.2.16.4. Los procesos críticos están soportados en aplicaciones e infraestructura técnica robusta, software y hardware confiable.
4.2.16.5. Se provee al personal activo la documentación de las acciones a llevar a cabo en el evento de un desastre o una emergencia que puede afectar las aplicaciones de la operación y la infraestructura técnica, habilitando los procesos críticos de VECOL S.A., para ser restaurados en escalas de tiempo aceptables.
4.2.16.6. Los planes de continuidad de Seguridad de la Información son probados periódicamente y como resultado de estas pruebas se realizan los ajustes correspondientes.
4.2.16.7. Se identifica, acuerda y documenta todas las responsabilidades y los procedimientos para la continuidad de los servicios informáticos.
4.2.16.8. Se realiza la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad de Seguridad de la Información.
4.2.16.9. Se realizan los análisis de impacto a la operación y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de Seguridad de la Información a que haya lugar.

4.2.17.POLÍTICA DE REGISTRO Y AUDITORÍA.

Esta política de Registro y Auditoría define lo pertinente a las auditorías que se realizan a los procesos que incluyen activos del Sistema de Gestión de Seguridad de la Información (SGSI) e indica temas del

registro y conservación de las evidencias de las actividades y acciones que afectan los activos de información. Con el fin de garantizar el cumplimiento de ésta política se establecen los siguientes lineamientos

4.2.17.1. El Departamento de Aseguramiento de Calidad es el responsable de planificar, establecer, implementar y mantener cada 2 años la programación de las auditorías internas del Sistema de Gestión de Seguridad de la Información (SGSI) y de designar al equipo auditor.

4.2.17.2. Las auditorías internas del Sistema de Gestión de Seguridad de la Información (SGSI) se programan con base en el estado e importancia de las actividades a auditar y se llevan a cabo por personal auditor calificado, e independiente del área que se audite.

4.2.17.3. Cada director o jefe de sección es responsable de suministrar los medios necesarios para el adecuado desarrollo de la auditoría interna dentro de su departamento o sección, y es responsable de establecer y aplicar las acciones correctivas que se deriven de ella.

4.2.17.4. Para llevar a cabo las auditorías internas de la calidad en VECOL S.A, se aplica lo descrito en el PRO-GC1-005 “Procedimiento para realizar auditorías internas y externas”. Las actividades de preparación de auditorías internas incluyen la revisión de los documentos del Sistema de Gestión de Seguridad de la Información (SGSI) relacionado con el proceso, la elaboración de un plan de auditorías en el FVC-GC1-683 “Plan de Auditorías” y la elaboración de listas de verificación empleando el FVC-GC1-450 “Lista de Verificación”.

4.2.17.5. La ejecución de la auditoría inicia con la realización de una reunión de apertura con el responsable del proceso a auditar y/o el auditado y los auditores, la recolección de información durante el desarrollo de las actividades de acuerdo con el plan de auditoría, la revisión y evaluación de hallazgos de auditoría y una reunión de cierre.

4.2.17.6. Como mínimo, se realiza un ciclo completo de auditoría una vez cada cuatro años (todos los procesos y todos los elementos del Sistema de Gestión de Seguridad de la Información (SGSI)).

4.2.17.7. Cada auditoría interna de la calidad conlleva a la emisión de un informe en el que se describen los hallazgos detectados. Este informe se transmite a los responsables de las áreas auditadas, quienes realizan las correcciones o acciones correctivas correspondientes en los plazos previstos.

4.2.17.8. Las actividades de seguimiento realizadas por el auditor tienen la finalidad de garantizar que se realizaron las mejoras y las del área de Aseguramiento de Calidad tienen la finalidad de verificar y documentar que las acciones correctivas se han implantado con éxito.

4.2.17.9. Los resultados de las auditorías internas forman parte de la revisión por la dirección del Sistema de Gestión de Seguridad de la Información (SGSI).