REPUBLICA DE COLOMBIA

DEPARTAMENTO DEL VALLE DEL CAUCA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VALLECAUCANA DE AGUAS S.A. E.S.P.

ENERO 2019

TABLA DE CONTENIDO

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1. Definición

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de Vallecaucana de Aguas S.A. E.S.P., con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Vallecaucana de Aguas S.A. E.S.P., para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

a) Mitigar los riesgos tecnológicos de la entidad.
b) Cumplir con los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Implementar el sistema de gestión de seguridad de la información.
g) Proteger los activos de información.
h) Establecer las políticas, procedimientos e instructivos en materia de Seguridad de la Información.
j) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos de Vallecaucana de Aguas S.A. E.S.P.
k) Garantizar la continuidad del servicio frente a incidentes.

1.2. Alcance

Esta política aplica a toda la entidad, servidores públicos y contratistas de Vallecaucana de Aguas S.A. E.S.P.

1.3. Base legal

Decreto 1151 de 2008 se estableció como objetivo de la Estrategia Gobierno en Línea "Contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación".
La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG).

La política de Gobierno Digital tiene como ámbito de aplicación, las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas.

1.4. MARCO DE ESTÁNDARES NORMATIVOS

1.4.1. SERIE DE NORMAS TÉCNICAS COLOMBIANAS NTC ISO/IEC 27000 – SGSI **–** Facilita La implementación de estándares de seguridad de la información y los sistemas computarizados de la Empresa.
1.4.2. SERIE DE NORMAS TÉCNICAS COLOMBIANAS NTC-ISO31000 Gestión del Riesgo **–** Contribuye al logro demostrable de los objetivos y a la mejora en el desempeño.
1.4.3. ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio –.

Los requisitos son un estándar de sistema de administración que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de administración documentado para proteger, reducir la probabilidad de ocurrencia, prepararse para, responder y recuperarse de incidentes disruptivos cuando surjan.

1.5. Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.
A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de Vallecaucana de Aguas S.A. E.S.P.

a) Vallecaucana de Aguas S.A. E.S.P., ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado

en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
c) Vallecaucana de Aguas S.A. E.S.P., protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.
d) Vallecaucana de Aguas S.A. E.S.P., protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
e) Vallecaucana de Aguas S.A. E.S.P., protege su información de las amenazas originadas por parte del personal.
f) Vallecaucana de Aguas S.A. E.S.P., protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
g) Vallecaucana de Aguas S.A. E.S.P., controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) Vallecaucana de Aguas S.A. E.S.P., implementa controles de acceso a la información, sistemas y recursos de red.
i) Vallecaucana de Aguas S.A. E.S.P., garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) Vallecaucana de Aguas S.A. E.S.P., garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
k) Vallecaucana de Aguas S.A. E.S.P., garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos de diferentes tipos ambientales.
l) Vallecaucana de Aguas S.A. E.S.P., garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Nota: “El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere”.

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1. Justificación

Vallecaucana de Aguas S.A. E.S.P., con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.
La seguridad de la información se entiende como la preservación de las siguientes características:

a) **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

2.2. Conceptos de seguridad de la información.

Adicionalmente, debe considerarse los conceptos de:

Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
No repudio: se refiere a evitar que una entidad que haya enviado o recibido información
NTC: Norma Técnica Colombiana.
Usuario Final: Es aquel funcionario que, por necesidades de su cargo, se le asignan recursos de cómputo, convirtiéndose así en un usuario del área de Sistemas.
Hardware: Son los equipos de cómputo, por ejemplo, Microcomputador o PC, impresora, módem, terminal portátil.
Firewall: Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos

configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.
Software: Son los programas que se ejecutan en los Microcomputadores.
Sistema Operativo: Programa central que administra el computador, sobre el que corren los demás programas.
Estación de trabajo: Es un ordenador que facilita a los usuarios el acceso a los servidores y periféricos de la red. A diferencia de un ordenador aislado, tiene una tarjeta de red y está físicamente conectada por medio de cables u otros medios no guiados con los servidores.
Sistemas de información: Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.

2.2.1. Criterios de Seguridad de la información:

Integridad: Capacidad para producir y mantener la información recibida o generada como resultado de cumplir las funciones del cargo, que sea precisa, coherente con las normas internas y externas, autorizada y completa.
Confidencialidad: Capacidad para producir y mantener la información recibida o generada como resultado de cumplir las funciones del cargo, debidamente protegida de accesos, modificaciones, consultas o borrado no autorizado.
Disponibilidad: Capacidad para producir y mantener la información recibida o generada como resultado de cumplir las funciones del cargo, disponible en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

2.2.2. Criterios de Calidad de la información

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.
Confiabilidad: La información debe ser la apropiada para la administración del Vallecaucana de Aguas S.A. E.S.P y el cumplimiento de sus obligaciones.
Vulnerabilidad informática: Ausencia o deficiencia que permite violar las medidas de seguridad informáticas para poder acceder a un canal de distribución o a un sistema específico de forma no autorizada y emplearlo en beneficio propio o como origen de ataques por parte de terceros.
Cifrado fuerte: Técnicas de codificación para protección de la información que utilizan algoritmos de robustez reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES y/o AES.

Sistema de Acceso Remoto (RAS): Para efectos de la presente circular, RAS hace referencia a la conexión realizada por un tercero a los sistemas de información de la entidad utilizando enlaces dedicados o conmutados.
Operaciones: Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que presta el Vallecaucana de Aguas S.A. E.S.P, clientes o usuarios Ej. Consulta de estado de licencias, permisos ambientales etc.
Cliente: Es toda persona natural o jurídica con la cual la Entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad.
Usuario: Aquella persona natural o jurídica a la que, sin ser cliente, la Entidad le presta un servicio.
Servicio: Es toda aquella interacción del Vallecaucana de Aguas S.A. E.S.P con sus clientes y usuarios para el desarrollo de su objeto social.
Dispositivo: Mecanismo, máquina o aparato dispuesto para producir una función determinada.
Eficacia: Capacidad de alcanzar o lograr las metas y/o resultados propuestos del cargo para los objetivos planteados.
Eficiencia: Capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.
Autocontrol: Capacidad de todos y cada uno de los funcionarios de la Entidad, independientemente de su nivel jerárquico para evaluar y controlar su PROPIO trabajo, detectar desviaciones y efectuar correctivos en el ejercicio y cumplimiento de sus funciones, así como para mejorar sus tareas y responsabilidades.
Autorregulación: Capacidad de la Vallecaucana de Aguas S.A. E.S.P para desarrollar en su interior, aplicando métodos, normas y procedimientos que permitan el desarrollo, implementación del SGSI, dentro del marco de las disposiciones legales aplicables.
Autogestión: Capacidad de la Entidad para interpretar, coordinar, ejecutar y evaluar de manera eficiente y eficaz su funcionamiento.
Hurto / Fraude: Actos de corrupción o delincuenciales que de forma intencionada defraudan y se apropian de activos de la Entidad. En este tipo de eventos pueden verse implicados empleados o personas externas a la Entidad.
Colusión: Pacto ilícito de varias personas para cometer un daño contra la Entidad.
Falsificación de dinero, cheques, títulos valores o documentos: Falsear o adulterar el papel, texto o números de contenido, forma, o firmas de billetes, cheques, títulos valores y otros documentos comerciales originales, con fines contrarios a la Ley.
Fraude en Contrato: Cuando el encargado de suscribir o vigilar la ejecución de contratos donde participa la Entidad, se confabula con intereses opuestos a los de la Entidad.
Fraude (Definición General): Acción contraria a la verdad y a la rectitud que perjudica a la persona contra quien se comete.

Fraude en cuentas por cobrar: Acto del deudor de la cuenta, generalmente simulado y rescindible, que deja al acreedor sin medio de cobrar lo que se le debe.
Fraude en Cuentas por pagar: Acto malicioso en contra de la Empresa para beneficiar inapropiadamente al acreedor de una cuenta por pagar, incluyendo proveedores, acreedores, contratistas, empleados con supuestos pagos laborales por pagar, entre otros.
Malversación de Fondos: Cuando empleados de la Entidad sustraen o facilitan que terceros sustraigan caudales económicos u otros activos, cuando tienen custodia o administración sobre los mismos.
Sanciones: Sanciones por incumplimiento de leyes o normas oficiales, en cualquier contexto, sea: laboral, comercial, tributario, cambiario, civil, penal, entre otros.
Pérdida de Imagen y Credibilidad Pública: Pérdida de reputación de la Empresa, desprestigio público, mala imagen, publicidad negativa, cierta o no, con respecto de la Empresa y sus prácticas de gestión humana, o sobre la administración de las compras, o debido a una percepción negativa en la calidad de los productos o servicios prestados de la Entidad, o por sospechas de mal manejo, no transparente, de sus activos, de forma que se cause pérdida de clientes y disminución de ingresos, especialmente cuando los productos o servicios también son ofrecidos por empresas competidoras.
Daño o Destrucción de Activos: Pérdidas por daños o perjuicios de activos físicos.
Fallas Tecnológicas: Pérdidas por incidentes de fallas tecnológicas en el hardware, software, peopleware (personal de sistemas o usuarios, que interactúa con la tecnología informática) y las telecomunicaciones.
Errores en la Ejecución y Administración de Procesos: Pérdidas por errores u omisiones en la ejecución y administración de los procesos. Incluye: Falta de planeación, falta de metas, falta de control, decisiones erróneas, desempeño deficiente, ineficiencia e ineficacia en los procesos, errores humanos (involuntarios) en la ejecución de los mismos.
Exceso de Egresos: Pérdida cuando la Caja gasta más dinero del presupuestado, o por errores consistentes en pagos de mayor valor, por cualquier concepto, pagos dobles o compras sin la debida evaluación costo-beneficio.
Pérdida de Ingresos: Dejar de ganar, perder clientes, falta de recuperación de cuentas por cobrar, principalmente.
Factores de Riesgo: Son las fuentes generadoras de eventos adversos y perjudiciales para la Entidad. Ejemplos: Recurso humano, procesos, tecnología, infraestructura y acontecimientos externos.
La Entidad clasifica los factores de riesgo en internos y externos, así:
Factores Internos
Talento Humano: Personas vinculadas directa o indirectamente para que ejecuten los procesos de la Entidad. Ejemplos: Proveedores / Ejecutores de Procesos / Clientes de los procesos.

- **Vinculación directa:** Por contrato de trabajo según la legislación laboral vigente.

- **Vinculación indirecta:** Para personas que prestan servicios externos, diferente a los que se originan en un contrato de trabajo.
- **Procesos:** Conjunto de actividades interrelacionadas para transformar entradas en productos o servicios con un valor agregado, a fin de satisfacer determinadas necesidades de los clientes del proceso.
- **Tecnología:** Conjunto de dispositivos, metodologías y procedimientos para automatizar procesos de la Entidad. Incluye: hardware, software y telecomunicaciones.
- **Infraestructura:** Conjunto de elementos que se necesitan para el funcionamiento de una Entidad. Ejemplos: edificios, instalaciones de trabajo, muebles y enseres, bodegas y transporte, principalmente.

Factores Externos: Eventos relacionados con la naturaleza u ocasionados por terceros, cuyas causas escapan al control de la Entidad.
Impacto del Riesgo: Pérdidas económicas por la ocurrencia de un determinado evento de riesgo, incluyendo los gastos derivados de su tratamiento.
Perfil de Riesgo: Resultado consolidado de acumular riesgos residuales ocurridos o a los que está expuesta la Empresa durante un periodo de tiempo en años.
Plan de Contingencias, Recuperación y Continuidad de Operaciones: Conjunto de procedimientos, sistemas y recursos necesarios para enfrentar contingencias, recuperar la funcionalidad de los procesos (manuales y sistematizados) y normalizar la continuidad de la operación de los mismos, cuando se presente una interrupción prolongada (según cada sistema) durante un lapso mayor al máximo tolerable. Las causas pueden ser: fallas humanas, fenómenos de la naturaleza, fallas tecnológicas, daño o destrucción de las instalaciones físicas, entre otras causas.
Probabilidad Anual del Riesgo: Resultado de dividir la cantidad de años en que ha ocurrido un determinado evento de riesgo por el número de años en que se ha medido su posible ocurrencia.
Riesgo en relaciones con empleadores, trabajadores afiliados, clientes, usuarios y beneficiarios: Fallas negligentes o involuntarias de las obligaciones de la Empresa ante empleadores y trabajadores afiliados, agregando clientes, usuarios y beneficiarios de los servicios sociales que presta la Empresa. Dichas fallas impiden satisfacer una obligación o compromiso frente a aquellos.
Riesgo en las Relaciones Laborales: Actos incompatibles con la legislación laboral, o con los acuerdos internos de trabajo.
Riesgo Inherente: Nivel de riesgo propio de la actividad u objeto social de la Empresa, incluyendo sus áreas de servicios y de Administración, sin considerar el efecto de los controles.
Riesgo Legal: Posibilidad de pérdidas para la Empresa en caso de ser sancionada u obligada a indemnizar por incumplimiento de normas, regulaciones y obligaciones

contractuales. El riesgo legal surge además por errores en los contratos y transacciones, o por actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones de la Empresa.
Riesgo Operativo: Posibilidad de pérdidas para la Empresa por errores o irregularidades de sus empleados, procesos, tecnología, infraestructura o por acontecimientos externos. Esta definición incluye el riesgo legal y el riesgo reputacional.
Riesgo Reputacional: Posibilidad de pérdidas por desprestigio público, mala imagen, publicidad negativa, cierta o no, respecto de la Caja y sus prácticas organizacionales, administrativas, de manera que pueda producirse pérdida de afiliados, clientes o usuarios de servicios o disminución de sus ingresos.
Riesgo Residual: Nivel del riesgo después de la acción de los controles.

2.3. Objetivo

Definir los mecanismos y todas las medidas necesarias por parte del Vallecaucana de Aguas S.A. E.S.P., para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.4. Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de Vallecaucana de Aguas S.A. E.S.P., a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.5. Roles y Responsabilidades

Es responsabilidad del Comité de Seguridad de Vallecaucana de Aguas S.A. E.S.P., la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.
El Comité de Seguridad de la Información cuya composición y funciones serán reglamentadas por una mesa de trabajo compuesta por:
a) Gerente o un delegado especializado.

b) Jefe de la Oficina de Control Interno o un delegado.
c) Director Administrativo
d) Profesional Universitario de apoyo Comunicaciones o delegado,
e) El responsable de Seguridad de la información de la entidad.
f) El encargado de la Gestión TIC

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la alta dirección para su aprobación.

2.6. Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, Vallecaucana de Aguas S.A. E.S.P., se reserva el derecho de tomar las medidas correspondientes.

2.7. Comunicación

Mediante socialización a todos los funcionarios de Vallecaucana de Aguas S.A. E.S.P., se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.
Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.vallecaucanadeaguas.gov.co.

3. DESCRIPCIÓN DE LAS POLÍTICAS

3.1. Generalidades

Vallecaucana de Aguas S.A. E.S.P., en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.
De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los

servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en el EPA.

3.2. Gestión de Activos

3.2.1. Política para la identificación, clasificación y control de activos de información

Vallecaucana de Aguas S.A. E.S.P., a través del Comité de Seguridad de la Información realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.
El facilitador del proceso de Gestión de Recursos Físicos con apoyo del técnico operativo de sistemas tiene la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.
Pautas para tener en cuenta
a) Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y limitación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.
b) La información física y digital de Vallecaucana de Aguas S.A. E.S.P., debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.
c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.
d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el

desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

3.3. Control de Acceso

3.3.1. Política de acceso a redes y recursos de red

El área de tecnología de sistemas de Vallecaucana de Aguas S.A. E.S.P., como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Pautas para tener en cuenta

a) El proceso Gestión de TIC debe asegurar que las redes inalámbricas de Vallecaucana de Aguas S.A. E.S.P., cuenten con métodos de autenticación que evite accesos no autorizados.

b) El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de Vallecaucana de Aguas S.A. E.S.P., así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

c) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de Vallecaucana de Aguas S.A. E.S.P., deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos Vallecaucana de Aguas S.A. E.S.P., deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

3.3.2. Política de administración de acceso de usuarios

Vallecaucana de Aguas S.A. E.S.P., establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y

el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información Vallecaucana de Aguas S.A. E.S.P.; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
b) El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
c) El proceso Gestión de TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
d) Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TIC, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.
e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

3.3.3. Política de control de acceso a sistemas de información y aplicativos

Vallecaucana de Aguas S.A. E.S.P., como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.
El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Pautas para tener en cuenta

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

c) El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos Vallecaucana de Aguas S.A. E.S.P.

d) El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

e) El proceso Gestión de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

f) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

g) Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

h) Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el

3.3.4. Políticas de seguridad física

Vallecaucana de Aguas S.A. E.S.P., provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido. Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso Gestión de TIC conserva las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.
b) El proceso Gestión de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.
c) El Director Administrativo debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones del Vallecaucana de Aguas S.A. E.S.P.
d) El Director Administrativo debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.
e) Los ingresos y egresos de personal a las instalaciones de Vallecaucana de Aguas S.A. E.S.P., en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
f) Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de Vallecaucana de Aguas S.A. E.S.P.; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.
g) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

3.3.5. Política de seguridad para los equipos

Vallecaucana de Aguas S.A. E.S.P., para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Pautas para tener en cuenta

a) El proceso Gestión de TIC debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de Vallecaucana de Aguas S.A. E.S.P.
b) El proceso Gestión de TIC debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

c) El proceso Gestión de TIC en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.
d) El proceso Gestión de TIC debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.
e) El proceso Gestión de TIC debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
f) El proceso Gestión de TIC debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.
g) El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de Vallecaucana de Aguas S.A. E.S.P., cuente con la autorización documentada y aprobada previamente por el área.
h) El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro.
i) El proceso Gestión de TIC es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P.
j) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TIC.
k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la Entidad, el usuario responsable debe informar al facilitador del proceso Gestión de TIC, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios de apoyo al proceso de Gestión de TIC.
m) Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
n) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

o) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
p) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
q) Los funcionarios de la entidad y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

3.3.6. Política de uso adecuado de internet

Vallecaucana de Aguas S.A. E.S.P., consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad

Pautas para tener en cuenta

a) El proceso Gestión de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
b) El proceso Gestión de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
c) El proceso Gestión de TIC debe monitorear continuamente el canal o canales del servicio de Internet.
d) El proceso Gestión de TIC debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
e) El proceso Gestión de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.
f) Los usuarios del servicio de Internet de Vallecaucana de Aguas S.A. E.S.P., deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
g) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
h) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

i) Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Ares, MSN, Yahoo, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del Vallecaucana de Aguas S.A. E.S.P.

j) No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

k) No está permitido el intercambio no autorizado de información de propiedad del Vallecaucana de Aguas S.A E.S.P., de los funcionarios, con terceros.

4. PRIVACIDAD Y CONFIDENCIALIDAD

4.1. Política de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, Vallecaucana de Aguas S.A. E.S.P., a través del Comité de Seguridad de la Información, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.
Se establece los términos, condiciones y finalidades para las cuales Vallecaucana de Aguas S.A. E.S.P., como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, Vallecaucana de Aguas S.A. E.S.P., exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Pautas para tener en cuenta

a) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.
b) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
c) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
d) Las Unidades de Gestión que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y

procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

e) Las Unidades de Gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

f) El comité de seguridad de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de Vallecaucana de Aguas S.A. E.S.P., de los cuales reciba y administre información.

g) El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

h) Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

i) Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico o por correo certificado, entre otros.

j) Los usuarios de los portales de Vallecaucana de Aguas S.A. E.S.P., deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

4.2. Disponibilidad del servicio e información

Vallecaucana de Aguas S.A. E.S.P., con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, ha decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

4.2.1. Política de continuidad, contingencia y recuperación de la información

Vallecaucana de Aguas S.A. E.S.P., proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

4.2.1.1. Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.
Las áreas de Vallecaucana de Aguas S.A. E.S.P., deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.
Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.
El proceso Gestión de TIC debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad.
La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Pautas para tener en cuenta

a) El Comité de Seguridad de la Información, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
b) El Comité de Seguridad de la Información, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres
c) El Comité de Seguridad de la Información debe realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
d) El Comité de Seguridad de la Información debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información
e) El Comité de Seguridad de la Información, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

5. POLÍTICAS DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

5.1. Documentación de procedimientos operativos

Los procedimientos operativos deben especificar las instrucciones detalladas para la ejecución de cada tarea, incluyendo las actividades de administración de sistemas. Dichos procedimientos deben estar documentados formalmente.

5.2. Cronograma de Copias de Seguridad

Los cronogramas de estas operaciones automatizadas que programa el personal de apoyo técnico deben planearse y contar con la autorización del encargado del área de Sistemas.

5.3. Control de Cambios Operacionales

Los cambios operacionales deben probarse exhaustivamente y ser aprobados formalmente antes de ser puestos en producción.

5.4. Respuestas ante incidentes de Seguridad de la Información

El encargado del área de Sistemas debe responder rápidamente a cualquier incidente de Seguridad de la Información, coordinando la recolección de información y sugiriendo medidas a tomar donde sea necesario.

5.5. Protección contra ataques de negación de servicio (DoS)

Se deben tener listos planes de acción contra ataques de negación del servicio (DoS) los cuales deben ser mantenidos y probados periódicamente para asegurarse de su eficacia.

5.6. Análisis de incidentes de Seguridad de la Información ocasionados por fallas de sistemas

Los incidentes de seguridad de la información originados por fallas de hardware o software deben investigarse de manera apropiada por especialistas.

5.7. Confidencialidad de los incidentes de Seguridad de la Información

La información relacionada a incidentes de seguridad de la información sólo puede ser divulgada entre personas autorizadas.

5.8. Segregación de funciones

Necesidad de control dual / segregación de funciones
Donde quiera que un incidente de seguridad de la información pueda ocasionar daño material o financiero a la Entidad, debe emplearse técnicas de control dual y segregación de funciones para mejorar el control de procedimientos de seguridad.

5.9. Separación de los ambientes computacionales de desarrollo y de producción

El encargado del área de Sistemas debe asegurarse que existe una segregación de funciones apropiada en todas las áreas encargadas de funciones de desarrollo, operaciones y administración de sistemas.

5.10. Tercerización de operaciones

En el caso de tercerización de operaciones, se deben identificar los riesgos por anticipado e incorporar al contrato las medidas de seguridad apropiadas.

5.11. Planeamiento de capacidad y prueba de nuevos sistemas

Para las pruebas de nuevos sistemas se deben aplicar criterios de capacidad, carga máxima y prueba de stress. Debe demostrarse que sus niveles de rendimiento y resistencia cumplen o exceden las necesidades o requisitos técnicos de la Entidad.

5.12. Paralelo de sistemas

Los procedimientos de prueba de sistemas deben considerar un período de funcionamiento paralelo antes que el sistema nuevo o mejorado sea aceptado para su uso en producción. Los resultados del paralelo no deben revelar problemas o dificultades diferentes a los ya vistos durante la prueba de aceptación de usuario.

5.13. Elaboración de bases de datos

Antes de poner una base de datos en producción, se deben realizar pruebas exhaustivas de su funcionamiento, tanto a nivel lógico de su estructura, como de su eficiencia en un ambiente de producción.

5.14. Medidas y controles contra software malicioso

Todos los recursos activos de tratamiento de información: infraestructura de red, software base y de aplicación, deben configurarse y protegerse adecuadamente contra ataques físicos e intrusión.

5.15. Defensa contra virus informáticos

Todas los PCs y servidores de la Entidad deben tener instalado un software antivirus actualizado diariamente. Igualmente, se deben escanear regularmente todos los equipos. El software antivirus debe adquirirse de un proveedor reconocido, que tenga soporte técnico adecuado.

5.16. Respuesta a incidentes de virus

Se debe desarrollar una estrategia integral y procedimientos de actuación para hacer frente a los virus informáticos, lo cual incluirá procedimientos y responsabilidades de administración, capacitación en el uso de software antivirus y recuperación después de los ataques de virus.

5.17. Descargar archivos e Información de Internet

Se debe tener mucho cuidado al descargar información y archivos de Internet a fin de evitar el ingreso de código malicioso, así como la descarga de material no apropiado.

5.18. Certeza de orígenes de archivos

Los archivos electrónicos recibidos de remitentes desconocidos deben ser eliminados sin ser abiertos.

5.19. Instalación usuaria de software adicional

Está prohibido instalar software no autorizado en las computadoras de la Entidad, tales como protectores de pantalla, software demostrativo, manejadores de música, video, mensajería instantánea, juegos, protectores de pantalla, aplicativos particulares (software con licencia adquirido por el usuario para uso doméstico), aplicativos recibidos por la red (correo electrónico, internet), aplicativos entregados en calidad de prueba; salvo autorización del encargado del área de Sistemas, para fines de evaluación y pruebas preliminares.

5.20. Respaldo y recuperación de la información.

Es de alta prioridad generar copias de respaldo de archivos de datos (backup) de la Entidad y garantizar la capacidad de restaurarlos. El encargado del área de Sistemas será responsable de que la frecuencia de tales operaciones y que los procedimientos aplicados se adecuan a las necesidades de la Entidad.

5.21. Monitoreo de los logs de operaciones

Los registros de log operacional deben ser revisados periódicamente por personal calificado y las discrepancias con los procedimientos operacionales deben ser comunicadas al usuario propietario de información y al encargado del área de Sistemas.

5.22. Registro y reporte de fallas de equipos

Toda falla de equipos (incluyendo daños) debe anotarse en un registro especialmente designado para tal fin por el personal encargado de su mantenimiento.

5.23. Registro y reporte de fallas de software

Se debe registrar y reportar formalmente toda falla de software a los responsables de soporte de software.

5.24. Gestión de redes

Los administradores de redes deberán implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadoras, así como la integridad de la red y protección de los servicios conectados contra accesos no autorizados.

5.25. Uso de medios removibles de almacenamiento

Solamente el personal autorizado a instalar o a modificar el software podrá utilizar medios removibles para transferir datos de la Entidad. Cualquier otra persona requerirá autorización expresa.

5.26. Eliminación segura de documentos

Todos los documentos de naturaleza confidencial deben ser destruidos cuando ya no se requieren. El dueño del documento debe autorizar o realizar esta destrucción.

5.27. Eliminación de Software

Sólo se debe eliminar un programa de software cuando se haya decidido que dicho programa ya no es necesario y que no se necesita tener acceso a sus archivos de datos mediante dicho programa.

5.28. Uso de buenas prácticas de gestión de información

Todos los usuarios deben proteger la confidencialidad, integridad y disponibilidad de los archivos durante la creación, almacenamiento, modificación, copiado y borrado/eliminación de archivos de datos.

5.29. Comprobación de exactitud y validez de documentos

Se debe confirmar la validez e integridad de documentos, especialmente aquellos que comprometen u obligan a la Entidad.

5.30. Dependencias entre documentos y archivos

Los documentos altamente sensibles o críticos no deben depender de la disponibilidad o integridad de archivos de datos sobre los que el autor no tenga control. Los documentos e informes importantes deben ser autónomos y contener toda la información necesaria.

5.31. Fotocopiado de información confidencial

Los trabajadores deben conocer los riesgos de brechas de confidencialidad durante el fotocopiado/duplicación de documentos. Sólo se debe duplicar documentos confidenciales con la debida autorización del dueño del documento.

5.32. Eliminación de archivos temporales (tmp)

Los archivos temporales en las computadoras de usuarios deben ser eliminados con regularidad para prevenir su posible mal uso por usuarios no autorizados.

5.33. Seguridad de la documentación de sistemas

La documentación de sistemas es un requisito obligatorio para todo sistema de información de la Entidad. Dicha documentación debe mantenerse actualizada y disponible.

5.34. Envío de información a terceros

Antes de enviar información a terceros, se debe verificar que el receptor está autorizado a recibir dicha información y que las medidas adoptadas por los receptores aseguran la confidencialidad e integridad de la información que se envía.
Se prohíbe facilitar reportes impresos, documentos, acceso a computadores personales e información propia de logs a personas ajenas a la Entidad, sin autorización.

5.35. Transporte de documentos confidenciales

Las medidas de protección de la confidencialidad, integridad y disponibilidad en el transporte o transmisión de documentos confidenciales serán establecidas por los dueños de dichos documentos, quienes deberán asegurarse que tales medidas son las apropiadas.

5.36. Desarrollo y mantenimiento de sitios Web

Solamente personal debidamente calificado y autorizado participará en el desarrollo y mantenimiento de sitios Web de la Entidad.

5.37. Seguridad en el Envío de correo electrónico.

Se debe utilizar el correo electrónico solamente para fines relacionados con la Entidad. Antes de adjuntar archivos a un mensaje de e-mail se debe verificar que la clasificación de información de dicho archivo permite su envío al destinatario previsto y también. Previamente se debe escanear y verificar que no exista virus u otro código malicioso.

5.38. Seguridad en la Recepción de correo erróneo

Los mensajes de correo electrónico no solicitado deben ser tratados con precaución y no ser respondidos.

5.39. Recepción de correo no solicitado

Se debe verificar la identidad y la autenticidad del remitente de cualquier mensaje de correo electrónico no solicitado antes de abrirlo.

5.40. Uso de correo electrónico

Está prohibido usar el correo electrónico para las labores ajenas a la Entidad. Se debe evitar el uso de lenguaje obsceno y/o abusivo.

Si se reciben mensajes de cadenas recomendando que los distribuya a sus amigos, NO lo haga. Elimínelos sin abrirlos.

Está prohibido el envío y distribución de mensajes desde el correo electrónico corporativo no relacionados con el desarrollo de las actividades de la Entidad. Cada empleado con acceso a Internet podrá utilizar su correo electrónico personal de forma razonable.
Se deberá tener en consideración que los mensajes enviados por el correo electrónico tendrán plena validez para todos los efectos, es decir serán considerados como documentos oficiales. Se deberá revisar los mensajes antes de enviarlos, verificando el

destinatario y/o las listas de distribución, para asegurarse que todos los receptores del correo requieren conocer la información.

5.41. Seguridad de sistemas públicamente disponibles

Se deben establecer controles en los sistemas públicamente disponibles de captura de información con la finalidad que la información confidencial se proteja durante su recojo y almacenamiento, y que el acceso a dicho sistema no permita accesos no autorizados a otras redes a las que está conectado el sistema.

5.42. Transmisión e intercambio de información de banca virtual u otra confidencial

Solamente se puede transmitir datos o información de banca virtual u otro tipo de información confidencial cuando la seguridad de los datos puede garantizarse razonablemente usando técnicas de encriptación.

5.43. Control de distribución de información

Los datos e información deben protegerse mediante controles técnicos y administrativos a fin de asegurarse que están disponibles solo para personas autorizadas.

5.44. Estándares de control de acceso

Los estándares de control de acceso de los sistemas de información deben establecerse de manera que prevengan ingresos de usuarios no autorizados y a la vez proporcionen acceso inmediato según los requerimientos de la Entidad.

5.45. Estructura de carpetas y datos para usuarios

Las estructuras de carpetas de datos de la red compartidos por los usuarios deben ser definidas por el encargado del área de Sistemas y los usuarios deben seguir dicha estructura. Las restricciones de acceso se deben aplicar para evitar o prevenir el acceso no autorizado.

5.46. Protección de documentos electrónicos con contraseñas

Se debe proteger la información confidencial usando, preferentemente, el control de acceso de la carpeta donde está situado el archivo correspondiente. No se recomienda el uso solamente de contraseñas para proteger documentos.

5.47. Defensa contra ataques internos intencionales

Los estándares de control de acceso y de clasificación de datos deben ser revisados y actualizados periódicamente para reducir la incidencia y la posibilidad de ataques internos.

Configuración de acceso a la Intranet. Se configuro la Intranet en Vallecaucana de Aguas S.A.E.S.P. y se socializo con los Jefes de área y procesos de esta Entidad.

5.48. Configuración de acceso a Internet

El personal encargado de configurar el acceso a Internet debe asegurarse que la red de la Entidad tenga la debida protección. Como mínimo se debe instalar un firewall debidamente configurado.

5.49. Acceso a información sobre proyectos de la Entidad

Solamente personas autorizadas pueden tener acceso a datos confidenciales sobre proyectos de propiedad de la Entidad o administrados por sus ejecutivos.

5.50. Documentación de sistemas

Todos los sistemas deben tener documentación completa y actualizada. Ningún sistema debe pasar a producción si no tiene la documentación de soporte disponible.

5.51. Análisis y especificación de los requisitos de seguridad

Todo desarrollo de software, dentro o fuera de la Entidad, debe contar con un sustento técnico-económico, un presupuesto adecuado, una justificación basada en requerimientos de usuario previamente descritos, analizados y aprobados al nivel adecuado por el encargado del área de Sistemas y del área usuaria. Así mismo debe existir un compromiso de disponer de los recursos necesarios para solventar el proyecto de inicio a fin.
La aprobación final del proyecto debe ser por parte de la Dirección Administrativa.

5.52. Desarrollo y mantenimiento de software

Las especificaciones técnicas y funcionales para el desarrollo y mantenimiento de software deben contemplar formalmente los requerimientos de seguridad, incluyendo los controles técnicos de acceso, la asignación restringida de privilegios y otros requisitos que resulten convenientes para dicha aplicación.

5.53. Interfaz de software aplicativo

El desarrollo de interfaz de sistemas es una tarea altamente especializada y por lo tanto sólo debe ser realizada por profesionales con la debida calificación y experiencia comprobada en el tema. Debe considerar sobremanera los aspectos de seguridad de los sistemas que son conectados y de las plataformas que intervienen.

5.54. Reporte de eventos y debilidades de la Seguridad de la Información

El área de Sistemas debe establecer un procedimiento formal de reporte de eventos o incidentes de riesgos sobre la seguridad de la información que indique las respuestas y las acciones que deben ser tomadas.

5.55. Procedimiento del reporte

Los procedimientos de reporte del cual deben tener conocimiento los empleados, contratistas y terceros, deben incluir: procesos de retroalimentación que aseguren que los eventos sean notificados; formulario de reporte, el cual apoya la acción del reporte y ayuda al encargado del reporte a recordar las acciones necesarias cuando se produce un evento.

5.56. Evidencias del evento de riesgo

Es indispensable recolectar evidencias después de la ocurrencia de eventos de riesgo sobre la seguridad de la información.

5.57. Integridad de material de evidencia

La integridad de todo material de evidencia debe ser protegida. Las copias deben ser supervisadas por personal confiable y se debe registrar la información de cuando y donde fue ejecutado el proceso de copia, quien realizo dicha actividad, y que herramientas y programas se utilizaron.

5.58. Probar debilidades

Se deben probar técnicamente las debilidades del sistema (Ethical Hacking) sin producir mal uso, ni ocasionar daños al mismo o al servicio de información, ni incurrir en responsabilidades legales para quien realiza la prueba.
La gestión de la continuidad del negocio debe incorporarse en los procesos y estructura de la Entidad, asignando la responsabilidad de coordinación de este proceso a la División de Sistemas.

El proceso de continuidad del negocio debe incluir la identificación y priorización de los procesos críticos y el impacto de las interrupciones. Los planes y procesos de continuidad así definidos deben probarse y actualizarse periódicamente.

5.59. Iniciativa para el Plan de Continuidad del Negocio

La Dirección Administrativa o en su ausencia del encargado del área de Sistemas se debe tener la iniciativa para iniciar la ejecución del Plan de Continuidad del Negocio.

5.60. Plan de recuperación de desastres

Los usuarios dueños de cada sistema de información deben asegurarse que disponen de planes de recuperación de desastres, documentados, probados y en funcionamiento.

5.61. Continuidad del negocio y análisis de impactos

Los usuarios dueños de los sistemas de información, conjuntamente con los responsables técnicos de su manejo e identificarán los eventos de riesgo potencialmente causantes de interrupciones a procesos y/o servicios.

5.62. Minimización de impacto de ataques informáticos

Se deben elaborar planes para minimizar los daños por posibles ataques informáticos, los que deberán ser mantenidos y probados periódicamente para asegurar su eficacia y que los tiempos de recuperación sean razonables.

5.63. Activación de los Planes de Continuidad

Cada plan de continuidad del negocio debería especificar claramente las condiciones para su activación, los procedimientos de emergencia a llevar a cabo, los procedimientos de respaldo que permitirán operar, los procedimientos de reanudación en condiciones de normalidad, así como las personas responsables de ejecutar cada etapa del plan.

5.64. Mantenimiento y concientización

Todo plan de continuidad debe tener un calendario de mantenimiento de pruebas del plan, así como prever actividades de concientización y capacitación diseñadas para asegurar que los procesos sean eficaces.

ORIGINAL FIRMADO

MOISES CEPEDA RESTREPO
Gerente General
VALLECAUCANA DE AGUAS S.A. E.S.P.

Elaboró y proyectó: Jesús Migdonio Mosquera – Contratista Técnico en Sistemas
Revisó: Control Interno y Calidad
Aprobó: El Firmante

Anexo

No.	TIPO DE ACTIVO: HARDWARE		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
1	Servidor HP	Marca: HP; ML350 GEN8V2; Serie: MX2416022J		X		1	2	1	B	Cuarto de servidor	Sistemas
2	Servidor IBM	Servidor principal donde se tiene: Carpetas compartidas, backup, MSQL y SIAF.		X		1	2	1	B	Cuarto de servidor	Sistemas
3	UPS	Marca: IBM; Modelo: X3200M3		X		1	2	0	B	Cuarto de servidor	Sistemas
4	UPS	Servidor segundario contiene Orfeo, programa de gestión documental.		X		1	2	0	B	Cuarto de servidor	Sistemas
5	Switch CORE	Marca: QBEX; Modelo: EPS FLOW 6000; Serie: 090515-87390038.- Unidad de poder para los equipos de cómputo.		X		1	2	1	B	Cuarto de servidor	Sistemas
6	Router con el proveedor	Ups bifásica; Marca: TITAN; Modelo: 6KVA		X		1	2	1	B	Cuarto de servidor	Sistemas
7	Firewall Micro TIK	Marca; Modelo: HPV1910-48G; Serie: CN38BX51WT		X		1	2	2	B	Cuarto de servidor	Sistemas
8	Rack	Swith conectividad ubicado en Rack 1.		X		1	2	2	B	Cuarto de servidor	Sistemas

No.	TIPO DE ACTIVO: HARDWARE		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
						Nivel del Criterio					
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Confidencialidad	Integridad	Disponibilidad			
9	Impresora.	RICOH, AFICIO MP2352SP		X		1	1	0	B	1° piso	Administrativa
10	Impresora.	KYOCERA, ECOSYS M3550IDN; Serie LSM6928171		X		1	1	0	B	2° piso	Jurídica
11	Impresora.	KYOCERA, ECOSYS M3550IDN; Serie LSM6928177		X		1	1	0	B	3° piso	Técnica
12	Impresora.	KYOCERA, Modelo: ECOSYS FS-P6021CDN; Serie: LW35104314		X		1	1	0	B	2° piso	Dir. Financiera
13	Impresora.	KYOCERA, Modelo: ECOSYS FS-C2026MFP; Serie: NN32800292		X		1	1	0	B	2° piso	Gerencia
14	Impresora	KYOCERA, Modelo: ECOSYS 4020; Serie: XVK0919705		X		1	1	0	M	1° piso	Sistemas
15	Impresora	KYOCERA; ECOSYS 4200		X		1	1	0	M	1° piso	Gestión documental
16	Impresora	HP; Modelo: LASERJET PRO M402DN; Serie: PHBQF27743		X		1	1	0	B	3° piso	Técnica/Aseguramiento
17	Impresora térmica	Impresora térmica en recepción.		X		1	1	0	B	1° piso	Adtva/recepción
18	Escáner	Marca: FUJITSU / Modelo: FI-6770; Serie: 700129		X		1	1	0	B	1° piso	Gestión documental

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
20	Computador de Torre	Marca: LENOVO; Modelo: H410; Serie:ES07167644 Computador de escritorio con monitor LCD		X		1	1	2	B	Lesly Gandara	Recepción
21	Computador todo en uno	Marca: LENOVO; Modelo: THINKCENTRE E73Z Serie: MJGVHZR. - Computador todo en uno.		X		1	1	2	B	Marisol Piedrahita	Talento Humano
22	Computador de torre	Marca: JANUS; Serie: 11021597063.		X		1	1	2	B	Estefany Rengifo Tulande	Talento Humano
24	Computador todo en uno	Marca: LENOVO; Modelo: C40-05; Serie: P9006T17		X		1	1	2	B	Luis Eduardo Pineda	Administrativa
25	Computador todo en uno	Marca: LENOVO; Modelo: C50-30; Serie: S100KAPJ		X		1	1	2	B	Aura Eliana Segura	Financiera
26	Computador todo en uno	Marca: LENOVO; Modelo: C50-30; Serie: S100KAPY		X		1	1	2	B	Liliana Otero	Financiera
27	Computador todo en uno	Marca: LENOVO; ModeloB540; Serie: VS70184473		X		1	1	2	B	Geovanna Eugenia Perlaza	Financiera

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
						Nivel del Criterio					
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Confidencialidad	Integridad	Disponibilidad			
28	Comp/dor todo en uno	Marca: LENOVO; Modelo: THINKCENTRE E73Z; Serie: S1H048TT		X		1	1	2	B	Jesus	Sistemas
29	Comp/dor todo en uno	Marca: LENOVO; Modelo: C40-05; Serie: P9006T2N		X		1	1	2	B	Sigifredo Ortega	Jurídica
30	Comp/dor todo en uno	Marca: DELL; Modelo: VOSTRO 320; Serie: CN-00F4NM-70163-116-009P		X		1	1	2	B	Sebastián Sánchez	Jurídica
31	Comp/dor todo en uno	Computador de escritorio con monitor LG Flatron E2240S, CPU JANUS		X		1	1	2	B	Héctor Fabio Ruiz	Juridica
32	Comp/dor todo en uno	Marca: LENOVO; Modelo: C50-30; Serie: S100LHW9		X		1	1	2	B	Fanny Bonilla	Financiera
33	Comp/dor todo en uno	Marca: LENOVO; Modelo: THINKCENTRE E73Z		X		1	1	2	B	Carolina García García	Financiera
34	Comp/dor todo en uno	Marca: LENOVO; Modelo: THINKCENTRE E73Z; Serie: SC1002CE6		X		1	1	2	B	Beatriz Hincapié	Técnica
35	Comp/dor todo en uno	Marca: LENOVO; Modelo: B340		X		1	1	2	B	Monica Lopez	Jurídica
36	Computador todo en uno	Marca: HP; Modelo: ELITE DESK 800; Serie: G1 SFMXL3500WZ9		X		1	1	2	B	Diego Calderón	Técnica

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
37	Computador de escritorio	Marca: LENOVO; Modelo: C50-30; Serie: S100LHW8		X		1	1	2	B	Katherine	Técnica
38	Computador de escritorio	Marca: LENOVO; Modelo: THINKCENTRE E73Z; Serie S1002CDG		X		1	1	2	B	Ramiro Carabalí	Técnica
39	Computador de escritorio.	Marca: LENOVO; Modelo:B540; Serie: VS70196837		X		1	1	2	B	Holmes Zúñiga	Técnica
40	Computador de escritorio.	Computador de escritorio con monitor LG Flatron E2240S; Marca: JANUS; Serie: 11030802426		X		1	1	2	B	Martha Lucía Parada	Técnica
41	Computador todo en uno	Marca: LENOVO; Modelo: C50-30; Serie: S100LHW8		X		1	1	2	B	Lucrecia Valencia Figueroa	Técnica
43	Computador todo en uno	Marca: LENOVO; Modelo: C50-30; Serie: S100LHW6		X		1	1	2	B	Andrés Felipe Solórzano	Dir. Jurídico
44	Computador todo en uno	Marca: LENOVO; Modelo: F0BE; Serie: P901ACE1		X		1	1	2	B	Moisés Cepeda	Gerente

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
45	Computador todo en uno	Marca: LENOVO; Modelo: THINKCENTRE E73Z; Serie: S1002CEY		X		1	1	2	B	Marjorie Lizcano	Secretaria Gerencia
46	Computador todo en uno	Marca: LENOVO; Modelo: F0BE; Serie: P901ACF6		X		1	1	2	B	José Edilson Rueda	Dir. Financiera
47	Computador todo en uno	Marca: LENOVO; Modelo: B540; Serie: VS70184443		X		1	1	2	B	Gustavo	Asesor financiera
48	Computador todo en uno	Marca: LENOVO; Modelo: THINKCENTRE E73Z; Serie: S1002CDU		X		1	1	2	B	Jeison Muñoz	Bodega
50	Teléfono alámbrico	Marca: PANASONIC; Modelo: KX-TS500LX; Serie: 2JBKH264200		X		1	1	0	B	José Édison Rueda	Dir. Financiera
51	Enrutador inalámbrico	Marca: LINKSYS ; Modelo: EA7300; Serie: 19T10S0A658785		X		1	1	0	B	José Edison Rueda	Dir. Financiera
52	Terminal de red óptica	Marca: HUAWEI; Modelo: ECHOLIFEHG8010H; Serie: 485754430B37249A		X		1	1	0	B	José Edison Rueda	Dir. Financiera

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
53	Computador de escritorio.	monitor Janus 2213LE; Marca: LENOVO; Modelo: H410; Serie: ES07167436		X		1	1	2	B	Johanna Jordán	Técnica
54	Computador de escritorio.	Monitor LG Flatron W1943C; Marca: JANUS		X		1	1	2	B	Anderson González	Técnica
55	Computador de escritorio	Monitor Janus 2213LE:; Marca: LENOVO; Modelo:H410; Serie: ES07167439		X		1	1	2	B	Diego Vieda	Técnica
56	Computador de escritorio	Monitor Lenovo D185WA; Marca: LENOVO; Modelo: H410; Serie: ES07167441		X		1	1	2	B	Olga Sofia Libreros	Técnica
57	Computador de escritorio	Monitor Lenovo D185WA; Marca: JANUS		X		1	1	2	B	Dayana Moreno	Control interno
58	Computador todo en uno	Marca: LENOVO; Modelo: C50-30; Serie: S100KALG		X		1	1	2	B	Carolina Villareal	Técnica
59	Computador portátil	Marca: TOSHIBA		X		1	1	2	B	Julio Higuera	Técnica
60	DVR grabador digital	Marca: ALHUA		X		1	0	0	B	Casa Sede 2	

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
61	Switch inalámbrico	Marca: TP LINK; Modelo:		X		1	1	1	B	Casa, Sede 2	
62	Router inalámbrico	Marca: CISCO; Modelo: DPC2425; Serie: 227031398		X		1	1	1	B	Casa, Sede 2	
63	Computador todo en uno	Marca: LENOVO; Modelo: B540; Serie: VS70196824		X		1	1	2	B	José Rodrigo Mendoza	Control interno
65	Computador de escritorio.	Computador de escritorio con monitor LG Flatron E2240S; Marca: Janus		X		1	1	2	M	Albeiro Belalcázar	Planeación
66	Computador todo en uno	Marca: LENOVO; Modelo: F0CB; Serie: MP15997R		X		1	1	2	B	Carlos Calderón	Asesor Gobernadora
67	Computador todo en uno	Marca: LENOVO; Modelo: B340; Serie: MJGVHZV		X		1	1	2	B	Juan Fracier Moreno	Planeación
68	Computador de escritorio con	Computador JANUS con monitor LG Flatron E2240S		X		1	1	2	B	Mónica Viviana Arco	Técnica

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
						Nivel del Criterio					
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Confidencialidad	Integridad	Disponibilidad			
69	Computador de escritorio	Computador JANUS con monitor LG Flatron E2240S		X		1	1	2	B	Sonia Soler	Técnica
70	Video beam	Marca: EPSON; Modelo: H723A; Serie: WFBF650151L		X		1	0	0	B	Ing. Miguel	Técnica
71	Video beam	Marca: EPSON; Modelo: H551A; Serie: TTF410074L		X		1	0	0	B	Sistemas	Sistemas
72	Video beam	Marca: EPSON		X		1	0	0	B	Ventanilla Departamental de Proyectos	Planeación Departamental
73	Video beam	Marca: BENQ; Modelo: MW529; Serie: PDY8G02131000		X		1	0	0	B	Gerencia	Gerencia
74	Computador portátil	Marca: LENOVO; Modelo: E40-80; Serie: MP12E0AN		X		1	1	2	B	Andrés Candamil	Técnica
76	Computador portátil	Marca: APPLE; Serie: MACBOOK AIR		X		1	1	2	B	José Edison Rueda	Dir. Financiera

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
77	Dvr grabador digital	Marca: HIKVISION; Modelo: CCTV		X		1	0	0	B	Divier Velásquez	Cuarto Servidor
78	Rack	Rack de comunicaciones		X		1	1	1	B	Divier Velásquez	Cuarto Servidor
79	Dvr grabador digital	Marca: NVRONE; Modelo:		X		1	0	0	B	Divier Velásquez	Cuarto Servidor
80	Dvr grabador digital	Marca: DELL; Modelo: TZ600		X		1	0	0	B	Divier Velásquez	Cuarto Servidor
81	Switch	Marca: HP; Modelo: V1910-48G; Serie: CN38BX51WT		X		1	0	0	B	Divier Velásquez	Cuarto Servidor
82	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Kiosco
83	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Sede parte izquierda
84	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Sede parte derecha

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
85	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Recepción
86	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Área Técnica
87	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Área Financiera
88	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Pasillo acceso Gerencia izquierda
89	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Pasillo acceso Gerencia parte derecha
90	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Pasillo baño mujeres
91	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Sala de Juntas
92	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Entrada Gerencia
93	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Entrada izquierda Gerencia
94	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Posterior inservibles
95	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Casa Primer Piso
96	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Cuarto Racks
97	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Caseta Portería

No.	TIPO DE ACTIVO:		Tipología			Clasificación del activo de información			Estado del Activo	Localización del activo / Responsable	Área/Dependencia
	Nombre del Activo	Descripción del activo de información	Software	Hardware	Servicios	Nivel del Criterio					
						Confidencialidad	Integridad	Disponibilidad			
98	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Cámara 2 Portería
99	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Entrada principal
10	Cámara de vigilancia análoga			X		1	0	0	B	Divier Velásquez	Sede parte derecha
101	Cámara de vigilancia domo			X		1	0	0	B	Divier Velásquez	Pasillo cocina
102	Cámara de vigilancia ojo de pez			X		1	0	0	B	Divier Velásquez	Recepción
103	Cámara de vigilancia ojo de pez			X		1	0	0	B	Divier Velásquez	Talento Humano