CONSORCIO SICOV-CRC

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

MN-SG-SI-1

ELABORÓ	REVISÓ	APROBÓ
Cargo: Oficial de Seguridad de la Información **Fecha:** Febrero de 2024	**Cargo:** Profesional Senior de Sistemas de Gestión **Fecha:** Febrero de 2024 **REVISÓ** **Cargo:** Oficial de Seguridad de la Información **Fecha:** Febrero de 2024	**Cargo:** Gerente proyecto SICOV CRC **Fecha:** Febrero de 2024

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

CONTROL DE CAMBIOS

VERSIÓN	FECHA APROBACIÓN	CARGO	CRITERIO(S)	CAMBIO
1	01/06/2018	Oficial De Seguridad De La información	Emisión	Se Creo El Documento
2	12/01/2023	Oficial De Seguridad De La Información	Modificación	Se modificaron los Objetivos Específicos, se modifica el alcance se modifica la dirección de la empresa, Se Agrega la dirección de SICOV al Comité de Seguridad de la información, se ajusta el formato y se actualiza
3	20/02/2024	Oficial De Seguridad De La Información	Modificación	Se realizó una actualización en los nombres de cargos y responsabilidades

INTRODUCCIÓN

Consorcio SICOV-CRC, dentro de su proceso misional y según los requerimientos de sus partes interesadas, requisitos legales y contractuales, debe cumplir a cabalidad con todos los requisitos de la Triada de Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad) en la ejecución de sus procesos misionales con la finalidad de garantizarle a sus clientes, usuarios y partes interesadas, el adecuado manejo de los activos de información que se tienen asignados.

De esta manera la política de seguridad de la información de Consorcio SICOV-CRC, emerge como el instrumento para concienciar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permitan cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la entidad, conscientes de que

La Alta Gerencia de Consorcio SICOV-CRC, se compromete con la seguridad de la información estableciendo un conjunto de políticas que brindan instrucciones claras y que permitan definir, especificar y elaborar los requisitos y procedimientos de seguridad para la gestión de la protección de los activos de la información de la empresa, de una manera consistente y efectiva dentro de las buenas prácticas establecidas en la ISO 27001:2013, garantizando la continuidad de los procesos de seguridad alineados a los objetivos estratégicos establecidos.

OBJETIVO GENERAL

Establecer y definir las políticas y lineamientos de seguridad de la información, que aseguren la confidencialidad, integridad y disponibilidad de la información para el conocimiento y cumplimiento de cada funcionario o usuario que acceda a los activos de información de Consorcio SICOV-CRC.

OBJETIVOS ESPECIFICOS

- Proteger la Información de colaboradores, proveedores, clientes y partes interesadas y la tecnología utilizada para su procesamiento, asegurando el cumplimiento de los principios de confidencialidad, integridad, disponibilidad y no repudio de la información.

- Identificar de manera temprana y oportuna los riesgos de seguridad de la información asociados a los activos de nuestra organización, para su adecuado tratamiento según lo establecido en el manual de gestión de riesgos.

- Fortalecer la cultura de Seguridad de la Información en nuestra organización para fomentar en los colaboradores, proveedores, clientes y partes interesadas, las buenas prácticas y comportamientos seguros en el manejo de la información actuando en concordancia con las políticas establecidas para tal fin.

- Monitorear el cumplimiento de los indicadores de gestión de Seguridad de la Información y continuidad del negocio para garantizar el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, según lo establecido en las políticas, los estándares y buenas prácticas del sector.

- Garantizar la mejora continua en la implementación, mantenimiento o mejora de los controles y/o lineamientos que permitan proteger la información frentes a nuevas amenazas y cambios que se produzcan en nuestra organización, el entorno y las tecnologías

ALCANCE

Las Políticas de Seguridad de la Información y documentos de seguridad complementarios aplican a cada persona que desempeñe alguna labor para Consorcio SICOV-CRC, sin importar su condición (empleado, contratista, consultor, personal temporal, practicante, personal de outsourcing, proveedor, socio de negocios, etc.) y cubre todos los activos de información de los procesos de la empresa, incluyendo, pero no limitándose a recursos tecnológicos como: computadores, dispositivos móviles, sistemas de red y componentes de su infraestructura, plataformas (sistemas operativos), aplicaciones, bases de datos, documentos impresos, personas, infraestructura e información.

Aplica para la sede de Bogotá Carrera 7 # 77-07 piso 7

DEFINICIONES

Acción correctiva: acción tomada para eliminar las causas de una no conformidad, de un defecto, o cualquier otra situación indeseable existente y materializada, para detener y/o impedir su repetición.

Acción de mejora: es aquella acción que no está motivada por una no conformidad (potencial o real), obedecen en su gran mayoría a optimizar la ejecución de procesos desde el factor humano y el factor tecnológico.

Acción preventiva: acción tomada para eliminar las causas de una no conformidad potencial, de un defecto, o cualquier otra situación no deseable para evitar que se produzca.

Aceptación del riesgo: decisión de asumir un riesgo.

Activo de información: cualquier elemento, material o inmaterial que procese, almacene o transmita información que sea de un valor importante para Consorcio SICOV-CRC.

Administración de usuario: Son las actividades de creación, modificación, consulta, bloqueo, desbloqueo y eliminación de usuarios, así como la revisión, asignación y revocación de privilegios.

Ambiente de capacitación: corresponde al ambiente en el cual el usuario final puede capacitarse en el funcionamiento de aplicativos o software base.

Ambiente de sistemas de información: se establecen los siguientes tipos de ambiente en sistemas de información: ambiente de desarrollo, ambiente de preproducción y ambiente de producción.

- Ambiente de desarrollo: en donde se realizan los cambios a los sistemas de información. Administrado por el equipo de Fábrica.

- Ambiente de preproducción: en donde se realizan las pruebas por parte del usuario líder o quien éste delegue para su aprobación antes de la puesta en marcha. Administrado por el equipo de Sistemas

- Ambiente de producción: corresponde al real. Es en donde se ejecuta la operación del negocio a nivel tecnológico. Administrado por el Equipo de Sistemas

Amenaza: causa potencial de un incidente no deseado, que puede ocasionar daño a los sistemas de información de Consorcio SICOV-CRC.

Análisis de riesgo: uso sistemático de la información para identificar las fuentes y causas de riesgo, estimar la probabilidad e impacto de riesgo, así como evaluar los controles a aplicar para mitigar, transferir, evitar o aceptar el riesgo.

Aplicación: conjunto de programas desarrollados en diferentes lenguajes de programación orientados a facilitar la administración de la información dentro de un proceso productivo o administrativo de una organización.

Autorización de datos personales: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: comunicación verbal y/o escrita generada por el responsable, dirigida al titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.

Backup: copia o respaldo de la información.

Base de datos: conjunto de registros de datos interrelacionados lógica y/o físicamente, que contienen información de usuario. Conjunto organizado de datos personales que sea objeto de tratamiento.

Call back: generación por parte del sistema de llamadas automáticas, para atender problemas que se presenten en los sistemas de información de la compañía.

Causa habiente: Persona que ha sucedido o se ha subrogado por cualquier título en el derecho de otra u otras.

Cifrado: método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que disponga de la clave de cifrado adecuada para decodificarlo.

Clientes: personas o entidades que establecen relaciones directas o indirectas con Consorcio SICOV-CRC.

Cobit 5: buenas prácticas de gobierno y gestión de tecnologías de la información.

Código malicioso: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.

Código móvil: es un código de software que se transfiere de un equipo a otro, luego se ejecuta automáticamente y lleva a cabo una función específica con poca o ninguna interacción del usuario. Ejemplo: controles ActiveX, JavaScript.

Comité de seguridad de la información: equipo de trabajo conformado por las personas responsables de definir los lineamientos de seguridad de la información dentro de la organización.

Comunicación del riesgo: intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

Confiabilidad: Garantía que la información es la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

Confidencial: información de uso y conocimiento exclusivo de una persona o grupo de personas externas o internas, que en caso de ser divulgada sin autorización afecta los intereses de la institución y de los clientes.

Confidencialidad: hace referencia a la protección de la información cuya divulgación fuera de las áreas interesadas no está autorizada.

Contingencia: acción encaminada a la recuperación de actividad del negocio, en casos de que se produzcan incidentes de seguridad que afecten a la información, las tecnologías que los soportan y continuidad de los mismos.

Continuidad del negocio: Mantenimiento de la operación misional de Consorcio SICOV-CRC. Durante las etapas de crisis.

Control: Medios y acciones para gestionar y mitigar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de Consorcio SICOV-CRC que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Criptografía: Es la técnica que consiste en cifrar un mensaje, conocido como, convirtiéndolo en un mensaje cifrado o criptograma, que resulta irreconocible e ilegible para todo aquel que no conozca el sistema ni las llaves utilizadas en el cifrado, haciendo indescifrable el contenido de la información que no conozca la forma de descifrar el criptograma.

Criptografía de llave simétrica: Técnica criptográfica donde dos o más partes comparten la misma clave y esta se usa tanto para cifrar como descifrar la información; esta clave debe mantenerse secreta durante su tiempo de vida, puesto que cualquiera que tenga acceso a ella puede descifrar toda la información cifrada con dicha clave, teniendo así mismo, la posibilidad de suplantar a alguna de las partes del mensaje.

Criptografía de llave pública: técnica criptográfica donde cada usuario tiene un par de llaves, una llave pública (que se puede revelar a cualquiera) y una llave privada (que se debe mantener en secreto). Las técnicas de llave pública se pueden usar para el cifrado de información de forma asimétrica al cifrar con la llave pública y descifrar con la llave privada, o para garantizar el no repudio al cifrar con la llave privada y descifrar con la llave pública.

Cumplimiento: tiene que ver con llevar a efecto las leyes, regulaciones y obligaciones contractuales a las cuales está sujeto el proceso del negocio; es decir, los criterios del negocio impuestos externamente por clientes o entes reguladores.

Custodios de la información: Son los individuos a los cuales se les delegan las labores rutinarias de administración y mantenimiento de los activos de información. Este se debe encargar de aplicar controles para mitigar riesgos existentes sobre los activos y mantener su adecuado funcionamiento. Implementa las políticas y guías fijadas por el propietario o por el ente de control.

Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Declaración de aplicabilidad: documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI del Consorcio SICOV-CRC.

Derechos de autor: el que la ley reconoce al autor de una obra para participar en los beneficios que produzca su publicación, ejecución o reproducción, y que alcanza, en algunos casos, a los ejecutantes e intérpretes.

Derechos de propiedad intelectual: los derechos de propiedad intelectual incluyen derechos de copia de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de códigos fuente.

Directriz: descripción que aclara lo que se debe hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Propiedad de la información, la cual debe estar accesible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

Efectividad: la información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

Eficiencia: el procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

Encargado de tratamiento de datos personales: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Estimación del riesgo: proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Evento de seguridad de la información: presencia identificada de un estado del sistema, servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

Evidencia digital: es un tipo de evidencia física o electrónica que puede tomar muchas formas como son: registros de aplicaciones, sistema operacional, comunicaciones (logs de seguridad, logs de intentos fallidos, etc.).

Evitación del riesgo: decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Firewall: es un filtro o cortafuegos (hardware o software) que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean permite o deniega su paso. El objetivo principal de un firewall es proteger a una red de otra. La red protegida es la red interna de la organización contra redes externas en las que no se pueden confiar y desde las que se pueden originar intrusiones. Para proteger la red debe evitarse que usuarios no autorizados tengan acceso a datos delicados, mientras que se debe permitir que usuarios legítimos tengan acceso irrestricto de acuerdo con su rol a los recursos. En general un “firewall” se coloca entre la red interna confiable y la red externa no confiable. El “firewall” actúa como un punto de cierre que monitorea y rechaza el tráfico de red no apropiado con base en las reglas de filtración programadas.

Colaboradores: son considerados colaboradores a los colaboradores y practicantes que tengan una relación contractual con el Consorcio SICOV-CRC.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar el riesgo dentro de la organización.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Impacto: Conjunto de efectos sobre los procesos de negocio de una modificación del entorno normal de operación, como consecuencia de la materialización de un riesgo.

Incidente de seguridad de la información: un evento o serie de eventos no deseados o inesperados que comprometen en mayor o menor grado la seguridad de la información de Consorcio SICOV-CRC.

Información: conjunto de datos ordenados, representados física, digital, verbal o simbólicamente, que da significado a un mensaje y es reconocida como un activo que tiene valor y vital importancia para el Consorcio SICOV-CRC.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos. Garantizando que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

ISACA: information systems audit and control association (asociación de auditoría y control de sistemas de información), la cual apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información

Líder de la aplicación: es el líder de la aplicación, ejecución y control de procesos que generan cambios a la información necesaria para la ejecución de las tareas de los niveles estratégico, táctico y operativo.

Misión crítica: Aplicaciones primordiales para el adecuado funcionamiento del negocio.

Nivel de seguridad c2: protección de acceso controlado. Nivel de seguridad informática definido por el departamento de defensa de los estados unidos que consideran un ambiente de acceso controlado y establece llevar una auditoría de accesos e intentos fallidos de acceso a objetos. Este nivel tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Operaciones monetarias: Son las acciones que implican o conllevan movimiento, manejo o transferencia de dinero.

Operaciones no monetarias: son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que prestan las entidades a sus clientes o usuarios y que no conllevan movimiento, manejo o transferencia de dinero.

PKI (Public Key Infrastructure): combinación de Hardware, Software y Políticas de seguridad que permiten la ejecución de operaciones criptográficas, garantizando el cifrado de las comunicaciones electrónicas por medio de algoritmos de clave pública.

Plan de auditoría: mecanismos de verificación y control para garantizar los principios básicos de confidencialidad, integridad, autenticidad y disponibilidad en el manejo de la información por parte de las personas, los procesos y la tecnología.

Plan de cuentas: configuración de los parámetros en el sistema para que el usuario intercale con éste, definiendo características como vigencia de la clave, horario de trabajo, longitud mínima de la clave, histórica de claves, entre otros.

Plataforma tecnológica: conjunto de elementos de hardware, software y comunicaciones destinados a un procesamiento de información con características específicas.

Política: toda intención y directriz expresada formalmente por la gerencia general del Consorcio SICOV-CRC.

Prioritaria: aplicaciones complementarias a las de misión crítica.

Privado: información de uso exclusivo de una persona o de la entidad.

Propietario o responsable de activo de información: identifica a un individuo o entidad que tiene responsabilidad aprobada por la gerencia general para el control de la operación, desarrollo, mantenimiento, uso y seguridad de los activos. En este documento el término “propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos, con excepción cuando se habla de datos personales.

Proyecto de SGSI: actividades estructuradas, llevadas a cabo por una organización para implementar un SGSI.

Público: información de dominio general.

Puertas traseras: son entradas no convencionales a los sistemas operacionales

que permiten acceso a intrusos sin que puedan ser detectados.

Reducción del riesgo: acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Repositorio: sitio, espacio o medio físico o digital disponible para almacenar información.

Requerida: aplicaciones utilizadas para la administración, operación y control institucionales. Se hace referencia a aplicaciones comerciales como procesadores de palabra, hojas electrónicas, graficadores y herramientas de desarrollo como java, cobol, etc.

Responsable de la información: será quien genera y mantiene los datos que utiliza la entidad a través de un conjunto determinado de sistemas y que son utilizados por un proceso determinado.

Responsable de la plataforma tecnológica: es la dependencia o persona encargada de operar y mantener el conjunto de elementos de hardware, software y comunicaciones a un procesamiento de información con características específicas.

Responsable de tratamiento de datos personales: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

Retención del riesgo: aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Riesgo en la seguridad de la información: potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a Consorcio SICOV-CRC.

Riesgo residual: nivel restante de riesgo después del tratamiento del mismo.

Riesgo: probabilidad de daño, heridas, perdida o cualquier ocurrencia negativa que es causada por vulnerabilidades internas o externas, las cuales tienen una probabilidad de materializarse, teniendo un nivel de impacto dentro de la organización o proceso.

Secreto: información de uso exclusivo de algunos colaboradores de la alta gerencia, la cual en caso de ser divulgada afecta los intereses institucionales (pin, claves, proyectos, etc.).

Seguridad de la información: Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información, al mantener y preservar la confidencialidad, integridad y disponibilidad de la información.

Seguridad perimetral: es un sistema de seguridad enfocado a controlar una red dividida en unidades lógicas desde una central, utilizando diferentes tipos de herramientas (hardware o software), los cuales tienen por objeto disuadir, detectar, frenar y avisar sobre cualquier intruso o violación que pueda ocurrir al perímetro protegido.

Servicios de procesamiento de información: cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

Sistema de gestión de seguridad de la información: parte del sistema integrado de gestión, basada en un enfoque hacia los riesgos globales de Consorcio SICOV-CRC, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Sistema de información: conjunto de datos, aplicaciones, equipos y recursos humanos que, en forma interrelacionada, proveen a la empresa la información necesaria para la ejecución de la tarea y la toma de decisiones de los niveles estratégico, táctico y operativo.

Spamming: correo masivo de mensajes de correo electrónico (e-mail) no solicitados.

Tcp/ip: Descripción de protocolos de red, usado para comunicaciones en redes, definiendo un conjunto de guías de operación para los equipos en red.

Teletrabajo: trabajo que se realiza desde un lugar fuera de la empresa utilizando las redes de telecomunicación para cumplir con las cargas laborales asignadas.

Tercera parte: persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.

Terceros: persona o entidad que tiene un tipo de relación directa o indirecta con Consorcio SICOV-CRC. Son terceros los proveedores, contratistas, visitantes, beneficiarios y aspirantes a programas del Consorcio SICOV-CRC.

Titular de datos personales: Es reconocido como Propietario de la Información Personal. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento. Consorcio SICOV-CRC en su proceder considera Titulares de datos personales a todas las personas que en calidad de colaboradores (colaboradores y practicantes) y Terceros (aspirantes y beneficiarios de los programas, proveedores, contratistas, visitantes o usuarios en general), proveen su información personal a la entidad. Igualmente, a los niños, niñas, adolescentes y sus representantes facultados legalmente de otorgar autorización del tratamiento de sus datos personales procedido del ejercicio del menor de su derecho a ser escuchado, valorada su opinión teniendo

en cuenta la madurez, autonomía y capacidad para entender el asunto.

Transferencia de datos: la transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Transferencia del riesgo: compartir con otra de las partes la pérdida o la ganancia de un riesgo.

Transmisión de datos: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la república de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Tratamiento de datos personales: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Usuario genérico: nombre de cuenta en un sistema de información o plataforma operacional (id de usuario) que es utilizado por más de una persona o que no está relacionado de forma directa a un usuario especifico.

Usuarios: Son todos los colaboradores o terceros que tienen acceso a la información del Consorcio SICOV-CRC, los cuales deben cumplir con las políticas de seguridad de la información, el tratamiento definido, y los procedimientos del Sistema de Seguridad de la Información. Los usuarios de la unidad de gestión deben reportar cualquier incidente de seguridad de la información del que tenga conocimiento por cualquiera de los medios definidos.

Usuario líder: usuario final corporativo responsable de la información que procesa una aplicación determinada para uno o varios procesos de la organización. Aunque es único por aplicativo, este podrá delegar funciones en otros cargos del área correspondiente.

Usuario privilegiado: perfil de usuario que maneja permisos especiales o superiores a la norma dentro de un sistema de información o plataforma operacional.

Utilitario sensitivo: paquete de programas que permite el acceso directo sobre los datos de un archivo cualquiera en una plataforma determinada.

Valoración del riesgo: proceso global de análisis y evaluación del riesgo.

Virus informático: programa que se auto replique, que consuma o que perjudique de alguna forma el rendimiento de los sistemas informáticos de forma intencional.

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

POLÍTICAS DEL PROCESO

1.1. Políticas específicas de Seguridad de la Información

Los colaboradores del Consorcio SICOV-CRC, deberán mantener la debida reserva sobre los documentos de trabajo y la información confidencial que esté a su cuidado, o que conozcan en ejercicio de su cargo, de tal forma que se pueda controlar y evitar que en cualquiera de las áreas de Consorcio SICOV-CRC se haga uso indebido de dicha información o que la misma sea conocida por personas que no tengan autorización para ello o no laboren en la respectiva área.

Por lo tanto, queda prohibido a los colaboradores y colaboradores revelar y/o transferir a otros colaboradores o a terceras personas las tecnologías, metodologías, know how, y secretos industriales, comerciales o estratégicos que pertenezcan a Consorcio SICOV-CRC, sus clientes o proveedores, a los que haya tenido acceso con ocasión de su cargo. Igualmente, no obtendrán ni intentarán el acceso a información que represente secreto industrial, comercial o estratégico en forma ilegítima. En los casos en los que se transfiera información confidencial o privada, el funcionario asumirá las sanciones disciplinarias, legales o penales que establezca la ley.

En consecuencia, Consorcio SICOV-CRC establecerá los controles o salvaguardas que se consideren pertinentes para garantizar la protección de la confidencialidad, integridad y disponibilidad de los activos de información de la empresa.

1.1.1. Política de Seguridad de la Información

Consorcio SICOV-CRC S.A.S, garantiza la protección de los activos de información, ejecutando sus funciones y responsabilidades frente a los organismos de control y partes interesadas, asegurando la confidencialidad, integridad y disponibilidad de la información de todos sus servicios, alineándose a los requisitos legales y a las buenas prácticas del sector que nos regula.

1.1.2. Política de Tratamiento de la Información de Datos Personales

Consorcio SICOV-CRC, en calidad de responsable y encargado de los datos personales

de sus actuales y anteriores colaboradores, clientes o terceros, define la Política de Tratamiento de la Información de datos personales en cumplimiento de su misión, la legislación vigente y seguridad de la información. (Ver documento *Política de Tratamiento de Datos Personales* (FR-SC-10). Este documento estará publicado en la página Web de Consorcio SICOV-CRC y es de libre consulta para las partes interesadas.

1.2. Revisión de la Política.

Esta política se debe revisar a intervalos planificados de un año, o sí ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.

1.3. Requisitos Organizacionales de la Seguridad de la Información

- Cumplir con la misión, visión y características de Consorcio SICOV-CRC.
- Garantizar la seguridad de la información de los clientes, beneficiarios, colaboradores y operaciones de Consorcio SICOV-CRC.
- Generación de valor a través de optimización e inclusión de la resiliencia de procesos. Fomentar la cultura organizacional en seguridad de la información en todo Consorcio SICOV-CRC.
- Garantizar la continuidad del negocio.
- Gestionar los riesgos de seguridad de la información de Consorcio SICOV-CRC.

1.4. Liderazgo y Compromiso de la Alta Dirección con el SGSI

La Alta Dirección de Consorcio SICOV-CRC demostrará Liderazgo y compromiso con el Sistema de Gestión de Seguridad de la Información, asegurando lo siguiente:

- El establecimiento de la política del SGSI, la política y objetivos de seguridad de la información, y que estos sean compatibles con la planeación estratégica de Consorcio SICOV-CRC.
- La integración de los requisitos del SGSI en los procesos de Consorcio SICOV-CRC.
- La disponibilidad de recursos necesarios para la operación del SGSI.
- Comunicando la importancia de una gestión de la seguridad de la información eficiente y el cumplimiento de los requisitos del SGSI.
- El logro de los resultados planeados del SGSI y que están estipulados en el Plan de Seguridad de la Información.
- Gerencia y apoyo a colaboradores, terceros pertinentes para lograr la eficacia del SGSI.
- Promoviendo la mejora del SGSI.

1.5. Estructura de Seguridad de la Información

La estructura de Seguridad de la Información en Consorcio SICOV-CRC, se encuentra alineada con los requerimientos y disposiciones de los planes estratégicos.

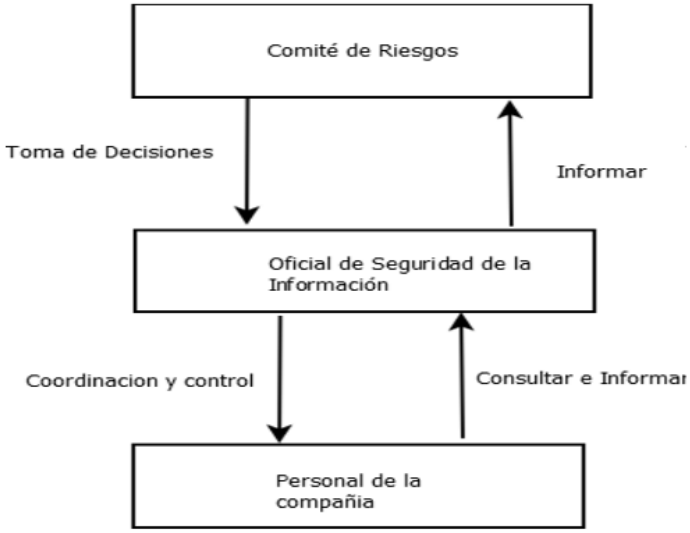
1.5.1. Actores del SGSI

- Comité de Riesgos.
- Oficial de Seguridad de la Información.
- Encargado del Sistemas de Gestión.
- Dueños de los procesos misionales y operativos del negocio.
- Colaboradores
- Clientes
- Especialistas Externos.
- Órganos de Control.
- Terceros.

1.5.2. Estructura Organizacional

Sin perjuicio de la Estructura Organizacional definida a continuación, toda la organización es responsable de la gestión y administración de seguridad de la información:

Ilustración 1. Estructura Organizacional



1.5.3. Roles y responsabilidades de la seguridad de la información

- **Comité de Riesgos:** Definir los criterios para la toma de decisiones con respecto a la seguridad de la información. Este comité se compone del Oficial de Seguridad de la Información y el encargado del Sistema de Gestión.

- El Consorcio SICOV-CRC, asignará la responsabilidad y autoridad al Gerente de SICOV para que reporte sobre el desempeño de la seguridad de la información.

- **Oficial de Seguridad de la Información:** Liderar el proceso de seguridad de la información al interior de Consorcio SICOV-CRC, asegurando el correcto manejo de los activos de información y coordinación de las actividades para planificar, dirigir y controlar el mismo.

  Así mismo, gestionar los riesgos asociados a la seguridad de la información al interior de Consorcio SICOV-CRC e implementar programas de formación y toma de

conciencia.

El Oficial de Seguridad de la Información deberá asegurar el cumplimiento de las políticas y lineamientos de la seguridad de la información de conformidad con lo establecido en los estándares internacionales vigentes y en todas aquellas leyes y demás normas que le sean competentes.

- **Todos los usuarios internos y externos**: Mantener la seguridad de la información en el lugar de trabajo, su entorno y sus actividades. Son los responsables de gestionar los requerimientos de Seguridad de la Información en conjunto con todos los dueños de los procesos Operativos y Misionales, de tal forma que las implementaciones en Seguridad de la Información generen valor para el negocio y mitiguen los riesgos identificados dentro de cada uno de los procesos que soportan la Misión y la Operación de la empresa.

1.6. Políticas Específicas de Seguridad de la Información

1.6.1. De las Políticas de Seguridad de la Información

1.6.1.1. *Orientación de la Alta Dirección para la Gestión de Seguridad de la Información.*

1. Establecimiento de las políticas para la seguridad de la información

La Gerencia de Consorcio SICOV-CRC, es el órgano encargado de aprobar las políticas de seguridad de la información.

a. Compromiso con la Seguridad de la Información

Consorcio SICOV-CRC asume el compromiso con la seguridad de la información, orientando y dando soporte sobre la misma de acuerdo con los requisitos del negocio, requerimientos legislación vigente y reglamentos que lo constituyen.

Teniendo en cuenta la Política General de Seguridad de la Información, la alta Dirección, los colaboradores de Consorcio SICOV-CRC, deberán mantener la debida reserva sobre los documentos de trabajo y la información confidencial que esté a su cuidado, o que conozcan en ejercicio de su cargo. Debiendo de esta forma, controlar y evitar que en cualquiera de las dependencias de Consorcio SICOV-CRC, se haga uso indebido de dicha información o que la misma sea conocida por personas que no tengan autorización para ello o no laboren en la respectiva área.

De tal manera, les resulta prohibido, revelar y/o transferir a otros colaboradores o a terceras personas las tecnologías, metodologías, know how, y secretos industriales, comerciales o estratégicos que pertenezcan a Consorcio SICOV-CRC, sus clientes o proveedores, a los que haya tenido acceso con ocasión de su cargo. Igualmente, no obtendrán ni intentarán el acceso a información que represente secreto industrial, comercial o estratégico en forma ilegítima.

b. Actualización de las Políticas de Seguridad de la Información

Cada responsable identificado en una política puede solicitar la modificación de estas de manera parcial o total. Los responsables de evaluar y definir la inclusión de una política son los miembros del Comité de Riesgos. Este comité será el encargado de realizar revisiones y mantenimiento de estas políticas al menos con una periodicidad anual o menor si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad. En las revisiones periódicas se debe tener en cuenta factores como: incidentes de seguridad sucedidos, nuevas vulnerabilidades detectadas o cambios dentro de la infraestructura organizacional o tecnológica.

c. Implementación de las Políticas de Seguridad de la Información

El Gerente del Consorcio SICOV-CRC facilitará los recursos humanos y técnicos necesarios para llevar a cabo la implantación de las políticas en la unidad de gestión.

Es deber del Oficial de Seguridad de la Información realizar las políticas de Seguridad de la Información y velar por la implementación de lo estipulado en las mismas.

Es deber del personal interno y externo dar cumplimiento cabal a las mismas según las exigencias de la compañía.

Es deber del Encargado del Talento Humano establecer y aplicar las medidas disciplinarias a las que haya lugar en el caso en el que se presente incumplimiento por parte del personal interno de la compañía.

Es deber del Gerente del Consorcio SICOV-CRC tomar las medidas pertinentes en el caso en el que se presente una violación a las políticas de seguridad de la información por parte de un personal externo de la compañía.

d. Comunicación de las Políticas de Seguridad de la Información

El manual de políticas de seguridad de la información debe ser comunicado de forma

apropiada a todos los colaboradores, contratistas, proveedores y demás personas que tengan algún tipo de relación con la información administrada por Consorcio SICOV-CRC.

Es deber de los colaboradores de la compañía leer los comunicados y atender a todas las reuniones que se establezcan para comunicar las políticas, los ajustes, remociones, cambios, entre otros, que se realicen sobre las políticas de Seguridad de la Información.

Es deber del Oficial de Seguridad de la Información informar sobre los cambios realizados a las políticas de forma oportuna.

e. Cumplimiento de las Políticas de Seguridad de la Información

Las políticas de seguridad de información de Consorcio SICOV-CRC han sido diseñadas considerando las medidas de protección establecidas en las leyes y regulaciones de la República de Colombia, alineadas con las mejores prácticas de la industria y teniendo en cuenta los lineamientos establecidos para el Consorcio SICOV-CRC.

Estas políticas son de obligatorio cumplimiento para los colaboradores, contratistas y terceras partes, su no cumplimiento acarreara las sanciones disciplinarias correspondientes determinadas por el Comité de Riesgos y gestión de riesgos ejecutadas por el área de Talento Humano.

Son Usuarios todos los colaboradores y/o terceros que tienen acceso a la información de los procesos de la organización, los cuales deben cumplir las políticas, procedimientos, manuales, lineamientos y toda la información documentada del proceso de seguridad de la información.

Los usuarios de Consorcio SICOV-CRC deben reportar cualquier incidente de seguridad de la información al correo electrónico del oficial de seguridad de la información de acuerdo con lo establecido en el procedimiento de gestión de incidentes.

2. Revisión de las Políticas de Seguridad de la Información

El Comité de Riesgos revisará las políticas de Seguridad de la Información periódicamente a intervalos planificados como mínimo una vez al año, o cuando sea requerido, con el fin de asegurar su conveniencia, adecuación, eficacia y la continuidad del negocio.

1.6.2. Organización de la Seguridad de la Información

1.6.2.1. *Organización interna*

Consorcio SICOV-CRC define un marco de referencia para gestionar y controlar la implementación y operación de seguridad de la información a nivel interno.

- **Separación de deberes**

Consorcio SICOV-CRC define y separa los deberes y las áreas de responsabilidad de seguridad de la información minimizando las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de información.

Los colaboradores y terceros tendrán deberes determinados sobre la Seguridad de la Información según su rol y su cargo, separando las responsabilidades entre ellos según corresponda a cada cargo y función.

- **Contacto con las Autoridades**

Consorcio SICOV-CRC mantendrá contacto apropiado, constante y oportuno con las autoridades pertinentes (civiles, militares, de supervisión de servicios públicos, emergencia, salud y seguridad, entre otras), que aseguren la continuidad del negocio y preservar la seguridad de la información. Este contacto se realizará según el tipo de emergencia presentada y según la aprobación de la Alta Dirección según la gravedad del caso.

Es deber de la Gerente del Consorcio SICOV determinar a cuál entidad se debe llamar según el caso.

Se cuenta con una matriz denominada " Listado de autoridades y grupos de interés" y se mantendrá actualizada por el Oficial de seguridad de la información.

- **Contacto con Grupos de Interés Especiales**

Consorcio SICOV-CRC, mantendrá contacto y/o establecerá acuerdos con grupos de interés especial tales como foros, sitios, redes sociales y/o asociaciones profesionales especializadas en seguridad de la información y apoyará a los colaboradores que requieran de la participación o interacción con los mismos.

El Oficial de Seguridad de la Información determinará los Grupos de Interés

Especiales a los cuales se les realizará una suscripción vía correo electrónico para recibir la información actualizada en cuanto a cambios en la seguridad de la información.

Es deber del Oficial de Seguridad actuar de forma oportuna según los reportes recibidos por parte de los Grupos de Interés Especial de forma oportuna.

Es deber del personal interno de la compañía realizar los cambios o ajustes que se requieran según lo reportado por parte del Oficial de Seguridad de la Información.

Es deber del equipo de Infraestructura realizar los ajustes en la tecnología que maneja Consorcio SICOV-CRC a partir de los reportes recibidos por parte del Oficial de Seguridad de la Información según lo reportan los grupos de interés especial.

Esta matriz se almacena en el documento *Listado de autoridades y grupos de interés*

- **Seguridad de la Información en la Gestión de Proyectos**

Consorcio SICOV-CRC incluirá y tratará la seguridad de la información en la gestión de proyectos que se realicen para la operación actual y futura del negocio, por medio de los requisitos mínimos de seguridad que deben cumplir los proyectos, así como los riesgos asociados a los mismos.

Así mismo, Consorcio SICOV-CRC garantizará que la información que se levante, se cree o se requiera para la ejecución y seguimiento del proyecto por parte del proceso de Gestión de proyectos se encuentre debidamente salvaguardada.

Es deber del Oficial de seguridad de la información garantizar el levantamiento de los requerimientos de Seguridad de la Información en cada proyecto que se ejecute en la compañía.

1.6.2.2. *Dispositivos móviles y teletrabajo*

Consorcio SICOV-CRC asegura la información manejada durante el teletrabajo y el uso de dispositivos móviles dentro de la organización, a través de las siguientes políticas:

1. Políticas para dispositivos móviles

Consorcio SICOV-CRC dispone de políticas y medidas de seguridad de soporte para el uso de dispositivos móviles dentro de las instalaciones en donde se procese la información, con el fin de gestionar de forma adecuada los riesgos que pueden presentarse por su uso en las operaciones del negocio.

La conexión de los dispositivos móviles que ingresen a Consorcio SICOV-CRC se realizará a través de las redes controladas por los segmentos de los equipos de Consorcio SICOV-CRC.

Los dispositivos móviles que correspondan a la operación Consorcio SICOV-CRC y que sean propiedad de la compañía, podrán ser monitoreados por el Oficial de Seguridad de la Información según se solicite por correo electrónico y con el apoyo del proceso de Gestión Tecnológica para escalar privilegios en el teléfono y acceder a las distintas Bases de Datos de los aplicativos, para tal fin, se tendrán dispositivos Android en dichas terminales.

La Gerencia de Consorcio SICOV autorizará el uso de dispositivos móviles al personal del NOC/SOC y sus visitantes por medio de un correo electrónico al Oficial de Seguridad de la Información.

2. Políticas para teletrabajo

Consorcio SICOV-CRC ajustado a las normas colombianas, dispone de herramientas que garantizan el uso adecuado de las políticas y medidas de seguridad para proteger la información que se accede, procesa y almacena a través del uso de teletrabajo.

Es deber del Oficial de Seguridad de la Información definir los controles que se aplicarán a las herramientas tecnológicas, instrumentos, equipos, conexiones y programas asignados al personal que realiza funciones en modalidad de trabajo en casa.

Es deber de la Gerencia de Consorcio SICOV es informar de forma oportuna sobre el rol que el personal de Teletrabajo realizará dentro de la organización en caso de que aplique.

Los colaboradores que operen bajo la modalidad de teletrabajo tendrán en los dispositivos que les asigna la compañía con los controles de seguridad correspondientes.

1.6.3. Políticas de Seguridad de los Recursos Humanos

1.6.3.1. *Antes de asumir el empleo*

El proceso de Talento Humano asegurará que los aspirantes a los cargos que hacen parte de Consorcio SICOV-CRC son los adecuados para los roles y responsabilidades que van a desempeñar, de acuerdo con lo establecido en los procedimientos de Talento

humano.

1. Atracción y Selección del Personal

En Consorcio SICOV-CRC se verificarán todos los antecedentes de todas las personas que aspiren a cargos, empleos o vacantes disponibles, de acuerdo con la legislación, normas, ética, requisitos del negocio, clasificación de la información, accesos a sistemas de información y riesgos asociados a los mismos.

Es deber de la Encargado del Talento Humano realizar la revisión de todos los antecedentes disciplinarios y penales de los candidatos que apliquen a la compañía. Es deber de los aspirantes a un cargo de Consorcio SICOV-CRC entregar la totalidad de la información solicitada de forma verídica de las referencias personales y profesionales. Es deber de la Encargado del Talento Humano validar las referencias personales y laborales de los aspirantes.

2. Términos y Condiciones del Empleo

En Consorcio SICOV-CRC se estipularán contratos con todo empleado o tercero que tenga algún tipo de relación contractual con la organización, en el cual se definirán todas las responsabilidades de estos y de la entidad frente a seguridad de la información.

Es deber de la Gerencia de Consorcio SICOV y de la Encargado del Talento Humano establecer las cláusulas de confidencialidad, protección de datos y entrega de información con los terceros.

Es deber del Líder de Proceso determinar el nivel de acceso a la información a la que tendrá cada empleado según el rol que le corresponda dentro de la organización.

Es deber del oficial de seguridad de la Información autorizar el nivel de acceso a la información a la que tendrá cada empleado según el rol que le corresponda dentro de la organización.

3. Acuerdos de confidencialidad

En Consorcio SICOV-CRC todos los colaboradores y terceros que tengan acceso a la información de los procesos de la organización deben firmar un acuerdo de confidencialidad con la intención de garantizar que la información no sea publicada o conocida por personal no autorizado. Quienes incumplan estos acuerdos o compromisos de confidencialidad serán sancionados de acuerdo con el régimen disciplinario, establecido al interior de Consorcio SICOV-CRC, sin perjuicio de las reclamaciones que sean pertinentes.

Es deber del Encargado de Talento Humano asegurar el cumplimiento de la política con los colaboradores y de la Gerente de Consorcio SICOV con los terceros.

1.6.3.2. *Durante la ejecución del empleo*

La Gerencia de Consorcio SICOV debe asegurar que los colaboradores y terceros tomen conciencia y cumplan las responsabilidades de seguridad de la información.

1. Responsabilidades de la Empresa

Consorcio SICOV-CRC exigirá a los colaboradores y terceros el cumplimiento de las políticas y procedimientos de seguridad de la información establecidos, según lo establecido en los contratos de trabajo y demás documentos asociados.

Es deber de la Gerencia de Consorcio SICOV, y del Oficial de Seguridad de la Información y del Encargado del Talento Humano exigir el cumplimiento de las políticas a los colaboradores y terceras partes según se establece en los acuerdos contractuales.

2. Educación, Formación y Concientización sobre la Seguridad de la Información

Todos los colaboradores de Consorcio SICOV-CRC y terceros serán concienciación, sensibilizados y capacitados en políticas, procedimientos, manuales, lineamientos y toda información documentada de seguridad de la información pertinente, y en sus actualizaciones, de acuerdo con las necesidades, funciones y roles asumidos con Consorcio SICOV-CRC. Se dará a conocer a través de las recomendaciones de seguridad por la intranet, inducción a colaboradores, capacitaciones anuales, entre otros.

Es deber de todos los colaboradores tomar los cursos de sensibilización y capacitación que organice la compañía y aprobar los exámenes que se realicen dentro de los mismos en los tiempos establecidos para tal fin.

Es deber del Encargado del Talento Humano preparar, diseñar y ejecutar el material de formación y concienciación para colaboradores y terceros.

Es deber del Encargado del Talento Humano realizar las sensibilizaciones iniciales a los colaboradores, así como también, tomar las medidas pertinentes en contra de los colaboradores que no aprueben los exámenes de sensibilización y capacitación.

3. Proceso Disciplinario

Consorcio SICOV-CRC a través de Talento Humano asegurará el cumplimiento del *Reglamento Interno de Trabajo,* como medida de control disciplinario en la organización en caso de violaciones o infracciones, en las cuales se contemplan las relacionadas con seguridad de la información por parte de colaboradores.

La Gerencia de Consorcio SICOV tomará las medidas pertinentes con los proveedores y terceros que incumplan con las políticas de seguridad de la información.

1.6.3.3. *Terminación y cambio de responsabilidades de empleo o labor contratada*

La Gerencia de Consorcio SICOV con el apoyo del Oficial de Seguridad de la Información definirán, comunicarán y velarán por el cumplimiento de las responsabilidades y deberes de seguridad de la información que permanecen válidos para los colaboradores y terceros después de terminación del contrato laboral o cambio de cargo.

Es deber del Encargado del Talento Humano reportarle al proceso de Gestión Tecnológica (Infraestructura) los retiros de personal y cambios de cargo que se presenten de forma oportuna.

Es deber del proceso de Gestión Tecnológica (Infraestructura) dar de baja todos los accesos del personal que se retira de la compañía.

Es deber del Oficial de Seguridad revisar los nuevos accesos y solicitar la depuración y el ajuste de permisos al proceso de Gestión Tecnológica (Infraestructura).

1.6.4. Política de Gestión de Activos

1.6.4.1. *Responsabilidad por los activos*

Todos los colaboradores y terceros que tengan algún tipo de relación contractual con Consorcio SICOV-CRC deberán proteger los activos de información de acuerdo con las políticas y buenas prácticas de seguridad de la información establecidas. Los líderes de proceso identificarán y asignarán los propietarios y responsabilidades sobre los activos de información de tal manera que contribuyan al mantenimiento e implementación de controles adecuados para su protección.

1. Inventario de activos

En Consorcio SICOV-CRC, se identificarán los activos de información y se mantendrán en un inventario actualizado de los mismos con el fin de llevar un control de estos teniendo cada uno de los componentes identificados de forma clara y el proceso al cual pertenecen

Es deber de los colaboradores de la compañía conocer y reportar de forma oportuna los activos de información que están bajo su custodia.

Es deber del Oficial de Seguridad de la Información mantener el listado actualizado de los activos.

2. Activos de Información

En Consorcio SICOV-CRC se categorizan los activos de información de la siguiente manera:

- Personas
- Hardware
- Software
- Servicios

3. Propiedad de los Activos

a. Propietario de los Activos

Todos los activos de información de Consorcio SICOV-CRC y servicios de procesamiento de información tendrán asignado un propietario o responsable según la responsabilidad que tenga sobre el activo dentro del proceso definido previamente. Este propietario estará indicado en el Inventario de Activos y es deber del mismo dar buen uso de los activos de información que tenga a su cargo.

Cualquier colaborador o tercero podrá tener propiedad sobre activos de información y deberán dar uso adecuado y seguro de los mismos.

b. Responsabilidades del Propietario de los Activos de Información

Es responsabilidad del propietario, funcionario o tercero proteger los activos asignados a su área o regional respectiva e implementar los controles necesarios para garantizar la seguridad de estos. Siguiendo los lineamientos indicados en esta política.

c. Asignación de la Propiedad y Delegación de Activos de Información

En Consorcio SICOV-CRC los propietarios de la información podrán delegar a otros colaboradores o terceras actividades el tratamiento de los activos de

información, pero la responsabilidad no se delega y se conserva en el propietario.

4. Uso Aceptable de los Activos

Es imperativo que los colaboradores, terceros y partes interesadas den uso adecuado y seguro de los activos de la Información, en cumplimiento de las políticas de seguridad de la información y de las normas o legislación aplicable.

El Oficial de Seguridad de la Información tomará todas las medidas para garantizar que los activos se utilizan de forma adecuada y segura y que los mismos no se utilizan con la finalidad de afectar la disponibilidad, integridad y confidencialidad de la información.

5. Prohibiciones en el uso de activos de información

En Consorcio SICOV-CRC se restringe el uso de activos de información, limitándose únicamente al uso conforme al cumplimiento de las funciones estipuladas en los procesos corporativos definidos.

Los colaboradores de la compañía no podrán compartir los activos de información con terceros no autorizados.

En caso de que se encuentre un incumplimiento, el Oficial de Seguridad de la Información le reportará al Encargado del Talento Humano para que tome las medidas pertinentes.

6. Auditoría y privacidad sobre los activos

En Consorcio SICOV-CRC, se establece el derecho de auditar, en cualquier momento, con o sin previo aviso, el uso de los activos de información en conocimiento a colaboradores y terceros.

El oficial de Seguridad de la Información podrá monitorear la información que se almacena en los dispositivos corporativos que hayan sido asignados a colaboradores y terceros.

Es deber de los colaboradores acatar las medidas disciplinarias a las que haya lugar según su actuar.

7. De la responsabilidad de los usuarios sobre los activos

Todos los colaboradores que hacen uso de los activos de información de Consorcio SICOV-CRC son responsables de dar estricto cumplimiento a las Políticas, Normas y Procedimientos de Seguridad de la Información de la

empresa.

El Oficial de Seguridad de la Información velará por la revisión del cumplimiento y deberá reportar a la Gerencia de Consorcio SICOV y/o al Encargado del Talento Humano sobre cualquier mal uso que se encuentre sobre los activos de información con la finalidad de que las mismas tomen las medidas del caso a las que haya lugar.

8. Del uso de información privilegiada

En Consorcio SICOV-CRC de acuerdo con la clasificación de la información, se considera información privilegiada la información confidencial y de uso interno. En consecuencia, ningún colaborador del Consorcio SICOV-CRC podrá suministrar a terceros datos o información privilegiada, salvo autorización expresa del líder de proceso, la cual se otorgará únicamente en aquellos casos que lo ameriten, y por finalidad ajena a especulación. Tampoco podrá utilizar dicha información en beneficio propio o de terceros.

En caso de incumplimiento de esta política, el Oficial de Seguridad de la Información realizará el reporte al Encargado del Talento Humano quien procederá a aplicar el procedimiento de medidas disciplinarias sobre los colaboradores que incumplan.

9. Devolución de activos

Todos los colaboradores y terceros al cambiar de cargo, terminar su empleo, contrato o acuerdo con Consorcio SICOV-CRC, deben devolver todos los activos de información que se encuentren asignados a su cargo.

Una vez se devuelvan los activos, el responsable de Infraestructura indagará con el jefe inmediato si es necesario realizar Copia de Seguridad o Backup de la información almacenada en el correo o en las plataformas correspondientes, una vez se realice Copia de Seguridad o Backup, en el caso en el que aplique, se procederá a realizar borrado seguro de la información que se haya almacenado en este equipo y/o destrucción de medios tecnológicos según sea el caso, siendo responsabilidad del proceso de Gestión Tecnológica (Infraestructura) la ejecución de dicha tarea.

10. Retiro de activos de forma definitiva

Todos los activos que se retiren de la compañía por daño deberán pasar por el siguiente proceso.

1) Se revisará internamente o por partes externas si el dispositivo puede

ser reparado por parte del tercero o el Responsable de Infraestructura.

2) Se ejecutará el procedimiento de borrado seguro de activos de información. Esta actividad de borrado la realizará por el proceso de Gestión Tecnológica (Infraestructura).

11. Retiro de activos de forma parcial

Todos los activos que se retiren de la compañía para trabajo desde otro sitio deberán cumplir con las siguientes especificaciones:

1) El usuario deberá tener toda la información referente al proceso que ejecuta, del equipo asignado, en una UNIDAD DE RED asignada por la compañía. El funcionario deberá consultar y actualizar toda la información en este medio únicamente.
2) En caso de pérdida, daño o robo, el funcionario deberá solicitar al proceso de Gestión Tecnológica (Infraestructura) el restablecimiento de todas las contraseñas que usaba para los distintos accesos a los aplicativos.

12. Clasificación de la Información

a. Aspectos generales de clasificación de la información

En Consorcio SICOV-CRC se clasificará la información que hace parte de las operaciones conforme a la necesidad y prioridad.

Es deber de todos los colaboradores dar cumplimiento a los niveles de clasificación de la información establecidos por cada líder de proceso según la sensibilidad de esta.

b. Niveles de clasificación de la información

En cumplimiento de los criterios mencionados, la información de Consorcio SICOV-CRC se clasifica en: confidencial, uso interno y pública.

Información Confidencial

Aquella información que por su contenido solo interesa a quienes va dirigido y cuya divulgación no autorizada puede ocasionar perjuicios a determinadas áreas o colaboradores de GSE.

Información Uso Interno

Es toda información y documentación generada en los procesos la cual contempla

las estrategias o lineamientos internos de nivel de la organización

Información Pública

Es toda aquella información y documentación generada en los procesos u obtenida por los colaboradores en sus actividades, con fines públicos y cuya divulgación a terceros no afecta los intereses de la organización, de los clientes y/o usuarios.

c. Directrices para clasificar la información

Las Gerencia de Consorcio SICOV y el Oficial de Seguridad de la Información son los encargados de establecer las directrices para la clasificación de la información, mantenimiento y el nivel de seguridad de esta.

Es deber de todos los colaboradores dar cumplimiento a la clasificación de la información y a garantizar la confidencialidad e integridad que la misma demanda según el nivel asignado, usando todos los recursos humanos y tecnológicos para tal fin.

d. Períodos para la Clasificación de la Información

Cada año el Oficial de Seguridad de la Información, el Encargado de Sistemas de Gestión y los líderes de proceso revisarán y actualizarán la clasificación de la información que se gestiona en cada uno de los procesos. El resultado de su análisis será aprobado por el líder de proceso, para su posterior publicación de acuerdo con el sistema integrado de gestión.

Es deber de los colaboradores aplicar todas las medidas necesarias para cumplir con los nuevos lineamientos aplicados a las políticas, sin perjuicio de prácticas previas que realizarán.

13. Etiquetado de la Información

En Consorcio SICOV-CRC se etiquetará la información de todos los procesos de acuerdo con el nivel de clasificación establecida según el tipo de información que se almacene y que se registre en los distintos formatos.

Es deber del Oficial de Seguridad verificar que la información está debidamente etiquetada.

Es deber de los colaboradores reportar si existe más información que deba

ser etiquetada con otra clasificación y de dar cumplimiento cabal a los controles que se requieran según la clasificación y el etiquetado de la información.

14. Manejo de Activos

En Consorcio SICOV-CRC se manejarán los activos de información que hacen parte de la operación del negocio de acuerdo con el nivel de clasificación establecido.

Es deber de todos los colaboradores dar un uso seguro y adecuado de los activos de información según su clasificación y reportar de forma directa al Oficial de Seguridad de la Información sobre cualquier riesgo o incidente que ocurra con los activos de información que se manejen bajo su cargo y custodia.

Es deber del Oficial de Seguridad velar por el adecuado cumplimiento del manejo de los activos, en caso de encontrar un mal uso de estos se deberán reportar al Encargado de Talento Humano y a la Gerencia de Consorcio SICOV sobre dicho hallazgo para que se tomen las medidas pertinentes para tal fin.

15. Manejo de Medios

El Consorcio SICOV-CRC no se divulgará, modificará, retirará o destruirá la información que se almacenan en los diferentes medios (físicos o electrónicos), sin la debida autorización del responsable de esta.

a. Gestión de medios removibles

El Consorcio SICOV-CRC se gestionarán los medios removibles que hacen parte de la operación del negocio de acuerdo con el nivel de clasificación establecida.

Ningún funcionario de Consorcio SICOV-CRC o tercero que tenga acceso a los sistemas informáticos propios de la organización podrá utilizar medios removibles en los sistemas informáticos de Consorcio SICOV-CRC en ninguna modalidad que permita el mismo dispositivo ahora y en el futuro.

Es deber del Responsable de Infraestructura implementar las políticas del directorio activo para realizar el bloqueo de los puertos de medios removibles, así como los elementos de Hardware que permitan insertar y utilizar los mismos según se identifique.

b. Disposición de los medios

En Consorcio SICOV-CRC se dispondrán de manera segura de los medios que ya no se requieran para las operaciones del negocio tal cual se encuentra establecido en el procedimiento de borrado seguro.

Los colaboradores no podrán realizar disposición de medios de forma autónoma.

c. Transferencia de medios físicos

En Consorcio SICOV-CRC se asegurará que los medios que contengan información de las operaciones del negocio se mantengan y protejan de manera segura contra acceso no autorizado, uso indebido o corrupción durante el transporte de los mismos.

No se permite por parte de ningún funcionario de la compañía o tercero la entrega de información por medios electrónicos físicos, los usuarios deben utilizar los canales seguros designados para tal fin.

d. Almacenamiento de información en medios o repositorios

Los líderes de proceso deben revisar mensualmente o cuando sea necesario la capacidad del almacenamiento de la información de sus procesos en los repositorios asignados (carpetas compartidas, discos duros o externos, entre otros), con el fin de solicitar con anticipación y debida justificación de la ampliación de disponibilidad de espacio en los sistemas de información.

Las carpetas asignadas a cada proceso en la unidad de red son el único repositorio autorizado por la compañía para poder salvaguardar la información de forma segura por parte de los colaboradores de la compañía y los colaboradores deberán usarla de manera adecuada.

1.6.5. Política de Control de Acceso

El Consorcio SICOV-CRC se controlará el acceso a la información y a las instalaciones que hace parte de sus operaciones y características de su negocio por medio de perfiles y roles según se indique dentro de los procesos de negocio y los procesos operativos, bajo las autorizaciones correspondientes.

1.6.5.1. *Requisitos del Negocio para Control de Acceso*

El Consorcio SICOV-CRC se limitará el acceso a la información e instalaciones de procesamiento de información (Áreas de la Oficina Principal, Centros de Cómputo Principal y Alterno), sólo a personal autorizado.

1. Directrices de Control de Acceso

El Consorcio SICOV-CRC se establece la política de control de acceso como directriz para controlar el acceso de personal no autorizado a la información y a las instalaciones de la organización. Únicamente tendrá acceso el personal autorizado a los centros de procesamiento de Datos. Estos accesos estarán registrados en las bitácoras correspondientes.

Los colaboradores tendrán accesos únicamente a la información que requieren consultar según su rol y según su cargo dentro de la organización, en ninguna circunstancia podrán consultar información fuera de sus funciones que tenga una clasificación no correspondiente con su perfil.

En cualquier momento y sin previo aviso, el Oficial de Seguridad de la Información puede revocar los derechos de acceso con la finalidad de ajustar los privilegios y dejarlos con el mínimo uso aceptable posible, si se evidencia una posible infracción a las políticas de seguridad de la información establecidas en este documento.

2. Distribución de la Información

El Consorcio SICOV-CRC se distribuirá la información que hace parte de las operaciones del negocio sólo a personal autorizado tanto a nivel interno como a nivel externo de acuerdo con la clasificación de la información descrita en el presente documento.

Los colaboradores no podrán utilizar su correo electrónico, ni ningún medio para enviar información sensible a usuarios no autorizados por los líderes de proceso y que no tengan relación con el proceso que ejecutan.

El Oficial de Seguridad podrá monitorear los canales de comunicación para certificar que ningún funcionario realice envíos a otros destinatarios distintos de lo establecido en sus procesos, en caso de incumplirse se le informará a la Gerencia de Consorcio SICOV y al Encargado del Talento Humano para que tomen las medidas correspondientes.

3. Acceso a Redes y a Servicios de Red

En Consorcio SICOV-CRC, el oficial de seguridad de la información establecerá los permisos de acceso de los usuarios a redes y servicios de red que sean autorizados para el desarrollo de funciones y podrá bloquear todos los accesos innecesarios para el desarrollo de sus funciones.

4. Uso de Internet

En Consorcio SICOV-CRC se limitará y controlará el acceso a Internet únicamente para la realización de las labores corporativas con permisos de acceso restringidos de los usuarios en desarrollo de sus funciones.

Los usuarios no podrán navegar a páginas y sitios con contenido que sea ajeno al ejercicio de sus funciones, entre los que se encuentran y no limitándose a:

- Redes Sociales o Piratería
- Pornografía o Drogas
- Streaming

Los usuarios podrán navegar a sitios Gubernamentales, de noticias o de pagos electrónicos siguiendo los lineamientos de buen ambiente laboral del área de Talento Humano.

5. Autenticación de Usuarios para Conexiones Externas

El Consorcio SICOV-CRC controlará el acceso remoto a través de la implementación de mecanismos de autenticación de usuarios con el controlador de dominio y por medio de acceso por VPN, al cual tendrán acceso únicamente los colaboradores que requieran trabajar desde fuera de la oficina. Los colaboradores que requieran de este tipo de accesos deberán solicitarlo a la Gerencia de Consorcio SICOV quien dará el aval para las conexiones.

La autenticación se realizará por medio del Directorio Activo en el sistema de acceso VPN y todos los colaboradores autorizados para trabajo remoto tendrán dicha restricción.

Es deber del proceso de Gestión Tecnológica (Infraestructura) establecer los permisos pertinentes según solicitud de la Gerencia de Consorcio SICOV.

6. Identificación de los Equipos en las Redes

En Consorcio SICOV-CRC se mantendrán identificados los equipos tecnológicos que se conecten a las redes corporativas por medio de un nombre finalizando en GD.

Los equipos así mismo se identificarán en la consola de Antivirus por su nombre y su dirección IP con el fin de conocer cómo se están viendo dentro de la red y que políticas están implementándose.

Es deber del proceso de Gestión Tecnológica (Infraestructura) implementar la identificación de los equipos.

7. Protección de los Puertos de Configuración y Diagnóstico Remoto

En Consorcio SICOV-CRC se controlará el acceso lógico y físico a los puertos de configuración y diagnóstico remoto a través de usuarios, contraseñas y procedimientos que describen el acceso físico a los mismos.

Así mismo, ningún funcionario que no esté autorizado podrá acceder remotamente a realizar monitoreo o diagnóstico de equipos según el caso.

Es deber del proceso de Gestión Tecnológica (Infraestructura) realizar el bloqueo de puertos no utilizados para el desarrollo de las funciones y de realizar la configuración y el diagnostico remoto.

Ningún usuario podrá utilizar técnicas de apertura de puertos para poder violar las restricciones de su perfil o degradar la seguridad de la información en la compañía.

8. Control de Conexión a las Redes

El Consorcio SICOV-CRC se restringirá y controlará la capacidad de los usuarios autorizados previamente para el acceso a las redes de acuerdo con las políticas de control de acceso y características del negocio.

Ningún funcionario tendrá acceso a sitios externos a los autorizados de forma expresa según su cargo.

Los terceros tendrán acceso a las redes corporativas internas de la compañía mediante autorización expresa de la Gerencia de Consorcio SICOV según la actividad a desempeñar, en todo caso solo podrán usar las redes Wifi de invitados.

9. Control del Enrutamiento en la Red

El Consorcio SICOV-CRC se controlará el enrutamiento de las redes que permitan asegurar las conexiones de los dispositivos electrónicos y los flujos de la información de acuerdo con las políticas de control de acceso establecidas de Consorcio SICOV-CRC.

Ningún funcionario tendrá accesos a servicios proxy o similares que enruten su tráfico por otro tipo de servicios que no estén autorizados o controlados por la compañía.

Los terceros tendrán sus equipos enrutados por una red diseñada para estar separada de los servidores misionales de la organización y deberán cumplir con dichos lineamientos salvo autorización expresa de la Gerencia de Consorcio SICOV.

1.6.5.2. *Gestión de Acceso de Usuarios*

El Consorcio SICOV-CRC se asegurará el acceso de los usuarios autorizados y autenticados a las plataformas de la siguiente manera:

1. Registro y cancelación del registro de usuarios

El Consorcio SICOV-CRC se controlará el registro y cancelación de usuarios a los sistemas y servicios de información según inactividad del usuario o según lo reporte el área de Talento Humano.

El personal interno de Consorcio SICOV-CRC no deberá compartir sus usuarios con otras personas internas o externas durante la existencia del mismo usuario.

El personal externo de la compañía no tendrá usuarios dentro de los sistemas de Consorcio SICOV-CRC con excepción del equipo Gestión Tecnológica (Infraestructura) y del personal de soporte.

Es deber del Encargado de Infraestructura crear los usuarios en el directorio activo, así como desactivarlos según lo reporte del Encargado de Talento Humano. Así también, velar por la deshabilitación de los usuarios en el directorio activo según se reporte, así mismo, debe velar por la oportuna creación de usuarios en el Directorio Activo según sea necesario.

Es deber de la Gerencia de Consorcio SICOV autorizar la cancelación del registro de los usuarios de la plataforma que estén inactivos según el tiempo que la misma estipule. Es deber del Oficial de Seguridad de la Información velar por la adecuada ejecución de la cancelación de usuarios de la plataforma de forma mensual.

2. Creación de usuarios especiales

Consorcio SICOV-CRC podrá generar usuarios especiales cuyas características difieran de las normalmente definidas para usuarios finales.

Dichos usuarios especiales se definirán con el objetivo de atender aspectos tales como la gestión de aplicativos, propietarios de esquema en base de datos, o a nivel de red, usuarios específicos de área de acuerdo con la gestión requerida y aprobada. Los mismos serán monitoreados de forma automática, y sus acciones serán reportadas al Oficial de Seguridad de la Información.

La Gerencia de Consorcio SICOV solicitará y autorizará, mediante correo electrónico dirigido al Responsable de Infraestructura, la creación de estos usuarios especiales según sea el caso.

Aparte de las autorizaciones que asignen desde Gerencia, ningún funcionario o tercero tendrá usuarios especiales.

3. Suministro de Acceso de Usuarios

Los responsables de los sistemas de información deben suministrar, asignar o revocar de manera formal los derechos de acceso de los usuarios a los sistemas y servicios de información, previa solicitud de la responsable de talento humano.

Los colaboradores y terceros deben utilizar únicamente su usuario asignado y no deberán prestarlo, venderlo, entregarlo a cualquier otro funcionario o tercero.

El responsable de Infraestructura deberá asignar o deshabilitar los usuarios según se reporte por parte del área de talento Humano.

4. Gestión de Derechos de Acceso Privilegiado

El Consorcio SICOV-CRC se restringirá y controlará la asignación y uso de los derechos de acceso privilegiado a los sistemas de información, según el principio de mínimo privilegio, los cuales serán implementados por el Responsable de Infraestructura.

Es deber de los colaboradores que cuenten con accesos privilegiados mantener la integridad del sistema de información.

Adicionalmente, ningún funcionario deberá instalar programas o aplicativos que no sean laborales o que no apliquen para sus funciones.

5. Gestión de Información de Autenticación Secreta de Usuarios

El Consorcio SICOV-CRC se controlará la asignación de información de autenticación secreta.

Los usuarios que reciban su contraseña por correo electrónico deberán realizar el cambio de contraseña de manera inmediata, por solicitud del sistema informático, utilizando contraseñas con las restricciones establecidas en el presente documento.

En caso de olvido de la información de Autenticación, el usuario deberá reportarle el caso directamente al Responsable de Infraestructura quien realizará el cambio de las credenciales de forma adecuada.

6. Revisión de los Derechos de Acceso de Usuarios

Los responsables de los activos de información deberán revisar periódicamente los derechos de acceso de los usuarios autorizados para ingresar a los sistemas de información de Consorcio SICOV-CRC.

Todo funcionario deberá reportar de forma oportuna los cambios de accesos que tenga para su respectivo ajuste, los colaboradores deberán tener derechos de acceso bajo mínimo privilegio según las funciones de su cargo.

7. Retiro o Ajuste de los Derechos de Accesos

Los derechos de acceso de los colaboradores y terceros (Proveedores, Contratistas o Pasantes), a la información, sistemas de información y a las instalaciones de Consorcio SICOV-CRC deben ser retirados inmediatamente, de forma total, en caso de haber terminado su contrato o acuerdo.

En caso de cambio de funciones o de cargo, se inactivarán y se realizarán los ajustes pertinentes a las credenciales asignadas.

Los colaboradores no deberán solicitar los usuarios de colaboradores ya retirados, sino que deberán solicitar la información almacenada en sus correos electrónicos y configuración de alias de correos en el caso de ser necesario.

1.6.5.3. *Responsabilidades de los Usuarios sobre el Control de Acceso*

El Consorcio SICOV-CRC se exigirá y pedirá cuentas a los usuarios de sistemas de información sobre la salvaguarda de su información de autenticación y el cumplimiento de las políticas establecidas.

1. Uso de Información de Autenticación Secreta

El Consorcio SICOV-CRC exigirá a colaboradores y terceros autorizados el cumplimiento de las buenas prácticas sobre el uso de la información de autenticación secreta (Nombres de Usuario, Contraseñas y Tokens), para el ingreso a los sistemas de información.

Los usuarios deberán utilizar claves que cumplan con las siguientes características:

- Claves de 10 o más caracteres

- No repetir las ultimas 10 claves
- Las claves deberán contener como mínimo: Letra Mayúscula, Minúscula, números y caracteres especiales.
- Las contraseñas deberán cambiarse en un tiempo no mayor a 90 días.

Es deber del Responsable de Infraestructura implementar las políticas pertinentes dentro del directorio activo que permitan cumplir con el control anteriormente mencionado y garantizar que las contraseñas se almacenan con algoritmos de cifrado de una sola vía y que no presenten vulnerabilidades conocidas.

Es deber del proceso de Gestión Tecnológica (infraestructura) entregar las credenciales de acceso a los usuarios con la parametrización de exigir el cambio de clave después de la primera validación.

Es deber del Oficial de Seguridad de la Información solicitar el cambio de credenciales de correo de un usuario puntual en el caso en el que se encuentre que dicha cuenta fue comprometida en un ataque hacia otro sitio.

Es deber del Oficial de Seguridad de la Información solicitar la forma en la cual las credenciales de acceso se almacenaran dentro de los aplicativos de Consorcio SICOV-CRC y garantizar que se cumple con lo establecido en esta política.

Los usuarios no deberán reutilizar las mismas credenciales dentro de los distintos sistemas informáticos a los que tenga acceso a nivel laboral. No deberán compartir sus claves con ninguna persona de forma interna o externa, ni deberán anotarla en ningún documento físico o electrónico salvo que se trate del software de administración de contraseñas autorizado por Consorcio SICOV-CRC para su uso.

1.6.5.4. *Control de Acceso a Sistemas y Aplicaciones*

Los propietarios y responsables de los activos de información deben evitar el acceso no autorizado a sus sistemas de información y aplicaciones.

1. Restricción de Acceso a la Información

El acceso a la información y sistemas de información será restringido de acuerdo con las políticas de control de acceso establecidas por Consorcio SICOV-CRC.

Ningún colaborador podrá acceder a la información a la cual no deba tener acceso. En caso de que el funcionario evidencie que cuenta con dicho acceso, este deberá reportar el caso al Oficial de Seguridad de la Información solicitando la inactivación de las credenciales respectivas.

2. Ingreso Seguro

El acceso a los sistemas de información de Consorcio SICOV-CRC será controlado, por medio de mecanismos de autenticación, basados en usuario y contraseña.

Para el acceso a las oficinas los colaboradores deberán registrarse en el sistema biométrico de acceso y control, en el caso de no tener registrada su información biométrica deberá registrar su acceso en las planillas dispuestas para tal fin y deberá solicitar el ingreso al Encargado de Gestión Tecnológica.

3. Uso de Programas Utilitarios Privilegiados

Los colaboradores de la compañía deberán tener instalados únicamente los programas autorizados con los permisos necesarios para su ejecución y de requerirse un programa adicional será revisado por el Gerente del Consorcio SICOV y el Oficial de Seguridad de la Información.

4. Control de Acceso a Códigos Fuente de Programas

En Consorcio SICOV-CRC se restringirá el acceso a los códigos fuentes de los programas o desarrollos que hacen parte de las operaciones del negocio.

Los terceros que la Gerencia de Consorcio SICOV determine que deban desarrollar soluciones para la compañía deberán dar acceso al código fuente únicamente al personal que requiera trabajar en el desarrollo de sus funciones.

1.6.5.5. Política de Trabajo Remoto.

Establecer una modalidad de trabajo remoto para que los colaboradores de Consorcio SICOV-CRC puedan prestar sus servicios como una medida para garantizar la continuidad del negocio.

El Consorcio SICOV-CRC se controlará el acceso remoto a través de la implementación de mecanismos de autenticación de usuarios con el controlador de dominio y por medio de acceso por VPN, al cual tendrán acceso únicamente los colaboradores que requieran trabajar desde fuera de la oficina. Los colaboradores que requieran de este tipo de accesos deberán solicitarlo a la Gerencia de Consorcio SICOV quien dará el aval para las conexiones.

La autenticación se realizará por medio del Directorio Activo en el sistema de acceso VPN y todos los colaboradores autorizados para trabajo remoto tendrán dicha restricción.

Es deber del área del proceso de Gestión Tecnológica (Infraestructura) establecer los permisos pertinentes según solicitud de la Gerencia de Consorcio SICOV.

1.6.6. Política de Criptografía

Controles Criptográficos

En Consorcio SICOV-CRC se asegurará el uso apropiado y eficaz de la criptografía en sus operaciones con el fin de proteger la confidencialidad, autenticidad e integridad de la información.

1. Uso de Controles Criptográficos

En Consorcio SICOV-CRC se implementarán cifrados seguros con los controles adecuados que permitan proteger la información en las operaciones del negocio.

Absolutamente todos los sitios de Consorcio SICOV-CRC sean producción o pruebas, deberán tener certificado digital SSL con criptografía apropiada y fuerte con la finalidad de disminuir la probabilidad de que los clientes puedan verse afectados por ataques a los DNS y sean redirigidos a paginas falsas.

Los servicios de Consorcio SICOV-CRC públicos deberán ser accedidos de forma segura por medio de certificados digitales, de lo contrario deberán ser accedidos por medio de VPN para el caso de servicios que por necesidad de negocio no puedan asegurarse con certificado digital (HTTP, FTP, entre otros)

Todas las copias de respaldo deben estar cifradas con algoritmos de cifrado solidos que defina el Oficial de Seguridad de la Información y que ejecute el responsable de Gestión Tecnológica.

Los clientes u organizaciones que requieran consumir servicios de Consorcio SICOV-CRC deberán realizarlo por medio de enlaces dedicados, VPN o por medio de SSL únicamente, no se autorizarán consumos por otros medios salvo que los mismos tengan un nivel criptográfico adecuado para la ejecución de actividades.

2. Funciones y Responsabilidades de Cifrado

Todos los colaboradores serán responsables de cumplir las políticas de cifrado de la información en toda transmisión de información confidencial o de uso interno.
Todos los colaboradores y terceras partes deberán entregar la información sensible cifrada con algoritmos seguros, validados por el Oficial de Seguridad de la

Información y con claves robustas para tal fin.

1.7. Gestión de Llaves

En Consorcio SICOV-CRC se gestionarán las llaves criptográficas durante todo su ciclo de vida a través de la política de controles criptográficos, el cual menciona el uso, protección e intercambio de estas.

Es deber del Oficial de Seguridad de la Información definir los mecanismos de intercambio de llaves, los cuales deben ser seguros

Es deber del Encargado de Gestión Tecnológica implementar en los servidores el intercambio de llaves seguras según lo indiquen las normas y las buenas prácticas aplicables.

Es deber de los usuarios que intercambian información cifrada realizar de forma periódica, en un tiempo no mayor a 90 días, con los terceros el intercambio de llaves de cifrado.

1.8. Uso de Tokens y Firmas Digitales

El Consorcio SICOV-CRC se implementarán y mantendrán actualizados los Certificados de Firmas Digitales que se utilicen en las operaciones del negocio. Estos certificados deben ser autorizados por un ente certificador debidamente avalado, con el fin de evitar suplantaciones, fraudes electrónicos, entre otras amenazas, así mismo, se garantizará que el ente certificador cumpla con la totalidad de requisitos establecidos por organismos internacionales para la generación de las firmas digitales, evitando que el mismo genere las llaves públicas y privadas de los certificados que se instalen en los servidores de Consorcio SICOV-CRC.

Es deber del Responsable de Gestión Tecnológica almacenar en un único sitio seguro las claves privadas de las firmas digitales.

Los colaboradores que utilicen Firma Digital deberán proteger las llaves de cualquier modificación, perdida o alteración de la información.

Es deber del Oficial de Seguridad de la Información solicitar las firmas digitales con los parámetros necesarios para la operación del servicio de forma segura.

1.8.1. Política de Seguridad Física y del Entorno

1. <u>Áreas Seguras</u>

En Consorcio SICOV-CRC se prevendrá el acceso físico no autorizado, daño e interferencia de su información en sus instalaciones y áreas de procesamiento de información a través de controles de accesos biométricos.

Los colaboradores y terceros no deberán acceder a las áreas seguras de la compañía a menos que por el perfil de cargo estén autorizados para el desarrollo de sus funciones.

Las áreas seguras de Consorcio SICOV-CRC son el cuarto de comunicaciones de la compañía y el NOC/SOC.

2. Perímetro de Seguridad Física

En Consorcio SICOV-CRC se establecerán y usarán los perímetros de seguridad física para proteger las áreas críticas del negocio donde se procese información y el mecanismo que se implementará será control de acceso biométrico para el personal autorizado.

Los colaboradores y terceros no autorizados para el ingreso y que deban ingresar por algún motivo especifico a las áreas críticas de negocio deberán estar acompañados en todo momento por algún funcionario del área.

3. Controles de Acceso Físicos

En Consorcio SICOV-CRC se controlará el acceso a las áreas seguras o instalaciones para asegurar el ingreso sólo de personal autorizado por medio biométrico.

Los colaboradores y terceros deberán acceder por medio del sistema biométrico según estén autorizados para tal fin.

4. Control de Ingreso de Visitantes

En la sede Bogotá de Consorcio SICOV-CRC se llevará un control de registro de visitantes y colaboradores con fecha y hora de entrada y salida, según el formato establecido.

Es deber de los colaboradores exigir el registro de los visitantes

Es deber de los terceros registrarse en el control de visitantes.

5. Seguridad de Oficinas, Recintos e Instalaciones

El Consorcio SICOV-CRC implementará y controlará la seguridad física en las

instalaciones y demás áreas del negocio por medio de acceso biométrico y uso de sistemas CCTV.

Los colaboradores y terceros deberán cumplir con las medidas mínimas de seguridad de oficinas tales como mantener la puerta cerrada, no dañar la infraestructura de la oficina, cerrar los elementos que contengan información confidencial de Consorcio SICOV-CRC de sus Clientes.

6. Protección Contra Amenazas Externas y Ambientales

El Consorcio SICOV-CRC se aplicarán buenas prácticas de seguridad física contra desastres naturales, ataques maliciosos o accidentes que apoyen la seguridad en el trabajo de sus colaboradores.

Los colaboradores deberán reportar cualquier condición insegura al Responsable de SG-SST y deberán aplicar lo solicitado en el Plan de Continuidad de Negocio en el caso de desastres naturales y reanudación de la operación.

7. Controles de seguridad contra incendios

El centro de cómputo de Consorcio SICOV-CRC posee detectores de humo, los cuales deben activarse de forma automática al momento de presentarse una emanación de humo, adicionalmente se cuenta con los extintores adecuados según su agente extintor. Estos dispositivos deben contar con un plan de mantenimiento preventivo que valide su funcionamiento.

Los colaboradores de SST deberán realizar el mantenimiento de los controles contra incendios según corresponda y según se evidencie por las buenas prácticas.

8. Trabajo en Áreas Seguras

Consorcio SICOV-CRC controlará y gestionará la seguridad física para el trabajo en áreas seguras tal como está establecido en el manual de áreas seguras.

Los colaboradores de Consorcio SICOV-CRC deberán usar llaves o acceso biométrico según el rol autorizado para el acceso a las áreas seguras de la compañía.

9. Áreas de Despacho y Carga

Consorcio SICOV-CRC definirá, controlará y aislará el acceso a áreas de recepción y/o de despacho y demás puntos donde existe la posibilidad de ingreso de

personal externo o público en general.

Los colaboradores que utilicen estas áreas deberán mantener la seguridad de la información entregada y recibida en estas áreas hasta su disposición o entrega final.

10. Equipos

En Consorcio SICOV-CRC se prevendrá la pérdida, daño, robo o compromiso de los activos de información e interrupción de las operaciones de su negocio.

a. Ubicación y Protección de los Equipos

Los equipos de Consorcio SICOV-CRC estarán ubicados y protegidos contra amenazas, peligros del entorno y acceso no autorizado.

b. Servicios de Suministro

Los equipos de Consorcio SICOV-CRC estarán protegidos contra falla o interrupción causada en el suministro de los servicios eléctricos, comunicaciones, administrativos o cualquiera que sea necesario para la continuidad del negocio.

c. Del Procesamiento de la Información

El procesamiento a la información que se realice sobre cualquier componente de la plataforma tecnológica debe cumplir con la normatividad establecida en materia de seguridad de la información con el fin de preservar la confidencialidad, integridad y disponibilidad de la misma.

d. Seguridad del Cableado

Todo el cableado de energía eléctrica, telecomunicaciones y servicios de suministro de Consorcio SICOV-CRC está adecuadamente organizado y asegurado contra amenazas, interceptación o daños.

Los colaboradores deberán cuidar los elementos eléctricos y de red a los que tienen acceso a nivel de cableado, y deberán reportar de forma inmediata cualquier anomalía del cableado que pueda afectar el funcionamiento adecuado de la labor de los colaboradores de la compañía.

e. Mantenimiento de Equipos y Software

En Consorcio SICOV-CRC se realizará mantenimiento periódico a los equipos

de cómputo de acuerdo con las características y recomendaciones del fabricante o cuando sea requerido por eventos o incidentes presentados, con el fin de asegurar la continuidad en su funcionamiento, integridad, disponibilidad y conservación de los mismos.

Los terceros de nuestro aliado de Gestión Tecnológica deberán realizar mantenimiento preventivo de los equipos de cómputo a los colaboradores de la compañía y realizar los ajustes necesarios.

f. Retiro de Activos

En Consorcio SICOV-CRC no se retirarán de sus instalaciones los equipos, información o software sin previa autorización del propietario o responsable del activo de información.

Los colaboradores y los terceros deberán informar sobre el retiro de los activos a la Gerente del Consorcio SICOV, quien dará el aval de retiro.

g. Seguridad de Equipos Fuera de las Instalaciones

En el Consorcio SICOV-CRC se suministrarán e implementarán medidas de seguridad apropiadas para los equipos que requieran estar fuera de las instalaciones, contemplando los riesgos a los que se pueden ver expuestos.

Los equipos de los colaboradores deberán tener el antivirus instalado con las políticas de bloqueo y de seguridad implementadas, la unidad de almacenamiento deberá estar cifrada y deberán conectarse a las redes de la empresa a través de VPN.

h. Disposición Segura, Reutilización o Eliminación de Equipos

En el Consorcio SICOV-CRC antes de la eliminación, disposición o reutilización de los equipos para ser entregados a los colaboradores o terceros se debe verificar todos los elementos que lo componen, especialmente los medios de almacenamiento (discos, memorias, unidades ópticas, entre otros), con el fin de asegurar que toda información y/o software licenciado haya sido retirado o sobrescrito de forma segura teniendo en cuenta lo establecido en el procedimiento de borrado seguro.

Los terceros deberán revisar la información de los equipos y deberán entregarlos a los colaboradores que requieran la información, así mismo el Oficial de Seguridad deberá determinar el método de borrado seguro y el proceso Gestión Tecnológica (infraestructura) deberá realizar el borrado seguro de los equipos que se retirarán de la compañía.

i. Equipos de Usuario Desatendido

Todos los colaboradores y terceros de Consorcio SICOV-CRC son responsables de asegurar que los equipos desatendidos cumplen con la protección adecuada. Así mismo se implementó una política del Directorio Activo que bloquea las pantallas después de un tiempo de inactividad en caso de que el usuario no ejecute la acción indicada.

Los colaboradores de la compañía deberán bloquear su equipo cada vez que se retiren de su escritorio.

j. Limitación del tiempo de conexión

Los sistemas de información de Consorcio SICOV-CRC se configurarán limitando el tiempo de conexión por inactividad.

Los terceros deberán ajustar los tiempos de inactividad para que los colaboradores reciban bloqueo de sus aplicaciones o pantallas por inactividad.

k. Política de Escritorio Limpio y Pantalla Despejadas

En Consorcio SICOV-CRC se implementará la Política de Escritorio Limpio y Pantalla Despejadas, con el fin de asegurar la información que se almacena en papeles, medios removibles o medios electrónicos.

Los colaboradores deberán mantener su escritorio sin archivos (únicamente accesos directos a aplicaciones) y no podrán tener en sus escritorios documentos sin custodia presencial del mismo funcionario o de quien este laborando con él.

1.8.2. Política de Seguridad de las Operaciones

1.8.2.1. *Procedimientos Operacionales y Responsabilidades*

El Consorcio SICOV-CRC se asegurará que las operaciones de su negocio se realicen de manera correcta y segura.

1. Procedimientos de Operación Documentados

En el Consorcio SICOV-CRC se documentarán, aprobarán, publicarán, revisarán, actualizarán y gestionarán los procedimientos de operación de su negocio.

Los colaboradores deberán reportar los cambios sobre los procesos operativos para realizar los respectivos ajustes en los documentos y realizar la revisión de

riesgos de los mismos, ajustando los mismos procesos para tal fin.

2. Gestión de Cambios

En el Consorcio SICOV-CRC se gestionarán y controlarán los cambios a nivel de organización, procesos, instalaciones y sistemas de información del Consorcio SICOV-CRC que afectan o inciden en la seguridad de la información.

3. Gestión de la Capacidad

En el Consorcio SICOV-CRC se gestionará y hará seguimiento a la capacidad y uso adecuado de recursos, ajustes y proyecciones de los sistemas de información que garanticen el desempeño requerido para las operaciones del negocio.

Los terceros deberán tener monitoreo de la capacidad y de los recursos tecnológicos, y deberán emitir las alertas de forma temprana y oportuna para la ampliación de recursos o la optimización de estos.

4. Distribución de funciones

En el Consorcio SICOV-CRC se segregarán las funciones con el fin de prevenir o mitigar el riesgo de errores o irregularidades en la organización.

Los colaboradores no podrán ejecutar actividades de otros cargos ni podrán tener privilegios que tienen otros colaboradores para la ejecución de tareas no competentes a su rol dentro de la Organización, reportando al Oficial de Seguridad de la Información en el caso en el que se encuentre que su perfil tiene más permisos de los estipulados por el cargo.

5. Separación de los Ambientes de Desarrollo, Pruebas y Producción

En el Consorcio SICOV-CRC se establecerá y mantendrá separado los ambientes para el desarrollo, pruebas y producción, como contribución a la mitigación de riesgos de acceso, cambios no autorizados, su adecuada administración, operación, control y seguridad sobre los sistemas de información en operación.

Es deber del proceso Gestión Tecnológica (infraestructura) mantener separados los ambientes de Desarrollo, pruebas y Producción por redes y por servidores de forma apropiada.

1.9. Protección Contra Códigos Maliciosos

En el Consorcio SICOV-CRC se asegurará que la información y las instalaciones de procesamiento de información se encuentren protegidas contra códigos maliciosos.

1. Controles Contra Códigos Maliciosos

En el Consorcio SICOV-CRC se implementarán controles de detección, prevención, recuperación y toma de conciencia de los colaboradores y terceros para protegerse contra códigos maliciosos. Por medio de antivirus centralizado que permita monitorear las amenazas que se presenten dentro de la red de la compañía.

Es deber del Oficial de Seguridad de la Información seleccionar el antivirus más apropiado según las necesidades de la compañía.

Es deber del proceso de Gestión Tecnológica realizar la instalación en todos los equipos de cómputo del antivirus.

Es deber del Encargado de Gestión Tecnológica implementar las reglas del Antivirus en la plataforma centralizada, de tal manera que se garantice la protección de la información aun cuando el equipo se encuentre fuera de las instalaciones de la compañía.

Es deber del Encargado de Gestión Tecnológica definir los roles que debe tener las políticas del antivirus según las matrices de Roles y Permisos establecidas en la compañía.

Es deber del Encargado de Gestión Tecnológica monitorear en la plataforma las amenazas detectadas por el antivirus.

2. Protección Contra Código Móviles

En Consorcio SICOV-CRC se restringirá la ejecución de código móvil aplicando políticas en el sistema operativo, en el software de navegación de cada máquina y en el sistema de control de navegación.

Es deber del Encargado de Gestión Tecnológica definir las políticas y la intensidad de escaneo del antivirus instalado para poder asegurar el sistema frente a los códigos móviles.

Los colaboradores no podrán modificar o instalar aplicativos que no estén autorizados según la política de dispositivos móviles.

1.10. Copias de Respaldo

El Consorcio SICOV-CRC protegerá la pérdida de datos o información, y asegurará la integridad, confidencialidad y disponibilidad de esta.

1. Respaldo de la Información

En el Consorcio SICOV-CRC se realizarán copias de seguridad de la información como respaldo o Backup de la misma y se validarán a través de pruebas periódicas de acuerdo con las políticas de respaldo o Backup de la información. Así mismo, la información de respaldo estará cifrada para prevenir un uso indebido por parte del personal de Consorcio SICOV-CRC.

La información se almacenará cifrada en sitios externos al Datacenter con la finalidad de mantener acceso a los Backup en el momento en el que se necesiten.

Es deber de los usuarios realizar una copia de respaldo de la unidad de red de la compañía con la finalidad de salvaguardar su información.

Es deber del equipo de Infraestructura realizar los Backup de los sistemas de información misionales de la compañía.

Es deber del Encargado de Gestión Tecnológica realizar copias de respaldo a los activos de información de forma periódica.

1.11. Registro y Seguimiento

En el Consorcio SICOV-CRC se registrarán los eventos y se generarán evidencias de las operaciones del negocio.

1. Registro de Eventos

En el Consorcio SICOV-CRC se elaborarán, conservarán y revisarán periódicamente de forma mensual, los registros de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información presentados en las operaciones del negocio. Dentro del Syslog de la compañía y dentro de las bases de datos según corresponda.

Es deber del Encargado de Gestión Tecnológica realizar el paso de los logs de los sistemas de información al Syslog de forma diaria.

Los terceros no deberán eliminar ningún log de los servidores ni del Syslog.

Es deber del Encargado de Gestión Tecnológica revisar que se está realizando el paso de logs al servidor de Syslog de forma diaria.

2. Protección de la Información de Registro

En el Consorcio SICOV-CRC se protegerán la información de registro y las instalaciones donde se encuentran guardados, contra alteraciones y acceso no autorizado.

El área de Infraestructura deberá proteger en el servidor Syslog la información de registro de logs que se genere en los distintos sistemas informáticos

3. Registros del Administrador y del Operador

En el Consorcio SICOV-CRC se registrarán, protegerán y revisarán periódicamente o cuando se requiera las actividades de administradores y operadores de los sistemas de información.

Los terceros que accedan a los servidores o bases de datos deberán ser monitoreados en sus acciones por el Oficial de Seguridad de la Información y no deberán eliminar ninguna traza dentro del equipo o base de datos

4. Sincronización de Relojes

En el Consorcio SICOV-CRC se mantendrán sincronizados todos los relojes de los sistemas de información de acuerdo con la hora legal Colombiana consultando los servidores NTP autorizados por la compañía.

Los colaboradores deberán tener sus relojes de sus equipos sincronizados con dicha hora y deberán reportar si ven un descuadre en sus relojes de forma inmediata al equipo de Gestión Tecnológica.

1.12. Control de Software Operacional

El Consorcio SICOV-CRC se asegurará la integridad del software y sistemas de información operacional al tener control en distintas áreas en la implementación del desarrollo y en la segregación de ambientes de Desarrollo, QA, Preproducción y Producción.

1. Instalación de Software en Sistemas Operativos

En el Consorcio SICOV-CRC se controlará la instalación y cambios en el software de todos sus sistemas de información por medio de la generación de documentos RFC los cuales son evaluados y aprobados por las partes técnicas y autorizados por las áreas operativas.

Los colaboradores y/o terceros únicamente podrán instalar los programas necesarios para el funcionamiento del aplicativo y para verificaciones sobre el mismo, así como los programas de Seguridad necesarios para el adecuado control de las máquinas. No se podrá instalar Software que degraden la Seguridad del Sistema Operativo.

2. Restricciones sobre la Instalación de Software

En Consorcio SICOV-CRC se controlará y restringirá la instalación de software en los sistemas de información sólo a personal y software autorizado.

Los terceros no deberán instalar software no autorizado o sin licencia en los equipos de los colaboradores, y ninguna de las partes deberán instalar software que degrade en cualquier forma la seguridad de la Información almacenada en los equipos de Consorcio SICOV-CRC.

1.13. Gestión de la Vulnerabilidad Técnica (Hacking ético, carga y estrés)

En Consorcio SICOV-CRC se prevendrán y minimizarán los riesgos de la explotación de las vulnerabilidades técnicas por usuarios. Por tal motivo, se realizarán pruebas de hacking ético, carga y estrés que permitan identificar oportunamente las vulnerabilidades técnicas de los sistemas de información, evaluar la exposición de Consorcio SICOV-CRC frente a las mismas y aplicar los planes de tratamiento o medidas adecuadas y necesarias que permitan la mitigación del riesgo en los mismos.

Se realizarán pruebas de hacking ético externas como parte de las políticas y buenas prácticas de seguridad de la información por lo menos una vez al año, cuando se evidencie alguna necesidad manifiesta de realizarlas o cuando sea requerido por la Alta Dirección.

Se realizarán pruebas de vulnerabilidades y Hacking ético a nivel interno de manera

continua para garantizar que se mantiene un nivel aceptable a nivel de seguridad de la información dentro de la compañía, se realizarán informes sobre las pruebas, y se escalarán los hallazgos a las áreas encargadas para dar cierre a los mismos de forma inmediata.

Los colaboradores y terceros deberán dar cierre oportuno a las vulnerabilidades según el reporte el Oficial de Seguridad de la Información

1.14. Consideraciones sobre Auditorías de Sistemas de Información

En el Consorcio SICOV-CRC se minimizará el impacto y maximizará la eficacia de las auditorías realizadas a los sistemas de información.

1. Controles de Auditorías de Sistemas de Información

En el Consorcio SICOV-CRC se planearán y acordarán los requisitos y actividades de auditoría sobre los sistemas de información de tal manera que se evite y minimice interrupciones a las operaciones del negocio.

Los colaboradores y terceros deberán ser auditados de forma continua y las actividades deberán ser ejecutadas con la total disposición de atención de la auditoria.

2. Protección de las herramientas de auditoría de los sistemas de información

En el Consorcio SICOV-CRC se protegerá y controlará el uso adecuado de las herramientas de auditoría, permitiendo sólo el acceso a personal autorizado. Los colaboradores y terceros deberán tener acceso según se requiera por atención de los puntos de auditoria dentro de cada uno de los elementos revisados, dichos accesos solo podrán ser autorizados por la Gerencia de Consorcio SICOV.

Los colaboradores y terceros autorizados deberán tener usuarios con roles determinados para el acceso de consulta de los registros de auditoría.

3. Registro de auditorías

En el Consorcio SICOV-CRC se elaborarán, mantendrán y conservarán registros de las auditorías realizadas a los sistemas de información. Estos registros se generarán en el mismo momento en el que ocurran y podrán ser consultados en distintas fuentes de información.

Los colaboradores y terceros podrán tener acceso a dichos registros únicamente para consulta en el sistema de información documental establecido en la compañía con la finalidad de atender sus planes de acción de forma acertada y oportuna.

1.15. Política de Seguridad de las Comunicaciones

1.15.1. Gestión de la Seguridad de las Redes

En el Consorcio SICOV-CRC se protegerá la información en las redes de comunicaciones y en instalaciones de procesamiento de información.

1. Controles de Redes

En el Consorcio SICOV-CRC se gestionarán, protegerán y controlarán las redes de comunicaciones con el fin de proteger la información en tránsito por los sistemas de información y aplicaciones que hacen parte de las operaciones del negocio.

Los colaboradores estarán restringidos a accesos a sitios WEB y a redes que no sean autorizadas y que no cumplan con los adecuados estándares de seguridad y no se alineen al desarrollo de sus funciones.

2. Seguridad de los Servicios de Red

En el Consorcio SICOV-CRC se identificarán todos los mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red prestados interna o externamente a la organización. Igualmente, se establecerán acuerdos de niveles de servicio con terceros que contemplen lo anterior.

El proceso de Gestión Tecnológica definirá todos los mecanismos aplicables para tal fin.

Los colaboradores y terceros deberán utilizar los mecanismos seguros a nivel de red que se establezcan con los proveedores y clientes, buscando entre ellos implementar nuevos canales seguros si se requiere.

3. Separación en las Redes

En el Consorcio SICOV-CRC se definirán grupos de servicios de información, usuarios y sistemas de información de manera separada en las redes de comunicaciones. De tal forma que las redes inalámbricas no pueden ver las redes internas o los servidores de la compañía

Los colaboradores y terceros deberán conectarse únicamente a las redes separadas de los servidores y fuentes de información de Consorcio SICOV-CRC cuando requieran conectar un dispositivo externo propio o no controlado por la compañía.

4. Seguridad de la documentación del sistema

En el Consorcio SICOV-CRC se protegerá la documentación referente a los sistemas de información de personal no autorizado.

Los colaboradores ni terceros podrán editar, eliminar, añadir o alterar información documental que se encuentre dentro del repositorio de gestión documental, teniendo únicamente permisos de consulta sobre la documentación.

1.15.2. Transferencia de Información

En el Consorcio SICOV-CRC se mantendrá la seguridad de la información y del software que se intercambia interna o externamente con terceros.

1. Directrices y Procedimientos de Transferencia de Información

En el Consorcio SICOV-CRC se controlará la transferencia e intercambio formal de información a través de cualquier tipo de medio o servicio de comunicación.

Los colaboradores y terceros deberán utilizar canales seguros en la transmisión de su información y deberán mitigar los riesgos de la transferencia manual de la información a fin de garantizar la integridad y disponibilidad de la misma.

2. Acuerdos sobre Transferencia de Información

En el Consorcio SICOV-CRC establecerá acuerdos o convenios a nivel interno y con terceros para la transferencia segura de la información, software o cualquier activo de información respetando la legislación aplicable al caso.

Los colaboradores y los terceros deberán transmitir la información por canales seguros o cifrada según sea el caso y deberán exigir el uso de transmisión segura en todo momento.

3. Mensajería Electrónica

En el Consorcio SICOV-CRC se protegerá la información manejada a través de la mensajería electrónica o cualquier medio de correo electrónico, redes sociales y chats corporativos.

Los colaboradores estarán sometidos a monitoreo constante del correo electrónico por parte del Oficial de Seguridad de la Información y no deberán utilizar el correo electrónico para enviar información sensible a correos personales o de terceros no autorizados, ni deberán usar el correo para fines distintos a los de

ejecución de sus funciones.

4. Acuerdos de Confidencialidad

En el Consorcio SICOV-CRC se identificarán, documentarán y revisarán periódicamente los acuerdos de confidencialidad, el cual deberá cumplir con las necesidades de protección de la información de Consorcio SICOV-CRC de acuerdo con los requisitos legales, contractuales y buenas prácticas de seguridad de la información vigentes.

Los colaboradores y terceras partes deberán aplicar, cumplir y hacer cumplir los acuerdos de confidencialidad que firmen con Consorcio SICOV-CRC o que le apliquen a Consorcio SICOV-CRC producto de las relaciones comerciales y contractuales que manejan

1.15.3. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

1.15.3.1. *Requisitos de Seguridad de los Sistemas de Información*

En el Consorcio SICOV-CRC la seguridad será parte integral de los sistemas de información durante todo su ciclo de vida el cual incluye requisitos sobre sistemas operativos, infraestructura, aplicaciones y servicios desarrollados o adquiridos para los usuarios y aquellos sistemas de información que prestan servicios a través de redes públicas.

1. Análisis y Especificación de Requisitos de Seguridad de la Información

En el Consorcio SICOV-CRC se incluirán requisitos de seguridad de la información para nuevos, cambios o mejoras en desarrollos o sistemas de información.

Los colaboradores deberán solicitarle al Oficial de Seguridad de la Información la revisión y el análisis de la totalidad de los requerimientos solicitados para que los mismos incluyan desde el principio los requisitos de Seguridad de la Información y que el mismo sea asegurado desde el mismo diseño.

2. Seguridad de Servicios de las Aplicaciones en Redes Públicas

En Consorcio SICOV-CRC se trabajará por preservar la seguridad de la información expuesta en servicios web o redes públicas contra amenazas informáticas, incumplimientos contractuales y legales, divulgación o modificaciones no autorizadas.

Los colaboradores y las terceras partes deberán acceder a las aplicaciones en

Redes Públicas utilizando protocolos y puertos seguros cifrados que permitan garantizar la confidencialidad e integridad de la información, así mismo, deberán reportar cualquier falla o cualquier riesgo que se detecte dentro de los servicios web de manera oportuna con la finalidad de prevenir la materialización de los riesgos.

3. Protección de Transacciones de los Servicios de las Aplicaciones

En Consorcio SICOV-CRC se protegerán y validarán las transacciones de servicios de aplicación con el fin de evitar transacciones incompletas, enrutamientos erróneos, alteración de mensajes, divulgación, duplicación o reproducción no autorizadas de mensajes.

Los colaboradores y terceras partes deberán utilizar únicamente los canales transaccionales definidos por Consorcio SICOV-CRC utilizando y siguiendo las prácticas de seguridad implementadas y solicitadas con la finalidad de garantizar que las transacciones se generan de forma completa y adecuada hasta su destino.

1.15.3.2. *Seguridad en los Procesos de Desarrollo y de Soporte*

En el Consorcio SICOV-CRC se diseñará e implementará la seguridad de la información en todo el ciclo de vida de desarrollo de sistemas de información aplicando las siguientes políticas:

1. Política de Desarrollo Seguro

En el Consorcio SICOV-CRC se establecerán y aplicarán directrices para el desarrollo, adquisición o alquiler de software, junto con las licencias a las que haya lugar.

El Oficial de Seguridad de la Información establece los lineamientos de desarrollo seguro y los dejara estipulados en el *Manual de Desarrollo Seguro de Software*

Es responsabilidad del Encargado de Gestión Tecnológica dar cumplimiento a los lineamientos allí exigidos, el Oficial de Seguridad de la Información realizará pruebas de forma periódica sobre los desarrollos entregados y ya en producción para garantizar el adecuado cumplimiento de esta política.

Los colaboradores que necesiten realizar requerimientos deberán incluir en los mismos los lineamientos de seguridad de la información, apoyándose por el Oficial de Seguridad en el levantamiento de los procesos

2. Control de Cambios en Sistemas

En el Consorcio SICOV-CRC se controlarán los cambios en los sistemas de información que se encuentren en desarrollo o en producción.

Es deber del tercero realizar una solicitud de Cambios diligenciando el formato de Control de Cambios establecido por Consorcio SICOV-CRC en su última versión

Es deber de los colaboradores implicados realizar las pruebas pertinentes en los ambientes de preproducción antes de dar el visto bueno al paso a producción de los requerimientos solicitados.

Es deber de la Gerencia de Consorcio SICOV revisar, y dar el aval de paso o no paso a producción del cambio a realizar.
Es deber del Oficial de Seguridad de la Información garantizar que los cambios puestos en Producción no degraden la Seguridad del aplicativo o servicio entregado.

3. Cambios al hardware

En el Consorcio SICOV-CRC se controlarán los cambios en los sistemas de información que se encuentren relacionados con el hardware, especialmente relacionados a la administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones.

Es deber del proceso de Gestión Tecnológica no incluir hardware o modificaciones de Hardware de degraden la Seguridad del sistema parcial o totalmente.

Es deber del Oficial de Seguridad de la Información velar por el cumplimiento del párrafo anterior utilizando los medios necesarios para su fin.

En caso de encontrarse una modificación en el Hardware se deberá solicitar su cambio o retiro de forma oportuna según se detecte y según se evalúe el impacto de cambio realizado.

Consorcio SICOV-CRC implementa aplicaciones de parches de seguridad de manera inmediata y cierre de puertos y acceso no necesarios para el uso adecuado de las aplicaciones.

4. Revisión Técnica de las Aplicaciones Después de Cambios en la Plataforma de Operación

En Consorcio SICOV-CRC se revisarán y realizarán pruebas a los sistemas y aplicaciones luego de realizar cambios en los mismos, con el fin de asegurar que

no hay impactos adversos en las operaciones y seguridad de la información en el negocio.
El Oficial de Seguridad de la Información deberá realizar pruebas de Seguridad, ya sea por medio propio o de un tercero, en los cambios de Plataforma que se presenten en la Operación e informar en caso de errores o falencias encontradas al tercero.

El proceso de Gestión Tecnológica (Infraestructura) deberá realizar pruebas en producción cada vez que se ejecute un cambio, verificando que el sistema no se degrada como consecuencia del mismo.

5. Restricciones en los Cambios a los Paquetes de Software

En el Consorcio SICOV-CRC se controlarán, restringirán y limitarán las modificaciones sólo a los cambios necesarios en el software, aplicaciones o sistemas de información, los cuales serán informados previamente por el líder técnico con su respectivo plan de retorno en caso de falla

Únicamente el proceso de Gestión Tecnológica podrá realizar los cambios en Producción de los paquetes de Software en producción.

Es deber del proceso de Gestión Tecnológica controlar los cambios realizados en los paquetes de Software durante el desarrollo de los aplicativos y tomar las medidas pertinentes en caso en donde se encuentren cambios no autorizados o que degraden la Seguridad de la Información del aplicativo.

El personal interno de la compañía deberá validar los cambios realizados reportando los errores a la Fabrica y las Vulnerabilidades al Oficial de Seguridad de la Información para darle un rápido tratamiento.

6. Principios de Construcción de los Sistemas Seguros

En Consorcio SICOV-CRC se establecerán, documentarán, y conservarán lineamientos para el desarrollo e implementación de software o sistemas de información de manera segura. Así mismo, se realizarán revisiones periódicas sobre el código fuente para poder garantizar el cumplimiento de dichos principios.

Es deber del Oficial de Seguridad de la Información, de los colaboradores internos y del proceso de Gestión Tecnológica levantar desde el principio de los requerimientos todos los requisitos de Seguridad de la Información que deberá tener el cambio o el sistema desde el principio para desarrollarlo con seguridad en diseño.

El Oficial de Seguridad realizará todas las pruebas pertinentes de seguridad a los

aplicativos para garantizar que se cumple con un Sistema Seguro debidamente construido.

7. Ambiente de Desarrollo Seguro

En el Consorcio SICOV-CRC se establecerá y protegerá el ambiente de desarrollo para el desarrollo de software o sistemas de información seguros durante todo su ciclo de vida.

Es deber del proceso de Gestión Tecnológica (Infraestructura) crear las máquinas de Desarrollo, Pruebas y Preproducción en VLAN y en ambientes separados y segregados entre sí.

Es deber del proceso de Gestión Tecnológica (Infraestructura) crear los usuarios de acceso a los servidores de Desarrollo a todo el personal de acuerdo a la matriz de roles y perfiles y garantizando la adecuada segregación de los ambientes.

Es deber del proceso de Gestión Tecnológica cumplir con los controles de accesos estipulados para tal finalidad.

8. Fuga de información

En el Consorcio SICOV-CRC se evitarán las oportunidades o riesgos que puedan ocasionar fugas de información. Para ello se implementarán sistemas de control de acceso a los servicios y monitoreo sobre las aplicaciones que puedan filtrar información a terceras partes.

El Consorcio SICOV-CRC y el Oficial de Seguridad de la Información puede supervisar los equipos de cómputo corporativos, tanto en vivo como el histórico, así como la totalidad de aplicaciones y datos que se almacenen, transmitan o procesen en estos equipos sin previo aviso. Monitoreando que la Información sea extraída a personas no autorizadas.

El personal interno de la empresa deberá usar todos los recursos informáticos que se le asignen de forma adecuada, dando uso únicamente para temas laborales respetando la confidencialidad, integridad y disponibilidad de la información a la cual tengan acceso.

El Oficial de Seguridad de la Información monitoreará los correos electrónicos corporativos y levantará las alertas al área de Talento Humano si se detecta una posible fuga o mal uso del correo electrónico.

9. Desarrollo Contratado Externamente

En el Consorcio SICOV-CRC se supervisará y hará seguimiento a las actividades de desarrollo de software en los sistemas de información contratado a terceros. Garantizando la ejecución adecuada de pruebas sobre el ambiente de preproducción, junto con las evidencias de dicha ejecución.

Es deber de la Gerente de Consorcio SICOV realizar seguimiento de todos los entregables. Es deber de los colaboradores reportar los errores o las posibles vulnerabilidades de los sistemas informáticos.
Es deber del Oficial de Seguridad de la Información velar por la aplicación de controles de seguridad en el aplicativo entregado.

10. Pruebas de Seguridad de Sistemas

En el Consorcio SICOV-CRC se realizarán pruebas de calidad y seguridad del software y sistemas de información, durante su desarrollo y para todo aquel que sea adquirido o contratado con terceros previamente a ser implementado.

Gestión Tecnológica deberá corregir todas las falencias que se encuentren de manera oportuna y sin dilaciones usando todos los medios tecnológicos y humanos para tal fin.

Es deber de los colaboradores participar en las pruebas de seguridad de los sistemas, así como en las pruebas funcionales de los mismos, detectando posibles riesgos de seguridad de la información sobre los procesos e informar de forma oportuna sobre los mismos con la finalidad de agilizar los procesos de corrección y mitigación del riesgo.

El Oficial de Seguridad de la Información, por medio propio o de terceros, podrá realizar pruebas de vulnerabilidad o penetración sobre los sistemas informáticos para garantizar el adecuado cumplimiento de los niveles de seguridad de la información exigidos.

11. Procesamiento Correcto en las Aplicaciones

a. Validación de los datos de entrada

Como norma general en Consorcio SICOV-CRC implementará controles para asegurar la validez de los datos que se ingresan a los sistemas de información.

Es deber de los colaboradores de la compañía solicitarles a los terceros la implementación de procesos automáticos que ejecuten la validación de datos de entrada según los parámetros que se requieran para cada uno, dando cumplimiento

a las políticas de seguridad de la información de la compañía.

b. Controles de procesamiento interno

En el Consorcio SICOV-CRC se implementarán controles para asegurar la integridad de los datos en el procesamiento, tales como monitoreo de inserción o actualización de datos.

Los colaboradores deberán acatar las políticas establecidas para el procesamiento de datos, solicitando que los mismos se realicen de forma automática y entregados en herramientas de consulta.

Este monitoreo se realizará sobre los equipos de cómputo y sobre la totalidad de la información que se procese, almacene o transmita sobre los mismos, con la finalidad de prevenir que la información sea alterada de forma indebida o no esté disponible, esto es responsabilidad del proceso de Gestión Tecnológica.

c. Integridad del mensaje

Como norma de seguridad de la información y también con el fin de dar cumplimiento a las regulaciones existentes del Consorcio SICOV-CRC, de acuerdo, a una evaluación de riesgos de seguridad se validará la integridad de los mensajes en las aplicaciones y cuál es el método más apropiado de implementación. La integridad del mensaje puede lograrse a través de la utilización de técnicas criptográficas como un medio apropiado para implementar la autenticación del mensaje.

Es deber de los colaboradores de la compañía solicitarles a los terceros la implementación de procesos automáticos que garanticen la integridad de los datos de salida según los parámetros que se requieran para cada uno, dando cumplimiento a las políticas de seguridad de la información de la compañía.

d. Validación de los datos de salida

Como norma general Consorcio SICOV-CRC implementará controles para asegurar la validez de los datos de salida.

Es deber de los colaboradores de la compañía solicitarles a los terceros la implementación de procesos automáticos que ejecuten la validación de datos de salida según los parámetros que se requieran para cada uno, dando cumplimiento a las políticas de seguridad de la información de la compañía.

e. Validaciones, controles y manejo de errores

Para reducir la probabilidad de ingreso erróneo de datos de alta sensibilidad, los procedimientos de ingreso de información deben contener controles de validación. Así mismo, en Consorcio SICOV-CRC se estimulará el uso de canales seguros automatizables de recepción de información.

Es deber de los colaboradores y terceros utilizar los controles de validación estipulados por la compañía para el proceso de datos de alta sensibilidad, así mismo es deber de los colaboradores solicitarle a la Fábrica de Desarrollo requerimientos que mitiguen el impacto de los procesos manuales que se ejecutan a nivel de validación de datos.

12. Prueba de Aceptación de Sistemas

En el Consorcio SICOV-CRC se establecerán criterios y realizarán pruebas de aceptación de todo software o sistema de información en desarrollo, nuevo o sobre cualquier actualización, versión, adaptación o cambio realizado en el mismo cumpliendo con todos los criterios establecidos.

Los colaboradores y terceras partes en conjunto deberán establecer los criterios y las condiciones de aceptación de las pruebas en los aplicativos desarrollados, realizando pruebas de forma individual o en conjunto para dar la aceptación al cambio o aplicativo.

13. Implantación del Software

En el Consorcio SICOV-CRC toda implementación de software debe tener una autorización previa de los responsables y cumplir con los criterios establecidos en la organización.

En todo caso se debe obtener la autorización de la Gerencia de Consorcio SICOV para realizar el paso a producción de cualquier aplicativo o plataforma tecnológica, verificando que en la implementación se cumpla con todas las pruebas realizadas y con lo establecido en el formato de solicitud de cambios.

1.15.3.3. *Datos de Prueba*

En el Consorcio SICOV-CRC se protegerá la información utilizada para las pruebas del software o sistemas de información.

1. Protección de los Datos de Prueba

En el Consorcio SICOV-CRC se seleccionará, protegerá y controlará la

información que se utiliza en la realización de pruebas durante el ciclo de vida de desarrollo del software o sistemas de información, al restringir los accesos a los datos por parte de usuarios no autorizados.

Los colaboradores y terceros que tengan acceso por algún medio a los ambientes de pruebas no deberán utilizar datos de producción para la ejecución de sus actividades, sino que deberán usar datos falsos de personal no existente o que no se pueda relacionar a una persona real por ningún medio con la finalidad de dar cumplimiento a las políticas de tratamiento de bases de datos.

2. Control de acceso al código fuente de los programas

En el Consorcio SICOV-CRC el acceso al código fuente de los programas y los ítems asociados (diseños, especificaciones, planes de verificación y de validación, entre otros), se controlarán para evitar la introducción de una funcionalidad no autorizada y evitar cambios no intencionados, así como dar protección a la propiedad intelectual de Consorcio SICOV-CRC.

Es deber de los colaboradores que administran el código fuente controlar y definir los usuarios que deben acceder a este, bajo los principios de mínimo privilegio. Estos usuarios deberán contar con cláusulas de confidencialidad de la información en los contratos.

1.15.4. Política de Relaciones con Proveedores

1.15.4.1. *Seguridad de la Información en las Relaciones con los Proveedores*

En el Consorcio SICOV-CRC se protegerán los activos de información accesibles por terceros.

Los proveedores deberán firmar un acuerdo de confidencialidad como requisito en la etapa previa de la contratación, en caso de requerir información confidencial e igualmente de requerir acceso a áreas seguras críticas de Consorcio SICOV-CRC.

1. Directrices de Seguridad de la Información para las Relaciones con Proveedores

En el Consorcio SICOV-CRC se documentarán y acordarán los requisitos de seguridad de la información con los terceros (Proveedores o Contratistas), con el fin de mitigar los riesgos asociados con el acceso por parte de estos a los activos de información.

a. Requisitos Contractuales de Seguridad de la Información con terceros

En el Consorcio SICOV-CRC en la contratación de outsourcing o tercerización se cumplirá lo establecido en el procedimiento de contratación.

Es deber de los colaboradores reportar y calificar a los proveedores que les prestan un servicio de forma directa en desarrollo de sus funciones.

Es deber de la Gerencia de Consorcio SICOV y del Oficial de Seguridad de la Información establecer los parámetros y las cláusulas de acceso a la información, confidencialidad de la información, seguridad de la información, entre otros, para el cumplimiento contractual por parte de los terceros.

Es deber de los terceros acatar las políticas de seguridad de la información en todo momento sin prejuicio del tipo de labor que realicen.

b. Identificación de los riesgos relacionados con las partes externas

En el Consorcio SICOV-CRC se identificarán los riesgos asociados al contratar servicios o productos con terceros que hagan parte o apoyen la operación del negocio.

Es deber del Encargado de Sistemas de Gestión y del Oficial de Seguridad de la Información identificar los riesgos relacionados con las partes externas y comunicarlos a la Gerencia de Consorcio SICOV de forma oportuna para que se incluyan los controles en los acuerdos contractuales con los terceros.

Los terceros deberán ejecutar los controles de los riesgos según se establezcan, manteniendo debida reserva de la información de Consorcio SICOV-CRC de la que tengan conocimiento durante el desarrollo de sus funciones.

c. Consideraciones de seguridad cuando se trata con los terceros

En Consorcio SICOV-CRC se definirá, acordará y supervisará el cumplimiento de las condiciones de seguridad establecidas contractualmente con los terceros.

Los colaboradores deberán ser partícipes de la definición de las condiciones de seguridad exigidas a los terceros y deberán colaborar en la supervisión del cumplimiento de las condiciones de seguridad establecidas contractualmente y en las políticas de seguridad de la información según la tarea a desempeñar.

2. Tratamiento de Seguridad dentro de los Acuerdos con Proveedores

En el Consorcio SICOV-CRC se establecerán y acordarán los requisitos de seguridad de la información con los terceros a través de acuerdos de niveles de servicio con el fin de establecer los derechos de acceso, y de procesamiento, almacenamiento, y transmisión de información que da soporte a los procesos misionales de Consorcio SICOV-CRC y de sus clientes.

Es deber de las terceras partes dar cumplimiento a la seguridad de la información que establezca Consorcio SICOV-CRC en sus políticas como un mínimo posible como acuerdo inicial. Es deber de los colaboradores de Consorcio SICOV-CRC exigir el cumplimiento a los terceros de las políticas estipuladas, así como darles una guía básica de como ejecutarlas.

Es deber del Oficial de Seguridad de la Información velar por el cumplimiento de los mínimos de Seguridad de la Información establecidos dentro de estas políticas y dentro de los acuerdos realizados en la relación contractual con los proveedores.

3. Cadena de Suministro de Tecnología de Información y Comunicación

En Consorcio SICOV-CRC establecerá acuerdos con terceros el cual incluyan los requisitos de seguridad de la información en el suministro de productos de servicios de las tecnologías de la información y las comunicaciones.

Los terceros deberán incluir dentro del análisis de requerimientos de entregables, según aplique, las medidas de seguridad necesarias previas al desarrollo y a la entrega del producto final según corresponda.

Es deber del Arquitecto de Seguridad garantizar que se cumple con la Seguridad desde el diseño de las aplicaciones e informar al tercero en el caso de incumplimiento.

1.15.4.2. *Gestión de la Prestación de Servicios de Proveedores*

En Consorcio SICOV-CRC mantendrá acuerdos de niveles de servicio, el cual contemple la seguridad de la información y la prestación de servicios en línea con los terceros.

1. Seguimiento y Revisión de los Servicios de los Proveedores

En Consorcio SICOV-CRC se monitoreará, se hará seguimiento, se revisará y se harán auditorías periódicas o cuando se requiera a la prestación de los servicios contratados con terceros.

Es deber del personal interno de Consorcio SICOV-CRC que tenga relación directa con los proveedores que realice la evaluación del proveedor siguiendo lo estipulado para tal fin

2. Gestión de Cambios en los Servicios de los Proveedores

En el Consorcio SICOV-CRC se controlarán los cambios en los servicios, mantenimiento y mejora de políticas, procedimientos y controles de seguridad de la información de acuerdo con su clasificación, sistemas, reevaluación de riesgos y procesos del negocio involucrados en la prestación de servicios con terceros.

Es deber del tercero implementar cambios que no degraden la seguridad de la información en ningún momento, contando con los requerimientos del mismo desde su diseño hasta su implementación.

1.15.5. Política de Gestión de Incidentes de Seguridad de la Información

1.15.5.1. *Gestión de Incidentes y Mejoras de Seguridad de la Información*

En Consorcio SICOV-CRC se gestionarán los incidentes de seguridad de la información en todos sus procesos.

1. Responsabilidades y Procedimientos

En el Consorcio SICOV-CRC se definirá y establecerán responsabilidades y el procedimiento de gestión de incidentes, eventos y vulnerabilidades de seguridad de la información en razón de asegurar una respuesta rápida, eficaz y ordenada de los mismos.

Todos los colaboradores y terceras partes involucrados de forma total o parcial en un incidente, o que tengan conocimiento de un evento o vulnerabilidad de seguridad de la información, deberá reportar al oficial de seguridad de la información de forma inmediata y oportuna sobre el mismo con la finalidad de darle cierre al mismo.

2. Reporte de Eventos de Seguridad de la Información

En Consorcio SICOV-CRC todos los eventos de seguridad de la información deben ser informados o reportados oportunamente por los colaboradores y terceros a través de los canales de gestión establecidos por Consorcio SICOV-CRC.

3. Reporte de Vulnerabilidades de Seguridad de la Información

En Consorcio SICOV-CRC todos los colaboradores y terceros que hacen uso de cualquier activo de información o utilizan servicios o sistemas de información de

Consorcio SICOV-CRC deben reportar cualquier hallazgo, debilidad o vulnerabilidad, o sospecha que pueda poner en riesgo la seguridad de la información. Así mismo, el Oficial de Seguridad de la Información y el Encargado de Gestión Tecnológica, deberá realizar todas las revisiones pertinentes para detectar y corregir vulnerabilidades de forma temprana.

4. Evaluación de Eventos de Seguridad de la Información y Decisiones sobre los Mismos

En Consorcio SICOV-CRC todo evento de seguridad de la información será evaluado y clasificado de acuerdo con la gestión de incidentes establecida.

Los colaboradores y los terceros, según se requiera, deberán ser partícipes y ser informados de la clasificación realizada al evento de riesgo detectado con la

finalidad de que puedan tomar las medidas adecuadas según la clasificación entregada.

5. Respuesta a Incidentes de Seguridad de la Información

En Consorcio SICOV-CRC todos los incidentes presentados tendrán una respuesta por parte del área o responsable encargado por medio de la herramienta de gestión de casos o por correo electrónico según sea el caso, así mismo, en el caso que la respuesta sea para un cliente interno, se dará respuesta con los logs de revisión y con la traza del incidente identificando en cada paso las acciones tomadas.

Los colaboradores y terceras partes deberán interactuar de forma dinámica y asertiva en la respuesta al incidente de seguridad de la información, brindando el conocimiento completo de sus procesos con la finalidad de entregar una respuesta que garantice la no repetición de dicho incidente.

En la herramienta de Gestión Documental se realizarán los planes de acción correspondientes dependiendo del tipo de incidente.

6. Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

En Consorcio SICOV-CRC se mantendrá una base de conocimiento del tratamiento de incidentes ocurridos como parte del aprendizaje para el análisis, respuesta y solución a incidentes posteriores, y a la minimización de impacto de seguridad de la información.

Es deber de los colaboradores y terceras partes solicitar la inclusión de la base de

conocimientos en la ejecución de sus procesos, conocer la base de conocimientos y aplicarla durante la ejecución de sus funciones, evitando de esta manera que se puedan repetir los incidentes detectados.

7. Recolección de Evidencia

En el Consorcio SICOV-CRC se identificará, adquirirá y preservará la información de las evidencias de los incidentes de seguridad de la información presentados.

La recolección de la evidencia se realizará inicialmente con un proceso de discovery para determinar los hechos que ocurrieron durante el incidente, así mismo, se entregaran todas las demás evidencias fílmicas, testimoniales, documentales, entre otras, a la Gerencia de Consorcio SICOV.

En caso de borrado de información, se realizará un proceso de informática forense, ya sea a nivel interno o por medio de algún proveedor que determine la Gerencia de Consorcio SICOV.

Los colaboradores y terceras partes deberán disponer de todos los recursos necesarios para que se pueda realizar esta función a cabalidad, sin alterar las evidencias del caso y siguiendo el procedimiento que el Oficial de Seguridad establezca.

El Oficial de Seguridad de la Información es la persona encargada de realizar la recolección de las evidencias tecnológicas según se presente el caso, garantizando la debida custodia de la información recolectada de los diferentes sistemas involucrados.

1.15.6. Política de Seguridad de la Información en la Gestión de la Continuidad del Negocio

1.15.6.1. *Continuidad de Seguridad de la Información*

En el Consorcio SICOV-CRC la gestión de la continuidad del negocio incluirá la seguridad de la información.

1. Planificación de la Continuidad de la Seguridad de la Información

- En el Consorcio SICOV-CRC se definirán los requisitos de seguridad de la información y continuidad de la gestión de la misma ante situaciones adversas, de crisis o desastres presentados en la organización.

  Es responsabilidad del Oficial de Seguridad de la Información velar por la realización de las pruebas del plan de continuidad y controlar la

implementación del mismo.

La Gerencia de Consorcio SICOV deberá invocar la aplicación del plan de continuidad de negocio según sea necesario.

Los usuarios del sistema deberán acceder al aplicativo en contingencia sin necesidad de realizar cambios adicionales en sus equipos.

Todo el personal de Consorcio SICOV-CRC y sus terceros deberán atender los requerimientos de continuidad que se establezcan dentro del plan, acatando las órdenes y requerimientos que se entreguen para continuar con la operatividad del sistema de información

El equipo de Gestión Tecnológica debe garantizar el correcto funcionamiento de los servidores de contingencia y su respectiva actualización con respecto a las librerías de los aplicativos, asegurando la mínima afectación posible para el negocio a nivel de accesos a la plataforma.

El Administrador de Base de Datos debe garantizar la adecuada replicación de la información en el centro alterno de contingencia, asegurando la mínima afectación posible para el negocio a nivel de datos.

Ver documentos de:

- Plan de Continuidad del Negocio

a. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

En Consorcio SICOV-CRC se dispondrá e implementará un proceso de gestión de la continuidad del negocio que incorpore requisitos de seguridad de la información. (Ver documento *Plan de Continuidad del Negocio)*

Es deber de los colaboradores y terceros cumplir a cabalidad, según su rol dentro del plan de continuidad de negocio los deberes y las responsabilidades asignadas cumpliendo las políticas de Seguridad de la Información.

b. Continuidad del negocio y evaluación de riesgos

En el Consorcio SICOV-CRC se evaluará y actualizará el análisis de riesgos, impacto al negocio y estrategias de continuidad del negocio.

Es deber de los colaboradores y las terceras partes conocer a cabalidad sus riesgos y aplicar las medidas para mitigarlos de forma oportuna, informando

adicionalmente sobre los nuevos riesgos que puedan evidenciar dentro de la implementación de la continuidad de negocio en cada uno de sus procesos.

c. Planes de emergencia, contingencia y recuperación

En el Consorcio SICOV-CRC se definirán, actualizarán y probarán los planes de contingencias, emergencias y recuperación establecidos como parte de la continuidad del negocio.

Es deber de los colaboradores y terceras partes conocer el plan de emergencias de la compañía y conocer cuáles son sus procedimientos a ejecutar en caso de una contingencia o en caso de la recuperación de los servicios que ejecutan o a los que prestan apoyo.

d. Estructura para la planificación de la continuidad del negocio

En el Consorcio SICOV-CRC se mantendrá una sola estructura sobre los planes de continuidad del negocio establecidos, consistentes y que incluyan los requisitos de seguridad de la información, prioridades de pruebas y mantenimiento de los mismos.

e. Desarrollo e implementación de planes de continuidad

En el Consorcio SICOV-CRC se desarrollarán e implementarán los planes de continuidad del negocio conforme a las necesidades para mantener las operaciones en normal funcionamiento, asegurando la prestación del servicio para el cumplimiento de su misión y visión.

2. Implementación de la Continuidad del Negocio Incluida la Seguridad de la Información

En Consorcio SICOV-CRC se establecerá, documentará, implementará y mantendrá la continuidad del negocio conforme al cumplimiento de los requisitos legales, contractuales y de buenas prácticas de seguridad de la información establecidas en la organización.

La implementación está detallada en el Análisis de Impacto de Negocio de la organización.

Es deber de los colaboradores conocer el plan de continuidad de negocio y seguirlo según su proceso y según el tipo de evento que se presente de tal manera que se disminuya el impacto adverso en su proceso y en el negocio.

3. Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la

Información

En el Consorcio SICOV-CRC se verificará, validará y evaluará la continuidad del negocio en cumplimiento de los requisitos legales, contractuales y de buenas prácticas de seguridad de la información establecidas en la organización.

Es deber de los colaboradores verificar, revisar y evaluar que los planes de continuidad de negocio planteados para sus áreas cumplen a cabalidad con lo que se requiere para continuar con la operación, en caso de incumplimiento, deberán reportarle al Oficial de Seguridad de la información y a la Gerencia de Consorcio SICOV el caso para que se tomen las medidas pertinentes de ajustes del plan.

1.15.6.2. *Redundancias*

En el Consorcio SICOV-CRC se asegurará la disponibilidad de la información y de las instalaciones donde realiza sus operaciones.

1. Disponibilidad de Instalaciones de Procesamiento de Información

En el Consorcio SICOV-CRC se dispondrá de instalaciones alternas que le permitan de manera redundante y suficiente continuar con las operaciones de su negocio frente a situaciones adversas.

Es deber de los terceros implicados en el proceso de montaje, instalación, configuración y mantenimiento de las instalaciones, mantener y subir los servicios de las mismas en el caso en el que se requiera de su uso.

Es deber de los colaboradores conocer y utilizar en los casos en los que se requiera los servicios de contingencia apuntando a las nuevas instalaciones en los casos en los que se presente una contingencia de negocio.

2. Respaldo y continuidad del negocio

Consorcio SICOV-CRC debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.

Es deber de los colaboradores cumplir a cabalidad con todas las recomendaciones y todas las indicaciones dadas por el Oficial de Seguridad y por la Gerencia de Consorcio SICOV en cuanto a cumplimiento de las políticas de continuidad de negocio y de Backup con el fin de garantizar su información.

1.16. Política de Cumplimiento

1.16.1. Cumplimiento de Requisitos Legales y Contractuales

En el Consorcio SICOV-CRC se cumplirán las obligaciones legales, estatutarias y contractuales relacionadas con la seguridad de la información. Implementando todas las medidas humanas y tecnológicas que garanticen el adecuado cumplimiento de los Requisitos.

1. Identificación de la Legislación Aplicable y de los demás Requisitos

En el Consorcio SICOV-CRC se identificarán, documentarán y mantendrán actualizados todos los requisitos legales y otros requisitos relacionados con la seguridad de la información. Estableciendo todas las acciones pertinentes al cumplimiento.

2. Derechos de Autor y Propiedad Intelectual

En el Consorcio SICOV-CRC se cumplirán los requisitos contractuales y legales vigentes sobre derechos de autor y propiedad intelectual, uso de software licenciado e información utilizada en la organización para sus operaciones.

3. Protección de Registros

En el Consorcio SICOV-CRC se protegerán los registros de todos los procesos contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con los requisitos contractuales, legales vigentes y políticas de seguridad de la información establecidas.

4. Política de Tratamiento de Datos Personales

De acuerdo con los requisitos legales vigentes relacionados con el tratamiento de la información de datos personales y al implementar buenas prácticas de seguridad de la información, Consorcio SICOV-CRC en calidad de responsable y encargado de los mismos define la Política de Tratamiento de la Información de Datos Personales. (Ver documento *Política de Tratamiento de Datos de Personales*).

5. Reglamentación de Controles Criptográficos

En el Consorcio SICOV-CRC se establecerán e implementarán controles criptográficos de acuerdo con los requisitos contractuales y legales vigentes que preserven la seguridad de la información. Así mismo, se dará prioridad a los cifrados más seguros siempre que la legislación no se actualice para considerar los

nuevos algoritmos de cifrado que existan en el mercado.

1.16.1.1. *Revisiones de Seguridad de la Información*

1. Revisión Independiente de la Seguridad de la Información

En el Consorcio SICOV-CRC se revisarán periódicamente cada semestre y de manera independiente todos los activos y elementos que hacen parte del Sistema de Gestión de Seguridad de la Información y su implementación.

Es deber del Oficial de Seguridad de la información solicitar el escaneo de vulnerabilidades a los terceros que se escoja como proveedor de la realización de dicha actividad y verificar que el mismo ejecuta la actividad.

Los colaboradores y terceros implicados en la corrección de las vulnerabilidades deberán dar cierre a las mismas de forma oportuna una vez reciban el consolidado de las mismas.

2. Cumplimiento con las Políticas y Normas de Seguridad

Los líderes de proceso de Consorcio SICOV-CRC deben revisar permanentemente el cumplimiento de las políticas de seguridad de la información y tratamiento de datos personales en su área y proceso bajo su responsabilidad de acuerdo a los requisitos contractuales y legales vigentes.

Todos los colaboradores y terceras partes deberán conocer y dar cumplimiento con las políticas de seguridad y de tratamiento de datos personales según aplique.

3. Revisión del Cumplimiento Técnico

En el Consorcio SICOV-CRC se realizarán revisiones periódicas o cuando se considere necesario sobre el cumplimiento de las políticas de seguridad de la información en todos los sistemas de información que hacen parte de las operaciones de su negocio.

Es deber de todos los colaboradores reportar cualquier módulo de los sistemas de información que manejan que no esté cumpliendo con las políticas de seguridad de la información, así mismo, es deber diseñar los módulos, siempre que aplique, alineados a las políticas de seguridad de la información de la compañía.

1.17. *De los Delitos Informáticos*

1. Acceso Abusivo al Sistema Informático

a. El funcionario que sin autorización o por fuera de lo acordado, acceda en todo o en parte a los sistemas informáticos protegidos de Consorcio SICOV-CRC o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, o del propietario del activo de la información, serán acreedores a las sanciones contenidas en el Artículo 269A de la Ley 1273 de 2009 denominado acceso abusivo al sistema informático.

b. Lo anterior sin perjuicio de las acciones judiciales y/o disciplinarias que pueda iniciar Consorcio SICOV-CRC para el pago o resarcimiento de los perjuicios que dicha conducta le ocasione.

2. Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicaciones

a. El funcionario que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a sistemas informáticos de Consorcio SICOV-CRC, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, serán acreedores a las sanciones contenidas en el Artículo 269B de la Ley 1273 de 2009 denominado obstaculización ilegítima de sistema informático o red de telecomunicaciones.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago o resarcimiento de los perjuicios que dicha conducta le ocasione.

3. Interceptación de Datos Informáticos

a. El funcionario que, sin orden judicial previa, o sin las debidas autorizaciones, intercepte datos informáticos en su origen, destino o en el interior de sistemas informáticos de Consorcio SICOV-CRC, o a las emisiones electromagnéticas provenientes de un sistema informático que los transporte, serán acreedores a las sanciones contenidas en el Artículo 269C de la Ley 1273 de 2009 denominado interceptación de datos informáticos.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago de los perjuicios que dicha conducta le ocasione.

4. Daño Informático

a. El funcionario que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos de Consorcio SICOV-CRC, o un

sistema de tratamiento de información o sus partes o componentes lógicos, serán acreedores a las sanciones contenidas en el Artículo 269D de la Ley 1273 de 2009 denominado daño informático.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago de los perjuicios que dicha conducta le ocasione.

5. Uso de Software Malicioso

a. El funcionario que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga de Consorcio SICOV-CRC o del Territorio Nacional software malicioso u otros programas de computación de efectos dañinos, serán acreedores a las sanciones contenidas en el Artículo 269E de la Ley 1273 de 2009 denominado uso de software malicioso.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago de los perjuicios que dicha conducta le ocasione.

6. Violación de Datos Personales

a. El funcionario que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, será acreedor a las sanciones contenidas en el Artículo 269F de la Ley 1273 de 2009 denominado violación de datos personales.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago y/o resarcimiento de los perjuicios que dicha conducta le ocasione.

7. Suplantación de Sitios Web para Capturar Datos Personales

a. El funcionario que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, será acreedor a las sanciones contenidas en el Artículo 269G de la Ley 1273 de 2009 denominado suplantación de sitios Web para capturar datos personales.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago de los perjuicios que dicha conducta le ocasione.

8. Hurto por Medios Informáticos y Semejantes

a. El funcionario que, superando medidas de seguridad informáticas, realice la conducta señalada en el Artículo 239 del Código Penal manipulando el sistema informático, la red de sistema electrónico, telemático u otro medio semejante de Consorcio SICOV-CRC, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, será acreedor a las sanciones contenidas en el Artículo 2691 de la Ley 1273 de 2009 denominado hurto por medios informáticos y semejantes.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago de los perjuicios que dicha conducta le ocasione.

9. Transferencia No Consentida de Activos

a. El funcionario que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de Consorcio SICOV-CRC, será acreedor a las sanciones contenidas en el Articulo 269J de la Ley 1273 de 2009 denominado transferencia no consentida de activos.

b. Lo anterior sin perjuicio de las acciones judiciales que pueda iniciar Consorcio SICOV-CRC para el pago de los perjuicios que dicha conducta le ocasione.

1.18. *Disposiciones Generales*

1. Cumplimiento del Manual del Sistema de Gestión de Seguridad de la Información

La Alta Dirección de Consorcio SICOV-CRC, velará porque se dé estricto cumplimiento a las disposiciones contenidas en el presente Manual. Su incumplimiento constituye una causal para iniciar las actuaciones disciplinarias contenidas en el *Reglamento Interno de Trabajo* de Consorcio SICOV-CRC, que pueden culminar con las sanciones allí dispuestas dada la gravedad de los hechos.

2. Publicidad

El presente Manual y cualquier modificación al mismo, deberá ser aprobado por la Alta Dirección, y ser publicado a través del sitio definido por Consorcio SICOV-CRC y comunicado a los colaboradores a través de sus correos electrónicos institucionales u otros medios.

3. Custodia de la información

El presente manual estará bajo la custodia de la Gerencia de Consorcio SICOV y del Oficial de Seguridad de la Información, quienes tendrán a su cargo consolidar, proponer, depurar, analizar y coordinar las modificaciones o adiciones correspondientes y necesarias, además de propender por la difusión y conocimiento del mismo.

4. Reforma

El Oficial de Seguridad y la Gerencia de Consorcio SICOV son los encargados de efectuar revisiones al texto del presente Manual como resultado de su aplicación para adaptarlo a nuevas normas o disposiciones legales sobre la materia que surjan, para la aprobación de este.

5. Vigencia

El presente Manual entra en vigor a partir de su aprobación de la Gerencia de Consorcio SICOV y *deroga todas* las normas y demás disposiciones que le *sean contrarias o que se consideren obsoletas.*