CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA - CVC

MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Santiago de Cali, diciembre de 2019

MANUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. OBJETIVO 4
1.1. INTRODUCCIÓN 4
1.2. OBJETIVO DEL MANUAL 4
2. ALCANCE 4
3. DEFINICIONES 5
3.1. TÉRMINOS Y DEFINICIONES NORMA NTC-ISO/IEC 27000 5
3.1.1. Seguridad de la información 5
3.1.2. Otros conceptos 5
3.2. DEFINICIONES 6
4. DESARROLLO 8
4.1. CONTEXTO DE LA ORGANIZACIÓN 8
4.1.1. Contexto general 8
4.1.2. Contexto interno 9
4.1.3. Contexto externo 10
4.2. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS 10
4.2.1. Partes interesadas pertinentes al SGSI 10
4.2.2. Requisitos de las partes interesadas pertinentes a la Seguridad de la Información 11
4.3. DETERMINACIÓN DEL ALCANCE DEL SGSI 12
4.3.1. Activos de información 12
4.3.2. Plataformas tecnológicas 12
4.3.3. Procesos 12
4.4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – SGSI 13
4.4.1. Liderazgo 13
4.4.1.1. Liderazgo y compromiso 13
4.4.1.2. Política 14
4.4.1.3. Roles, responsabilidades y autoridades en la organización 14
4.4.2. Planificación 23
4.4.3. Soporte 25
4.4.4. Operación 26
4.4.5. Evaluación del desempeño 27
4.4.5.1. Seguimiento, medición, análisis y evaluación 27
4.4.5.2. Auditoría interna 28
4.4.5.3. Revisión por la dirección 28
4.4.6. Mejora 29

4.4.6.1. No conformidades y acciones correctivas 29
4.4.6.2. Mejora continua 30
4.5. OTROS DOCUMENTOS RELACIONADOS 30

1. OBJETIVO

1.1. INTRODUCCIÓN

La implementación de un Sistema de Gestión de Seguridad Información o SGSI, en las organizaciones está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Para la Corporación Autónoma Regional del Valle del Cauca, en adelante CVC, la información es un activo vital, por lo tanto, su seguridad se convierte en una prioridad, y con el ánimo de protegerla se ha propuesto el establecimiento de un Sistema de Gestión de Seguridad de la Información, lo cual le permite aportar en el uso estratégico de las tecnologías de la información, contribuyendo al cumplimiento de la misión y los objetivos estratégicos de la Corporación.

En este documento se presentan las directrices, políticas y estrategias que la CVC ha establecido para alcanzar los objetivos de seguridad de la corporación y a su vez dar cumplimiento a los requisitos de la norma ISO-IEC 27001:2013, teniendo como eje central la gestión de riesgos, un enfoque basado en procesos y el mejoramiento continuo.

1.2. OBJETIVO DEL MANUAL

El presente documento manual Sistema de Gestión de la Seguridad de la Información, SGSI, tiene como fin dar los lineamientos donde se especifican los requisitos para establecer, implementar, mantener y mejorar continuamente el SGSI en la CVC.

2. ALCANCE

El presente manual de sistemas de gestión se encuentra estructurado bajo los lineamientos estipulados por la norma ISO-IEC 27001:2013 y describe la estructura del Sistema de Gestión de Seguridad de la Información, SGSI, de la CVC. En este se detalla la disposición e interacción de los procesos estratégicos, misionales y de apoyo al interior de la corporación, los cuales permiten el mejoramiento continuo en la protección de la información de sus partes interesadas. Este manual puede ser consultado por todos aquellos que se vean interesados por comprender el sistema de gestión, su propósito, alcance y estructura.

El SGSI se implementa en la Oficina de Tecnologías de la Información, OTI, apoyado por los demás procesos de la CVC. El SGSI es aplicado en la sede principal de la corporación ubicada en Valle del Cauca y/o nodos en el territorio nacional colombiano. La implementación de este sistema busca proteger los datos e información de la CVC, a través de la aplicación de políticas y controles de seguridad con base en las buenas prácticas de seguridad informática y de la información.

3. DEFINICIONES

3.1. TÉRMINOS Y DEFINICIONES NORMA NTC-ISO/IEC 27000

3.1.1. Seguridad de la información

Entiéndase como la preservación de los siguientes tres pilares que son:

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

3.1.2. Otros conceptos

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Evento de seguridad de la información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la

información o falla en salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.

No repudio: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

3.2. DEFINICIONES

A los efectos de una correcta interpretación del presente manual, se consideran las siguientes definiciones:

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, Documentos...) que tenga valor para la organización.

Análisis de Impacto al Negocio – BIA: Por sus siglas en inglés Business Impact Analysis - BIA, consiste en un análisis para determinar los impactos que se producirían en los casos de que alguno de los riesgos llegara a materializarse, así mismo los niveles de riesgos determinados por la probabilidad e impacto de qué amenazas pueden materializarse al aprovechar ciertas vulnerabilidades.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Ethical Hacking: Consiste en la implementación de metodologías, métodos y técnicas para realizar pruebas de penetración o intrusión a los sistemas de información, como parte de la seguridad informática, con el fin de encontrar vulnerabilidades, aprender y buscar corregir puntos débiles en los sistemas y de esta forma mantener la seguridad en los niveles aceptables.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Plan de Recuperación de Desastres – DRP: Disaster Recovery Plan - DRP por sus siglas en inglés, es la planificación de estrategias y protocolos para levantar servicios corporativos en los casos de que se materialicen desastres de cualquier tipo o eventos que provoquen caídas por largos lapsos de tiempo.

Sistema de Gestión de Incidentes de Seguridad de la Información - SGISI: Es el sistema encargado de gestionar todo lo relacionado con los incidentes, eventos y/o fallas en los sistemas o personas que puedan comprometer la seguridad de la información, busca contener amenazas, aplicar controles de contingencia y de erradicación de amenazas para mantener los servicios activos y en buen estado.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Sistema de Gestión de la Seguridad de la Información - SGSI: "Un Sistema de Gestión de la Seguridad de la Información (SGSI) consiste en las políticas, procedimientos, directrices y recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos de negocio. Se basa en una evaluación de riesgos y en los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y aplicar los controles apropiados para asegurar la protección de estos activos de información, según se requiera, contribuye a la implementación exitosa de un SGSI." - ISO/IEC 27000: 2014.

Sistema de Gestión de la Continuidad del Negocio – SGCN: Aquel sistema que permite realizar la gestión para la continuidad de los servicios de la organización basados en los análisis de impacto al negocio, la gestión del riesgo y aceptación de riesgos residuales, donde se planifican planes de contingencia para la continuidad, así como los planes de recuperación ante desastres. BCM Por sus siglas en inglés Business Continuity Management, en él se incluye el BCP, Business Continuity Plan, o Plan de Continuidad de Negocio.

Sistema de Gestión Unificado de Amenazas – UTMS: Por sus siglas en inglés UTMS, Unified Threats Management System, es el sistema encargado de mantener o agrupar diferentes servicios de la seguridad informática para asegurar la información en el medio informático. En este sistema se agrupan políticas y controles a nivel de Firewalls, IPS, IDS, Antivirus, AntiSpam, entre otros mecanismos como los Laboratorios forenses y de Ethical Hacking.

Tecnología de la Información: Se refiere al hardware y software operado por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

4. DESARROLLO

4.1. CONTEXTO DE LA ORGANIZACIÓN

4.1.1. Contexto general

La **Corporación Autónoma Regional del Valle del Cauca**, es una entidad pública del gobierno colombiano dotada de autonomía administrativa y financiera, encargada de la administración pública de los recursos ambientales y su protección en su jurisdicción comprendida en el Departamento del Valle del Cauca.

El SGSI se implementa con el fin de garantizar y asegurar las operaciones de la corporación, a través de una apropiada evaluación de riesgos y niveles de aceptación de riesgos, para la apropiada gestión del riesgo teniendo en cuenta las cuestiones internas y externas.

4.1.1.1. Visión

En el año 2036 la CVC será reconocida por su gestión efectiva sobre las situaciones ambientales en el área de su jurisdicción contribuyendo a la construcción de una cultura ambiental regional y al desarrollo sostenible del Valle del Cauca.

4.1.1.2. Misión

Somos la entidad encargada de administrar los recursos naturales renovables y el medio ambiente del Valle del Cauca, que como máxima autoridad ambiental y en alianza con actores sociales propende por un ambiente sano, contribuyendo al

mejoramiento de la calidad de vida de la población y la competitividad de la región en el marco del desarrollo sostenible.

4.1.1.3. Objetivos corporativos

a) Fortalecer los procesos de planificación y ordenamiento ambiental del territorio, como instrumento básico de la gestión ambiental.

b) Mejorar las condiciones de los ecosistemas con base en el conocimiento, la recuperación y el aprovechamiento sostenible de sus bienes y servicios ambientales.

c) Disminuir los impactos generados por las actividades antrópicas en los centros poblados.

d) Promover el uso de tecnologías y prácticas que permitan la reducción de los impactos generados por procesos productivos.

e) Fortalecer la capacidad de los actores sociales, a fin de hacer efectiva su participación en la gestión ambiental.

f) Mejorar la capacidad de gestión (eficiencia, eficacia y efectividad) de la Corporación, que facilite la administración y manejo de los recursos naturales y el ambiente.

4.1.2. Contexto interno

Internamente el SGSI debe contar con el apoyo de la Dirección General, el Consejo Directivo, Asamblea Corporativa y Secretaria General, a quienes se designa el rol de la alta gerencia, así como de las oficinas, direcciones ambientales, demás áreas y personal, incluyendo a los de servicios generales, para que se logren cumplir con los propósitos del SGSI. Los actores anteriores deben ser conscientes de la necesidad de la seguridad de la información y por tanto deben promover una cultura de seguridad a través del cumplimiento de las políticas, normativas y/o directrices enfocadas a la seguridad de la información.

Otro de los aspectos internos son las planificaciones de las operaciones, las cuales se deben alinear con las tecnologías que la corporación tiene y los requerimientos mínimos de seguridad para las mismas.

El SGSI a nivel interno debe contar con la tecnología necesaria para salvaguardar la información, dispositivos, servicios, equipos y operaciones, para lo cual la corporación debe ser consciente de que es necesaria la inversión en tecnología, especialmente para los equipos de Seguridad, Infraestructura tecnológica y el personal capacitado. También es necesario el apoyo de la Dirección y el Consejo Directivo para la aprobación e implementación del SGSI.

4.1.3. Contexto externo

Externamente el SGSI debe contar con el apoyo para que las personas hagan el uso adecuado de los servicios publicados y prestados por la CVC. Se deben tener los instructivos, manuales y otros recursos educativos a través de mecanismos que logren que los clientes, socios, afiliados y público en general logren entender los canales adecuados para obtener los servicios prestados por la corporación, tales como Créditos, Depósitos, Administración de Recursos, Asesoría y Capacitación, Gestión de Proyectos, entre otros. A nivel tecnológico, como se mencionó en el anterior párrafo, se debe contar con el apoyo para implementar los dispositivos, mecanismos y controles necesarios para prevenir, contener y contrarrestar los ataques y/o amenazas externas; así mismo, se deben planificar las operaciones externas de tal manera que no se violente la seguridad de la información, en principio su confidencialidad, integridad y disponibilidad.

4.2. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Las necesidades de minimizar las brechas y blindar las vulnerabilidades de seguridad de la información y seguridad informática hacen pensar en la implementación del SGSI. Estratégicamente se trabaja en una adecuada gestión del riesgo para suplir las necesidades de seguridad en la tarea de proteger la información corporativa.

4.2.1. Partes interesadas pertinentes al SGSI

Estas son aquellas que se benefician del Sistema y para los cuales se ve necesario la implementación de los equipos de seguridad o en si el SGSI.

a) Dirección General: Interesada en la salvaguarda de los datos e información corporativa, a su vez es pertinente para el apoyo a nivel de gobierno y de recursos económico al SGSI.

b) Consejo Directivo, Asamblea Corporativa y Secretaria General: Al igual que el anterior, interesados en la salvaguarda de datos e información corporativa, pertinente para el apoyo al SGSI.

c) Oficina de Tecnologías de la Información - OTI: Como responsable por los servicios de TI, interesada en la salvaguarda y continuidad de los mismos. Es clave para la planificación, implementación, cumplimiento, gestión y apoyo, tanto en gobierno como destinación de rubros al SGSI.

d) Oficinas y Direcciones Ambientales Regionales: Pertinentes para los cumplimientos de las políticas y normativas del SGSI, interesados en la salvaguarda de las aplicaciones, datos e información bajo su custodia o gestión. Son pertinentes para el trabajo conjunto revisión y redefinición de los controles y/o mecanismos de seguridad, así como para el cumplimiento interno y externo.

e) Usuarios y público en general: interesados en la salvaguarda de sus datos e información bajo la custodia o gestión de la CVC.

4.2.2. Requisitos de las partes interesadas pertinentes a la Seguridad de la Información

Los requisitos generales para los cuales se implementa el SGSI son los de:

a) Salvaguardar los datos e información que se trata a través de las aplicaciones y/o herramientas corporativas.

b) Garantizar la continuidad en los servicios tecnológicos corporativos y así ayudar a mantener activas las operaciones de la corporación.

c) Realizar una adecuada gestión de riesgos y en sí garantizar la seguridad de la información.

Para el cumplimiento de lo descrito anteriormente se ve necesario implementar diversas políticas y controles corporativos para el SGSI basado en la norma NTC-ISO/IEC 27001 de 2013 y su respectivo anexo A.

4.3. DETERMINACIÓN DEL ALCANCE DEL SGSI

El SGSI se implementa y aplica para la CVC, en todas sus sedes, nodos, oficinas, direcciones y áreas en el territorio de su jurisdicción, el cual opera desde la sede principal ubicada en la ciudad de Santiago de Cali, Valle del Cauca – Colombia, a través de la Oficina de Tecnologías de la información - OTI. El SGSI es aplicable para cualquier agente o entes que se involucren con la corporación directa o indirectamente.

El SGSI implementa los controles y requisitos mínimos de seguridad para las operaciones, equipos, dispositivos, aplicaciones y servicios tecnológicos corporativos de la CVC. Se adoptan las medidas de seguridad perimetral, dispone de la normativa y controles para la seguridad de la información, la seguridad física y la seguridad informática.

En la CVC la gestión de la seguridad de la información busca establecer y mantener programas, controles y políticas para conservar la confidencialidad, integridad y disponibilidad de la información.

El SGSI debe ser aplicado en todos los activos de información de la CVC, en sus plataformas tecnológicas, oficinas y direcciones ambientales regionales.

4.3.1. Activos de información

Dentro del alcance del SGSI están los activos de información identificados y clasificados en las oficinas y direcciones ambientales regionales, el lugar donde se alojan dichos activos de información, las oficinas, las direcciones, los funcionarios y contratistas de la CVC.

4.3.2. Plataformas tecnológicas

Las plataformas tecnológicas que hacen parte del alcance del SGSI, a través de las cuales se implementan los controles y requisitos mínimos de seguridad para los equipos, dispositivos, aplicaciones, operaciones y servicios tecnológicos corporativos de la CVC.

4.3.3. Procesos

Hacen parte del alcance del SGSI todos los procesos descritos en el mapa de procesos de la CVC, que están clasificados en procesos de Dirección, Misionales y de Apoyo.

4.4. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – SGSI

"Un Sistema de Gestión de la Seguridad de la Información, SGSI, consiste en las políticas, los procedimientos, las directrices y los recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos de negocio. Se basa en una evaluación de riesgos y en los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz. Analizar los requisitos para la protección de los activos de información y aplicar los controles apropiados para asegurar la protección de estos activos de información, según se requiera, contribuye a la implementación exitosa de un SGSI." ISO-IEC 27000:2014

A continuación, se describen varias secciones que estructuran o componen el SGSI:

4.4.1. Liderazgo

4.4.1.1. Liderazgo y compromiso

Aunque el SGSI está liderado por un Oficial de seguridad o quien haga sus veces, es muy importante que la Dirección General y la OTI de la CVC demuestren liderazgo y compromiso con el SGSI, teniendo en cuenta los siguientes aspectos:

a) Asegurar que se establezcan las políticas de seguridad de la información y los objetivos de la seguridad de la información, y que estos estén alineados con la CVC.

b) Asegurar la integración de los requisitos del SGSI en los procesos de la corporación.

c) Asegurar o garantizar los recursos que el SGSI necesita.

d) Comunicar la importancia del SGSI y la responsabilidad de contribuir a su cumplimiento y desarrollo normal, para que el mismo logre los resultados planificados.

e) Dirigir y apoyar a las personas, para contribuir al SGSI, así como orientar a la mejora continua.

Los aspectos mencionados anteriormente son claves para que se puedan cumplir con los objetivos del SGSI.

4.4.1.2. Política

La dirección general y el consejo directivo de la CVC deben aprobar y/o establecer una política de seguridad de la información acorde con las siguientes características:

a) Relacione los objetivos de la seguridad de la Información, acordes a los propósitos de la corporación.

b) Establezca los compromisos para el cumplimiento de los requisitos relacionados con la seguridad de la información.

c) Agregue las directrices para la mejora continua del SGSI.

d) Que la política de seguridad de la información esté disponible como información documentada y sea comunicada para la CVC y las partes interesadas.

La política de seguridad de la información será redactada y/o revisada por el Oficial de Seguridad de la Información o quien haga sus veces y las partes interesadas del SGSI. Deberá enviarse a la Dirección General quien deberá revisar, aprobar, firmar y comunicar dicha política. Así mismo el Consejo Directivo, las oficinas, direcciones y demás dependencias de la Corporación podrán hacer sugerencias y aportes al mejoramiento de la Política de Seguridad de la Información

4.4.1.3. Roles, responsabilidades y autoridades en la organización

Se designan los roles, responsabilidades y autoridades de la corporación pertinentes al SGSI, los cuales se describen a continuación:

4.4.1.3.1 Dirección General / Gerente

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de la Norma ISO/IEC 27001:2013;

b) Informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

c) La revisión y aprobación de las Políticas de Seguridad de la Información.

d) Promover activamente una cultura de seguridad de la información dentro y fuera de la corporación.

e) Facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad sin excepción alguna.

f) El aseguramiento de los recursos, infraestructura y talento humano adecuados para implementar y mantener el SGSI.

g) Hacer que el personal directivo de la entidad, así como los líderes de cada proceso sean responsables de que los colaboradores a su cargo, conozcan, apliquen y cumplan las políticas de seguridad de la información sin excepción alguna.

4.4.1.3.2 Dirección de Planeación / Gestión de Calidad

Deben asegurar los siguientes aspectos:

a) Realizar el acompañamiento en la gestión de la seguridad de la información y apoyar en la documentación de procesos y procedimientos concernientes a la seguridad de la información.

b) Verificar el cumplimiento de las políticas de Seguridad de la Información y activar el procedimiento de escalamiento a la Oficina de Control Interno cuando se compruebe el no cumplimiento de estas.

4.4.1.3.3 Oficina de Control Interno / Asesoría y Verificación del Sistema de control Interno

a) Analizar, planear y ejecutar las auditorías internas al SGSI, en cuanto a su implementación y cumplimiento por parte de los procesos o etapas de

procesos involucrados, con el fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad, regulaciones normativas y la legislación aplicable.

b) Reportar los hallazgos y/o las no conformidades de las auditorías en el cumplimiento del SGSI, al Oficial de Seguridad de la Información o quien haga sus veces y al proceso Gestión de Tecnologías de la Información y demás procesos responsables.

c) Informar a los procesos responsables los hallazgos de las auditorías.

4.4.1.3.4 Oficina de Tecnologías de la Información - OTI / Gestión de Tecnologías de Información

a) Analizar e implementar las acciones pertinentes frente a los incidentes de seguridad que han sido escalados con el fin de subsanar las brechas y vulnerabilidades respectivas a la seguridad de la información.

b) Realizar las planificaciones para el mejoramiento de la infraestructura tecnológica relacionada con la seguridad de la información.

c) Brindar apoyo necesario al personal responsable del SGSI.

d) Implementar los controles y medidas de seguridad adecuadas con el fin de asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de los sistemas operativos, bases de datos, repositorios, servidores, plataforma tecnológica, sistemas de información y servicios de telecomunicaciones de la CVC.

e) Asignar las funciones, roles y responsabilidades de Seguridad Informática, a los colaboradores para la operación y administración de las plataformas tecnológicas de la entidad. Dichas funciones, roles y responsabilidades recaen principalmente sobre el Oficial de seguridad de la información o quien haga sus veces, su equipo, y demás personal de la Oficina de Tecnologías de la Información.

f) Disponer, llevar y reportar el adecuado control de cambios en el software que se desarrolla dentro de la CVC - In-House, con el fin de garantizar los requisitos mínimos de seguridad.

g) Disponer de los espacios y tiempos necesarios para la revisión de la seguridad de la información del software desarrollado In-House, con los fines de salvaguardar los datos tratados a través de los aplicativos desarrollados internamente.

h) Resolver los incidentes de seguridad que hayan sido detectados y reportados por fallas en el desarrollo de software.

i) Adaptar las metodologías, métodos, herramientas y estrategias adecuados para el desarrollo de software seguro.

4.4.1.3.5 Oficial de Seguridad de la Información o quien haga sus veces – CISO / Profesional Especializado Seguridad.

El Oficial de Seguridad de la Información o quien haga sus veces, Chief Information Security Officer - CISO por sus siglas en inglés, es un rol que tiene diversas responsabilidades en la gestión de la seguridad de la información a un profesional especializado de la OTI, el cual dispone de los siguientes roles y responsabilidades dentro del SGSI:

a) Coordinar la implementación y mantenimiento del Sistema de Gestión de la Seguridad de la Información, SGSI, según la norma NTC-ISO 27001 vigente, de acuerdo a los requerimientos de la CVC.

b) Definir, diseñar, proponer, actualizar y mantener las políticas de seguridad de la información y de seguridad informática que permitan un nivel adecuado de las mismas dentro de la empresa.

c) Gestionar oportunamente los requerimientos de seguridad informática de los funcionarios, brindando soluciones ya sea a nivel interno o con terceros expertos en la materia.

d) Coordinar con los otros procesos la aplicación de las políticas de seguridad de la información en la empresa.

e) Garantizar la incorporación de elementos de seguridad de la información en los diferentes componentes tecnológicos del sistema de información de la CVC.

f) Garantizar, validar y hacer seguimientos a la generación de copias de seguridad de bases de datos, programas, configuraciones, archivos empresariales, y archivos de usuarios finales.

g) Mantener informada a la corporación de la normativa, regulaciones y legislación aplicable en materia de la seguridad de la información.

h) Supervisar que los controles de seguridad informática implementados en la empresa estén operando correctamente.

i) Apoyar la implementación de buenas prácticas de seguridad en la gestión de TI., basada en normas y estándares internacionales.

j) Realizar interventoría de contratos con proveedores relacionados con seguridad de la información y mantener el contacto con los mismos.

k) Canalizar oportunamente los requerimientos de seguridad de los usuarios de aplicativos e implementar las soluciones respectivas.

l) Apoyar y asesorar a la empresa desde el enfoque de seguridad de la información para la toma de decisiones en la adquisición o compra de software externo.

m) Definir, proponer y mantener y actualizar la documentación del SGSI.

n) Reportar a la gerencia y el Consejo Directivo periódicamente, no más de un año, sobre el estado de la seguridad de la información de la entidad.

o) Coordinar y realizar labores de educación, divulgación y concientización de Seguridad de la Información en conjunto con gestión de talento humano para todos los funcionarios y terceros que tengan acceso a los activos de información de la CVC.

p) Evaluar y apoyar la implementación de controles específicos de Seguridad Informática para los sistemas o servicios de la corporación, sean preexistentes o nuevos.

q) Asesorar y apoyar en el proceso de medición de la eficiencia de los controles de seguridad implementadas por cada proceso o dependencia o área de la CVC.

r) Realizar el análisis de riesgos de seguridad de la información a los procesos que se determinen, de los definidos en la CVC.

s) Evaluar, seleccionar y sugerir la implantación de herramientas que faciliten las labores de seguridad y contingencia.

t) Recibir y/o solicitar capacitación en seguridad de la información.

u) Coordinar pruebas de hacking ético y explotación de vulnerabilidades.

v) Fomentar la coordinación entre los procesos de la CVC implicados en el logro de un nivel apropiado de seguridad de la información.

4.4.1.3.6 Comité de seguridad de la información

a) El SGSI dispondrá de un Comité de seguridad de la información, el cual debe ser transversal a la corporación.

b) El Oficial de seguridad de la información o quien haga sus veces debe gestionar para que se establezca el Comité de Seguridad de la Información, así como las responsabilidades del mismo. El mismo puede estar conformado por funcionarios de alta gerencia, jefes de oficinas y direcciones ambientales regionales.

4.4.1.3.7 Dirección Administrativa y del Talento Humano / Gestión de Talento Humano

a) Garantizar que el talento humano de la corporación cuente con las competencias que permitan el cumplimiento de las políticas de seguridad de la información.

b) Garantizar que la vinculación de los funcionarios se realice siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual está orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos, entre los que incluye los roles y responsabilidades frente a la seguridad de la información.

c) Hacer conocer el manual de Políticas de Seguridad de la Información a todo el personal sin excepción alguna como también a las terceras partes relacionadas con la CVC.

4.4.1.3.8 Oficina Asesora Jurídica / Asesoría y Representación Jurídica

a) Conocer e interpretar la normatividad vigente relacionada con seguridad de la información bajo el contexto de la corporación.

b) Velar por el cumplimiento de las regulaciones, normatividad y leyes vigentes en la corporación, para lo cual deberá trabajar conjuntamente con la Oficina de Tecnologías de la Información - OTI, y en específico con el Oficial de Seguridad de la Información, o quien haga sus veces, y su equipo.

c) Identificar, documentar y actualizar la documentación pertinente para cumplir con los requisitos legales, reglamentarios o contractuales aplicables a la CVC relacionados con seguridad de la información.

4.4.1.3.9 Propietario de los activos de información

Es el funcionario, contratista o área de la CVC al cual se le ha asignado la responsabilidad formal sobre un activo de información. Sus principales responsabilidades son:

a) Cumplir con la política de seguridad de la información aprobada por el comité de seguridad de la información.

b) Identificar, establecer el alcance y el valor o criticidad de los activos de información de los cuales es propietario.

c) Clasificar los activos de información siguiendo la metodología de identificación y clasificación de activos aprobada por el responsable del funcionamiento del SGSI.

d) Identificar, definir y evaluar los riesgos a los que pudieran estar expuestos los activos de información de los cuales es propietario.

e) Definir los requerimientos de seguridad de los activos de información en relación con su confidencialidad, integridad y disponibilidad.

f) Informar los requerimientos y controles requeridos por los activos de información a los custodios y usuarios de los activos de información.

g) Efectuar una verificación periódica de la correcta ejecución de los controles requeridos sobre los activos de información bajo su responsabilidad.

4.4.1.3.10 Custodio de los activos de información

Es el funcionario, contratista o área de la CVC responsable de administrar y hacer efectivos los controles que el propietario del activo de información haya definido.

Sus principales responsabilidades son:

a) Implementar y mantener los controles requeridos en los contenedores donde estén almacenados los activos de información que se encuentren a su cargo.

b) Administrar los recursos donde residen los activos de información dando los permisos definidos por el propietario del activo a los usuarios interesados.

c) Proteger los activos de información presentes en los contenedores a su cargo en la situación que corresponda: almacenamiento, transporte y procesamiento.

4.4.1.3.11 Líderes de procesos

Es un funcionario de la CVC al cual se le ha asignado la responsabilidad formal sobre un proceso de la entidad.

Sus principales responsabilidades son:

a) Apoyar la identificación de los activos de información que intervienen en el proceso correspondiente.

b) Validar los activos de información identificados junto con las características básicas de cada uno de ellos.

c) Apoyar y validar la identificación y designación de los propietarios de los activos de información de su proceso.

4.4.1.3.12 Usuario de la información

Es el funcionario o contratista de la CVC que utiliza la información para desempeñar sus funciones.

Sus principales responsabilidades son:

a) Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera de la CVC.

b) Conocer la clasificación de los activos de información que maneja.

c) Preservar la seguridad de la información utilizada en el desempeño de sus funciones y obligaciones.

d) No divulgar la información clasificada sin autorización del propietario del activo de información.

e) Procurar el buen manejo de todos los activos, buscando protegerlos en relación con los principios de seguridad.

4.4.2. Planificación

Esta es una parte muy importante para el SGSI donde se planifican las acciones para tratar los riesgos y los objetivos de la seguridad de la información.

4.4.2.1. Acciones para tratar riesgos y oportunidades

Dentro de la planificación para el tratamiento de riesgos y oportunidades el SGSI considera los requerimientos y cuestiones relacionadas pertinentes a la CVC frente a la seguridad de la información, se determinarán los riesgos y oportunidades que es necesario tratar con los propósitos de que el SGSI pueda lograr sus objetivos, prevenir o reducir impactos no deseados y mantener la mejora continua. Por lo tanto, se contempla un componente para la gestión del riesgo de la CVC pertinente a la seguridad de la información los cuales se encuentran descritos en el documento Metodología de Gestión de Riesgos de Seguridad de la Información.

4.4.2.2. Objetivos de seguridad de la información y planes para lograrlos

Los objetivos de proyectos de seguridad del SGSI deben ser coherentes a la política de seguridad de la información, así mismo se deben realizar los planes estratégicos para lograrlos.

Los objetivos de seguridad son establecidos por la CVC, los cuales se relacionan a continuación:

4.4.2.2.1. Objetivo general

Realizar una adecuada gestión de riesgos manteniendo la seguridad en los niveles de riesgo aceptables para garantizar la operatividad y que la CVC logre los objetivos propuestos; garantizando la confidencialidad, la integridad y la disponibilidad de la información, a través de la aplicación de un proceso de gestión del riesgo, y brindar confianza a la corporación y a las partes interesadas.

4.4.2.2.2. Objetivos específicos

a) Realizar una adecuada gestión de riesgos con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, a través de políticas y controles de seguridad de la información.

b) Capacitar y sensibilizar al personal en temas relacionados con seguridad de la información, buscando un aumento progresivo en la cultura de seguridad al interior de la corporación, reflejado en el nivel de cumplimiento de políticas y procedimientos y, el reporte de eventos e incidentes de seguridad.

c) Gestionar de manera adecuada los incidentes de seguridad de la información generando, documentando y aplicando las lecciones aprendidas, con el fin de reducir la posibilidad o el impacto de incidentes futuros.

d) Mejorar continuamente el desempeño del SGSI mediante la implementación de acciones correctivas eficaces, auditorías internas y las revisiones de seguridad de la información.

4.4.2.2.3. Planificaciones para lograr los objetivos

Estructurar los objetivos planteados en proyectos y subproyectos de seguridad que permitan una eficacia hacia el cumplimiento de los objetivos planteados, entendiendo que el trabajo sobre el SGSI es totalmente continuo.

a) La OTI debe coordinar los proyectos de seguridad planteados para determinar y/o contextualizar el recurso necesario, (humano, tecnológico, financiero), así poder realizar las gestiones para obtener dicho recurso y ejecutar los proyectos de seguridad.

b) Dar a conocer a la gerencia los proyectos de seguridad, evidenciando las ventajas, beneficios y garantías para la CVC del desarrollo del o los proyectos, y así obtener la aprobación y apoyo de los recursos necesarios para la ejecución.

c) Para lograr los objetivos planteados se pueden desarrollar múltiples proyectos de seguridad, para los cuales se deben crear planes y estrategias para que estos puedan ser aprobados y ejecutados. Dichos planes deben ser desarrollados en su momento o en el tiempo que resulten, teniendo en cuenta el momento o situación actual de la corporación, de igual forma los objetivos pueden resultar más específicos en cada nuevo proyecto de seguridad.

4.4.3. Soporte

4.4.3.1. Recurso

La CVC a través del proceso Gestión de Tecnologías de la Información debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.

4.4.3.2. Competencia

En relación a la competencia para la administración del SGSI la corporación, a través de los procesos de selección del talento humano, debe determinar la competencia necesaria de las personas que realizan un trabajo que afecta su desempeño de la seguridad de la información, deben asegurarse de que las personas sean competentes, basándose en la educación, formación o experiencias. Es importante que cuando sea aplicable o necesario se tomen las acciones para adquirir la competencia necesaria y evaluar su eficacia, así como conservar la información documentada que puede servir como evidencia de la competencia.

4.4.3.3. Toma de conciencia

Las personas que laboran bajo el control de la CVC deben tomar conciencia sobre la cultura de seguridad y lo establecido en las políticas de seguridad de la información, su contribución a la eficacia del SGSI, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información, así mismo ser conscientes de las implicaciones de la no conformidad con los requisitos del SGSI. El liderazgo y promoción de concientización sobre la importancia de la seguridad de la información estará a cargo del Oficial de seguridad de la información o quien haga sus veces y este es quien debe realizar una planificación estratégica al respecto.

4.4.3.4. Comunicación

Es importante que se determine la necesidad de realizar comunicaciones internas o externas pertinentes al SGSI, para lo cual el Oficial de seguridad de la información o quien haga sus veces deberá determinar dichas necesidades y socializarlas con el equipo de la OTI, así como con los demás agentes que se involucren.

Las características principales de las comunicaciones de seguridad deberán contemplar los siguientes aspectos:

a) Contenido de la comunicación
b) Cuando Comunicar
c) A quién comunicar
d) Quién debe comunicar
e) Procesos para llevar a cabo la comunicación

4.4.3.5. Información documentada

4.4.3.5.1. Generalidades

Dentro de la información documentada para el SGSI, debe incluirse la información documentada requerida por los estándares o normativas referenciadas para la implementación del SGSI, incluyendo la información documentada para la eficacia del SGSI. Para llevar a cabo esta actividad, la CVC dispone de un Sistema de Gestión de Calidad en el cual es llevada la organización de la documentación corporativa referente al SGSI.

4.4.3.5.2. Creación y actualización

Cuando se crea o actualiza la información documentada, Gestión de Calidad verifica que la estructura del documento esté acorde a lo establecido para la documentación corporativa, haciendo una revisión y aprobación con respecto a la idoneidad y adecuación.

4.4.3.5.3. Control de la información documentada

Con respecto a la información documentada del SGSI, el Oficial de seguridad de la información, o quien haga sus veces, conjuntamente con el equipo de Gestión Ambiental y Calidad de la Dirección de Planeación, deberán realizar los controles respectivos cuando haya cambios en la documentación; garantizando su confidencialidad, integridad y disponibilidades.

4.4.4. Operación

4.4.4.1. Planificación y control operacional

El SGSI es un proceso continuo, por lo cual es necesario que se realicen las planificaciones, controles e implementaciones necesarias por lo menos una vez al año con el fin de cumplir los requisitos de seguridad de la información. Esta actividad debe

ser liderada por el Oficial de seguridad de la información o quien haga sus veces con el apoyo de la OTI.

Es importante que se planifique y tenga control sobre los cambios, así como los imprevistos o cambios no planificados.

4.4.4.2. Valoración de riesgos de la seguridad de la información

Dentro de las operaciones importantes del SGSI se encuentra la valoración de riesgos de seguridad de la información. Para la CVC esta operación se realizará por lo menos una vez al año de acuerdo con los lineamientos que se han establecido en la metodología de riesgos de seguridad de la información y según lo planificado por el equipo de seguridad, se debe llevar la información documentada al respecto. Lo anterior es responsabilidad del Oficial de seguridad de la información o quien haga sus veces.

4.4.4.3. Tratamiento de riesgos de la seguridad de la información

Este es un proceso continuo el cual debe realizarse a la par con la detección de riesgos de seguridad, por tanto, es importante que se realice un plan de tratamiento de riesgos de la seguridad de la información acorde con la metodología de gestión de riesgos de seguridad de la información definidos. Es importante que se lleve la información documentada respectiva. Esta actividad es responsabilidad del Oficial de seguridad de la información o quien haga sus veces.

4.4.5. Evaluación del desempeño

4.4.5.1. Seguimiento, medición, análisis y evaluación

El desempeño y eficacia del SGSI será revisado y evaluado por la Corporación a través de los informes gerenciales por lo menos una vez al año o cuando sea requerido, en donde se determina:

a) Hacer seguimiento y medición al cumplimiento de los controles y políticas de seguridad de la información.

b) Revisar las mediciones y seguimientos del SGSI de acuerdo con los indicadores y métricas definidos. Las mediciones y seguimientos deben ser realizados por el Oficial de seguridad de la información o quien haga sus

veces. Así mismo, la alta dirección revisará dichos datos para la toma de decisiones.

c) Realizar una vez al año el análisis y evaluación de los resultados de seguimiento y medición, esto lo debe realizar el Oficial de seguridad de la información o quien haga sus veces y presentar esos resultados a la gerencia.

Es importante mantener la documentación en el desarrollo del ejercicio o actividades anteriores.

4.4.5.2. Auditoría interna

A través de la Oficina de Control Interno, se deben realizar auditorías internas por lo menos una vez al año, con el fin de tener información acerca del nivel de madurez del SGSI, y determinar si es o no conforme con:

a) Los requisitos de la organización para el SGSI.
b) Los requisitos y controles de la Norma ISO 27001:2013.
c) Si el SGSI es implementado y mantenido eficazmente.

Los programas de auditoría deben ser planificados, establecidos, implementados y mantenidos, donde se englobe los intervalos, métodos, responsabilidades, requisitos, criterios e informes. Es importante que se tengan en cuenta los procesos involucrados, así como los informes de anteriores auditorías.

Se deben definir los criterios, objetivos y alcances para cada auditoría. Tener presente el criterio de objetividad para lo cual se debe escoger los auditores detenidamente.

Mantener la información documentada como evidencia, informar sobre los resultados de la auditoría a las diferentes dependencias de la Corporación, incluyendo las sedes y direcciones ambientales regionales pertinentes.

4.4.5.3. Revisión por la dirección

El SGSI debe ser revisado al menos una vez cada año y cuando sea pertinente por la Dirección General, el Comité Directivo y la OTI, esto se hará a través de los informes gerenciales, otros informes sobre el SGSI y reuniones.

En la revisión se tendrán en cuenta los siguientes aspectos:

a) Sucesos y tendencias de las tecnologías pertinentes a la seguridad de la información.

b) Cambios en el entorno corporativo, a nivel interno y externo pertinentes a la seguridad de la información.

c) Información sobre el SGSI, su desempeño, no conformidades y acciones correctivas, seguimientos de mediciones, resultados de auditoría y cumplimiento de los objetivos de seguridad de la información.

d) Informes sobre los resultados de análisis y la gestión de riesgos.

e) Proyecciones de la mejora continua.

4.4.6. Mejora

4.4.6.1. No conformidades y acciones correctivas

Cuando al Oficial de seguridad de la información o quien haga sus veces, o al equipo del SGSI sean reportadas no Conformidades, es importante que se cumplan con los siguientes aspectos:

a) Reaccionar frente a la no conformidad que se reporte, tomando las acciones de control o corrección, según corresponda, así como afrontar los impactos o consecuencias.

b) Analizar las necesidades de medidas para erradicar las causas de las no conformidades y evitar futuras ocurrencias similares, teniendo en cuenta la revisión del reporte, las causas de la no conformidad y si existe relación con otras no conformidades.

c) Aplicar las correcciones necesarias, revisar que las correcciones sean eficientes.

d) Realizar modificaciones en el SGSI, políticas, controles u otros mecanismos de ser necesario, y comunicar los cambios en el SGSI.

4.4.6.2. Mejora continua

Es importante que el SGSI tenga el apoyo de toda la corporación con el fin de mejorar continuamente los aspectos de conveniencia, adecuación y eficacia. Para tales fines el SGSI dispone de canales de comunicación con los diferentes actores de la corporación para que los mismos puedan realizar los aportes, opiniones y retroalimentación de los aspectos pertinentes a la seguridad de la información o al SGSI.

4.5. OTROS DOCUMENTOS RELACIONADOS

- Política General SGSI.
- Metodología de gestión de riesgos de seguridad de la información.
- MN.0720.02 Políticas de seguridad de la información.