VIGENCIA 2025

Código TRD 1000.27.14.001-2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

ENERO 2025

Tabla de contenido

1. OBJETIVO

Establecer los controles o políticas necesarias para asegurar y proteger los activos tecnológicos y de información, por medio del proceso de Gestión Informática, logrando como propósito de controlar los riesgos de seguridad digital, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la Entidad.

1.1. Objetivos Específicos

- Disminuir amenazas de seguridad en los datos y la información de Vallecaucana de Aguas S.A. E.S.P.
- Proteger los activos de información de Vallecaucana de Aguas S.A. E.S.P. con base en los criterios de confidencialidad, integridad y disponibilidad.
- Evitar comportamiento y uso inapropiado de los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P.
- Crear conciencia en la comunidad sobre el uso seguro de los recursos tecnológicos como sistemas de información, infraestructura informática, canales de comunicación y servicios de red de Vallecaucana de Aguas S.A. E.S.P.

2. ALCANCE

El plan de seguridad y privacidad de la información de Vallecaucana de Aguas S.A. E.S.P. será aplicado a los procesos estratégicos, misionales, de apoyo, y control por tal

motivo, deberá ser conocido y cumplido por todas las partes como para funcionarios, contratistas y terceros hagan uso de los servicios tecnológico e informáticos de la entidad, para así asegurar la continuidad de los servicios tecnológicos de la entidad.

3. MARCO CONCEPTUAL PARA LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Adware: Software o código maliciosos no deseados que facilita el envío de contenidos publicitarios.

Aplicaciones: Software que se utiliza para la gestión de la información.

Advertencia: Mensaje que informa al usuario final sobre acciones que podrían causar daños o pérdida de datos en el equipo del usuario o en la red.

Alarma: Señal visual o sonido que se activa al momento de producirse errores en el sistema.

Activo de información: Se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la Entidad (sistemas, soportes, activo físico, hardware, recurso humano).

Amenaza Interna y Externa: Amenaza originada dentro y fuera de la entidad, y causa potencial incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgo proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgo incluye la estimación de riesgo (ISO/IEC 27000).

Antivirus: Software de seguridad que se encarga de proteger un equipo de virus informáticos, generalmente lo hace por medio de detecciones en tiempo real o mediante análisis del sistema.

Virus: Programa escrito para distorsionar o alterar el funcionamiento de la máquina, sin permisos del usuario, se ejecuta por sí mismo poniendo su código en la ruta de ejecución de otro programa instalado en el equipo; se reproduce reemplazando o alterando archivos en el equipo infectado.

Aplicaciones Engañosas: Programas que pretenden engañar al usuario para que tome nuevas acciones encaminadas a descargar malware adicional o recopilar información confidencial.

Arquitectura de Seguridad: Práctica de aplicación de un método riguroso para describir la estructura y el comportamiento de procesos de seguridad de la información de una organización, con el fin de ajustarlos a las necesidades de los usuarios e implementar servicios y niveles de seguridad frente a las posibles amenazas.

Ataques Multietapas: Instrucciones que inicia normalmente con un ataque que instala códigos maliciosos para dañar u obtener información.

Ataques Web: Intrusión a una aplicación alojada en el equipo cliente originada desde un sitio web ya sea desde sitios autorizados o sitios maliciosos creados con el fin de generar daños u obtener información confidencial.

Auditoria: proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditora (ISO/IEC 27000).

Autenticación: Provisión de una garantía de que una característica firmada por una entidad es correcta (ISO/IEC 27000).

Blacklist (Lista Negra): Proceso mediante el cual se identifican y se proponen a bloquear programas, remitentes de correos, direcciones IP, dominios desconocidos o maliciosos.

Bot: Computadora individual infectada con malware que forma parte de una red.

Botnet: es una red de dispositivos infectados con malware que son controlados de forma remota por un ciberdelincuente.

Caballo de Troya (Troyano): es un tipo de malware que se disfraza de un programa legítimo para obtener acceso a la computadora de un usuario. Por lo general, se propagan por correo o mediante la descarga y ejecución de archivos de internet.

Ciberdelito: Delito cometido usando recursos tecnológicos como computadores, redes, hardware y software, el cual puede ocurrir en la computadora o en otros lugares de la red.

Contraseña: Cadena exclusiva de caracteres asignada por el usuario como forma de identificación para acceder a equipos o archivos de forma exclusiva.

Control: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, practicas, entre otras acciones que modifican el riesgo

Control Detective: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige (ISO/IEC 27000).

Control de Acceso: Significa garantizar que el acceso a los activos este autorizado y restringido según los requisitos comerciales y de seguridad (ISO/IEC 27000).

Control Disuasorio: Control que reduce la posibilidad de materialización de una amenaza, por ej: por medio de avisos o de medidas que llevan al atacante a desistir de su intención (ISO/IEC 27000).

Control Preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse (ISO/IEC 27000).

Cuarentena: Forma preventiva de aislamiento de archivos sospechosos y maliciosos, con el fin de que no se puedan abrir ni ejecutar.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpir las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de una manera significativa (ISO/IEC 27000).

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada (ISO/IEC 27000).

Encriptación: Método de cifrado de datos para evitar que los usuarios no autorizados accedan o manipulen la información contenida, solamente los usuarios con contraseña podrán hacerlo. En algunos casos el malware usa una encriptación para ocultarse de los programas de seguridad.

Eventos: Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento a veces puede ser referido como un "incidente" o "accidente" (ISO/IEC 27000).

Filtración de Datos: Evento que compromete un sistema al exponer información a un entorno no confiable; son resultados de ataques maliciosos que buscan obtener información confidencial para usarla con fines malintencionados o delictivos.

Grooming: Un engaño pederasta, más conocido por el anglicismo grooming o ciberacoso es una serie de conductas y acciones emprendidas por adultos, en muchos casos a través de Internet, con el objetivo deliberado de ganarse la amistad de menores de edad.

Identificación de Riesgos: La identificación de riesgos implica la identificación de las fuentes del riesgo, eventos, sus causas y sus posibles consecuencias. La identificación de riesgo puede involucrar datos históricos, análisis teóricos, opiniones informadas y expertos, y las necesidades de las partes interesadas (ISO/IEC 27000).

Incidente de Seguridad de la Información: Evento único o serie de eventos de seguridad de la información inesperada o no deseada que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (ISO/IEC 27000).

Información Documentada: Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida. La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros) (ISO/IEC 27000).

Ingeniería Social: Procedimiento usado con el fin de engañar a los usuarios para ejecutar acciones que no haría normalmente, las cuales tendrán consecuencias negativas, tales como descargas de malware o divulgación de datos confidenciales, la mayoría de los ataques de Phishing se basan en ingeniería social.

Integridad: Propiedad de la información relativa a su exactitud y completitud (ISO/IEC 27000).

Keystrke Logger (Captura de Teclado): Tipo de malware creado para detectar las pulsaciones del teclado, los movimientos y los clics del ratón de forma encubierta, con el fin de obtener ilegalmente información confidencial, cuentas y contraseñas del usuario.

Malware: Programa con efectos malicioso o no deseado, como virus, gusanos, troyanos y puertas traseras. Se propagan usando herramientas comunes como correos, aplicaciones de mensajería y medios magnéticos extraíbles. En su Mayoría busca obtener información confidencial para usarla en acciones delictivas.

Mecanismo de Propagación: Medio usado por las amenazas para infectar sistemas informáticos.

Monitoreo: Determinar l estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente (ISO/IEC 27000).

Negación de Servicio (DoS): Ataques que generan cantidades masivas de peticiones de servicios a una misma maquina o dirección IP, que aumenta el consumo de los

recursos del servicio hasta agotar su capacidad de respuesta lo que se refleja n el rechazo de peticiones, es ahí, donde se materializa la denegación del servicio.

Nivel de Riesgo: Magnitud de un riesgo expresado en relación a la combinación de consecuencias y probabilidades (ISO/IEC 27000).

Objetivo: En el contexto de los sistemas de gestión de seguridad de la información, la organización establece los objetivos de seguridad de la información, de acuerdo con la política de la información para lograr resultados específicos (ISO/IEC 27000).

Objetivo de la revisión: Declaración que describe lo que se debe lograr como resultado de una revisión (ISO/IEC 27000).

Pharming: Forma de ataque que busca redirigir el tráfico de un sitio web hacia un sitio web faso, diseñado para imitar al sitio original; el objetivo de este método es que el usuario ingrese su información personal en el sitio falso para ser obtenida por el cibercriminal.

Phishing: método usado para obtener información confidencial con el fin de ser usad en estafas bancarias y tarjeta de crédito.

Plan de Tratamiento de Riesgos: Documentos que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma (ISO/IEC 27000).

Recursos de Tratamiento de Información: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento (ISO/IEC 27000).

Redes Punto a Punto: Red de informática distribuida en la que parte de los recursos están a disposición de los miembros de la red, sin necesidad de servidores centralizados; son usadas para compartir música, películas, juegos y otros archivos. Sin embargo, son usadas también de forma maliciosa para la distribución de virus, adware, troyanos y otros tipos de malware.

El riesgo informático: es la posibilidad de que los sistemas, redes, aplicaciones y datos de una organización sean atacados por vulnerabilidades o debilidades.

Rootkits: Componente de malware que se mantiene en los equipos de forma anónima e indetectable; realiza procesos de instalaciones sin autorización ni conocimiento del usuario. Estos malware no infectan las maquinas como los virus, solo proveen un ambiente indetectable para la ejecución de códigos maliciosos.

sistema de detección de intrusos (IDS): es una tecnología de seguridad que monitorea la red y los dispositivos conectados a ella para detectar intentos de acceso no autorizados. El IDS envía alertas a un centro de operaciones de seguridad (SOC) que puede tomar medidas para hacer frente a la amenaza.

Sistema de Gestión de Seguridad de la Información: identifica e implementa mecanismos para lograr el cumplimiento de la normatividad y estándares en seguridad de la información ·

Sistemas de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información (ISO/IEC 27000).

Sistema de Prevención de Intrusos: Este sistema por lo general se compone con un dispositivo ya sea Hardware o Software que se encarga de supervisarla actividad de la red en busca de eventos inusuales, no deseados o maliciosos y reacciona en tiempo real bloqueando y evitando este tipo de actividades, también debe ser parte de la estrategia de seguridad de la organización.

Spam: Comúnmente conocido como correo basura, son mensajes prácticamente idénticos enviados a muchos destinatarios; en su mayoría se difunde con el fin de obtener más direcciones de correo electrónico para continuar enviando malware adjuntos y en propagación de los ataques de phishing.

Spyware o Software Espía: Es un paquete de software que hace seguimiento y envío de información confidencial a terceros; buscan datos como detalles bancarios, números

de tarjetas, contraseñas; estos programas por lo general se liberan de forma remota al equipo local.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/IEC 27000).

Ramsonware: es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Definición.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de EVA, con respecto a la protección de los activos de información, que soportan los procesos de la Entidad, y se reconoce que contribuyen a la generación de la memoria institucional y gestión del conocimiento por lo que es necesario avanzar en su Seguridad y Privacidad.

En EVA se debe asegurar e implementar la política, para gestionar el cumplimiento de los objetivos de Seguridad de la Información, como son:

a) Mitigar los riesgos tecnológicos de la entidad
b) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Proteger los activos de información.

g) Fortalecer la cultura de seguridad de la información en los funcionarios y usuarios de los diferentes aplicativos.

h) Cumplir con los principios de Seguridad de la información.

i) Implementar el sistema de gestión de seguridad de la información.

j) garantizar la continuidad de los servicios frente a incidentes de seguridad de la información.

4.1 implementación de políticas de seguridad de la información

Este Plan de Seguridad y Privacidad de la información deberá realizarse para el año 2025.

4.1.1 Descripción de las políticas

Generalidades:

La finalidad de este plan es la de gestionar de forma adecuada los recursos de TI y los sistemas informáticos garantizando 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 Vallecaucana de Aguas S.A. E.S.P.

Entre los temas a tratar están:

5. LINEAMIENTOS ASOCIADOS A LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación

de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

5.1 Responsabilidades

Principios Generales: Todos los directores de cada área y colaboradores de Vallecaucana de Aguas S.A. E.S.P., tienen la responsabilidad de velar por la seguridad de los recursos y los activos tecnológicos de la entidad que se encuentran a su cargo según las instrucciones y recomendaciones entregadas y firmadas por ellos en el Acta de Entrega de dispositivos TI.

Oficina TIC´s: Serán los responsables de la seguridad Informática de Vallecaucana de Aguas S.A. E.S.P., y se encargara de:

- Desarrollar, revisar y actualizar políticas y procedimientos TIC´s.
- Proveer lineamientos funcionales en el ámbito de la seguridad informática de Vallecaucana de Aguas S.A. E.S.P.
- Definir las prioridades de seguridad informática de vallecaucana de aguas S.A. E.S.P.
- Coordinar la ejecución de la políticas y planes de seguridad informática de Vallecaucana de Aguas S.A. E.S.P.
- Asegurar la seguridad de los Activos de TI de Vallecaucana de Aguas S.A. E.S.P.,
- Garantizar la seguridad informática correspondiente en todos los proyectos y trabajos de Vallecaucana de Aguas S.A. E.S.P.

- Definir planes y políticas de accesos para usuarios por la dependencia correspondiente y según el nivel asignado a los datos, la red y sistemas de información necesarias para el desarrollo de sus labores diarias.
- Definir políticas de contraseñas seguras para acceso de los usuarios a la red, las bases de datos y sistemas de información de Vallecaucana de Aguas S.A. E.SP.
- Determinar políticas procedimientos para monitorear y detectar accesos no autorizados, registrar evento que sirvan de soporte en caso de presentarse incidentes relacionados con la seguridad informática.
- Mantener actualizada la documentación de procedimientos de acceso a los recursos tecnológico de Vallecaucana de Aguas S.A: E.S.P., para los terceros autorizados.
- Proporcionar herramientas de protección tales como antivirus.
- Antimalware, antispam, antispyware, ramsonware, que reduzcan el riesgo de propagación de software malicioso y que permitan respaldar la información contenida en los dispositivos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., y los servicio que ejecutan en la red.
- Implantar Procedimientos, responsabilidades y restricciones para el control de la instalación de Software en los equipos de Vallecaucana de Aguas S.A. E.S.P.
- Ejecutar respaldos mediante procesos de copias de seguridad de la información reservada de Vallecaucana de Aguas S.A.E.S.P., cuyo tiempo de vida sea mayor al del medio en el que se encuentra almacenada.
- Efectuar pruebas de hacking ético y vulnerabilidades en periodos de tiempo establecidos por medio de un tercero que cumpla con los estándares para tal fin.
- Originar, aplicar y monitorear planes de acción para disminuir vulnerabilidades técnicas detectadas en la plataforma tecnológica Vallecaucana de aguas S.A: E.S.P.
- Implantar procedimientos, responsabilidades y restricciones para el control del uso de dispositivos móviles conectados a las redes de la Vallecaucana de Aguas.

- Determinar políticas para realización de planes de auditorías internas que evidencien el cumplimiento de las condiciones de Seguridad Informática estipulados por Vallecaucana de Aguas.

Los colaboradores: Son responsabilidades de todos los funcionarios y contratitas (PS= de Vallecaucana de Aguas S.A. E.S.P.:

- Cumplir los planes y procedimientos de seguridad impartidos por Vallecaucana de Aguas S.A. E.S.P., con la indicación de sus responsabilidades de seguridad.
- Conservar de forma confidencial sus contraseñas y credenciales de acceso a los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., para prevenir el acceso de terceros no autorizados a la información almacenada en la red.
- Asegurar los equipos de cómputo asignados y la información allí almacenada.
- Informar el área de sistemas de forma inmediata cualquier sospecha de violación de seguridad o cualquier vulnerabilidad detectada incluyendo sospechas de propagación de contraseñas a terceros.
- Acatar los alineamientos e indicaciones establecidos en este documento.

5.1.2 El Director administrativo y Talento Humano:

Informa al encargado de sistemas toda novedad de personal de nómina o de prestación de servicios, para la creación de usuarios de red, correos institucional y acceso a los recursos de TI de Vallecaucana de Aguas S.A. E.S.P.

De los prestadores de Servicios y Terceros:

- Todo proveedor que proporcione servicios y tenga acceso a los recursos informáticos de Vallecaucana de Aguas S.A. E.S.P., y la información confidencial, deberán apegarse a las disposiciones legales, reglamentos e instrumento normativos relacionados con el acceso a la información pública y protección de datos personales.
- Todo servicio informático otorgado a terceros será monitoreado y revisado por la persona responsable de la supervisión de su contrato, con el fin de asegurar el cumplimiento de los términos estipulados en el mismo.
- Todo dispositivo (Computador) que proporciones servicios en las instalaciones de Vallecaucana de Aguas debe cumplir con las políticas de seguridad en la empresa, usos de redes, equipos con software licenciados, antivirus vigentes.

Implementación: Con el fin de poner en marcha controles de seguridad informática eficaces y efectivos, por medio este manual de seguridad informática se debe:

- Implementar controles de prevención, detección y recuperación.
- Implementar controles complementarios en todos los niveles de seguridad informática, con el fin de no crear dependencia de un solo nivel de control.

- En caso de ser posible y se justifiquen los costos, procurar la automatización de los controles de seguridad informática.

- Simplificar los controles y reducir la complejidad de las herramientas de seguridad para que haya compromiso en todos los niveles jerárquicos de Vallecaucana de Aguas S.A. E.S.P.

5.1.3 Responsabilidad del encargado de sistemas

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
- Verificar el control de la realización de las copias de respaldo de información, así como la prueba periódica de su restauración.
- Gestionar con proveedor contratista de sistemas tercerizado la implementación de los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Proveer el servicio de internet a los funcionarios para trabajar exclusivamente en las tareas asignadas.
- Solicitar al proveedor contratista de sistemas de mantenimiento tercerizado actualizar periódicamente los softwares necesarios en los computadores, parches de seguridad y antivirus.
- Verificar los equipos de terceros que necesiten conectarse a la red informática de la entidad que cumplan con los requisitos mínimos de seguridad para no vulnerar y poner en peligro la red de Vallecaucana de Aguas S.A.E.S.P.
- No compartir o divulgar información de la empresa sin autorización de la directiva de la empresa.

- Bloquear sitios web detectados o identificados como peligrosos y con contenido no autorizadas.
- Evitar la descarga de música, sonidos y videos, así como la descarga e instalación de programas no autorizados.
- Asignar mediante acta o formato de préstamos a los funcionarios los activos informáticos según las necesidades para el desarrollo de sus labores, la persona a la que se le asigne el activo será el único responsable del equipo y de la información contienda.
- El proveedor contratista de sistemas de mantenimiento tercerizado de los computadores se encuentra autorizado para hacer reparaciones y cambios en los activos informáticos.

5.1.4 Responsabilidades de los funcionarios

- Entregar la información almacenada en dispositivos personales que sean utilizados por él, proveedores y contratistas para adelantar sus funciones en EVA, teniendo en cuenta que la información almacenada, procesada y generada a través de estos medios, se considera propiedad de la Entidad y el uso inadecuado de estos puede conllevar a las sanciones disciplinarias y legales correspondientes.

- Los funcionarios, contratistas y proveedores de la EVA tienen la obligación de conocer y cumplir lo establecido en la "Política de Seguridad y Privacidad de la Información" y propender por la integridad, disponibilidad y confidencialidad de esta, so pena que la Entidad tome las medidas disciplinarias, legales y administrativas correspondientes.

- Los funcionarios, y directores de áreas se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la Entidad, tales como escritorios remotos y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros. Los dispositivos móviles de propiedad de la Entidad son de estricto uso para el cumplimiento de la misionalidad de la misma y por ende se deben gestionar desde la Dirección Administrativa de EVA.

- Los funcionarios o contratistas de la EVA deben almacenar la información de la entidad únicamente en los medios designados por la Entidad, tales como: servidor de archivos, almacenamiento en la nube, medios magnéticos, entre otros. Una vez finalizada la vinculación con la Dirección, se deberá entregar toda la información procesada dentro de los equipos a cargo, al jefe inmediato o al supervisor del contrato y hacer entrega del inventario correspondiente al jefe inmediato.

- Todos los funcionarios y contratistas de EVA son responsables de hacer un uso adecuado del internet y cumplir con las políticas para tal fin.

- Los funcionarios deben adelantar los procesos correspondientes para retirar de las sedes de la EVA, dispositivos informáticos o que contengan información de la Entidad, contando con los vistos buenos de los responsables de la misma y los jefes inmediatos correspondientes.
- Los funcionarios y contratistas de la EVA son responsables de hacer un uso adecuado del internet y cumplir con las políticas para tal fin.

5.2 POLÍTICA PARA EL CONTROL DE ACCESO

5.2.1 Consideraciones generales

- El líder de seguridad de la información en el caso de un tercero que preste el soporte técnico como el proveedor contratista de sistemas deben definir la gestión de accesos a todos los sistemas, bases de datos y servicios de información de EVA incluyendo accesos a internet, el uso de computación móvil, teletrabajo y trabajo remoto.
- El líder de seguridad de la información debe verificar el cumplimiento de las pautas establecidas relacionadas con control de accesos, registro de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios.
- Es responsabilidad del líder de seguridad de la información gestionar campañas de concientización al personal sobre el uso apropiado de usuarios y contraseñas.

5.2.2 Administración de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, para lo cual deben cumplir, como mínimo, los siguientes lineamientos:

- Mantener las contraseñas en secreto.
- Pedir o generar el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- Seleccionar contraseñas de calidad, de acuerdo con las recomendaciones del proveedor contratista de sistemas tercerizado y en cumplimiento de los siguientes parámetros:

  - Sean fáciles de recordar.

- Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar contraseñas antiguas.
- Cambiar la contraseña provisional definida para el primer inicio de sesión.
- Notificar cualquier incidente y /o evento de seguridad relacionado con sus contraseñas, tal como pérdida o indicio de pérdida de confidencialidad.
- No deben estar basadas en algún dato personal que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona.
- Las "claves" de usuario deben ser alfanumérica, contener caracteres especiales y una longitud no menor a 08 (ocho) caracteres, sin utilizar espacios en blanco. Deben contener tanto caracteres alfabéticos como numéricos, y al menos 4 (cuatro) caracteres distintos entre sí.

5.2.3 Acceso a la red

- Únicamente se debe proporcionar a los funcionarios o contratistas el acceso a los servicios para los que específicamente se les haya autorizado su uso.
- Se deben utilizar métodos apropiados de autenticación para el control de acceso a los usuarios remotos.
- Se deben implantar controles adicionales para el acceso por redes inalámbricas.
- Se debe establecer una adecuada segregación de redes, separando los entornos de red de usuarios y los servicios.

- El líder de recursos informáticos debe asignar un código único a los equipos a los funcionarios que ejercen sus labores, y cuyos privilegios de acceso a los recursos informáticos, equipos tecnológicos estarán determinados por el tiempo de vinculación la empresa y así de esta manera poder mantener el control de acceso a dichos recursos.

- Los funcionarios y contratistas deben realizar el cambio de las claves de acceso a los recursos de red al ser entregada por primera vez por medio de la aplicación a la cual va a acceder y pertenece el usuario con el fin de mantener la privacidad de la información.
- Los funcionarios y contratistas deben asegurarse que los usuarios y contraseñas no deben ser compartidos con el fin de mantener la privacidad de la información.
- Los funcionarios y contratistas que ejercen funciones públicas deben cambiar la contraseña de su(s) cuenta(s) en el sistema de información cada 60 días y ésta no puede coincidir con las cinco (5) anteriores.

5.3 GESTIÓN DE ACTIVOS

5.3.1. Responsabilidades generales

- Es responsabilidad del líder de sistemas el inventariar, clasificar, documentar y mantener actualizada la información a su cargo de acuerdo con su grado de sensibilidad y criticidad, así como definir los permisos de acceso a la misma.

- El líder de la seguridad de la información debe asegurar que los lineamientos para la utilización de los recursos de la tecnología de la información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan. Los controles y riesgos definidos para cada caso.

5.3.2. Inventario de activos

- Es responsabilidad del líder de sistemas, identificar los activos de información asociados a cada sistema de información, sus respectivos propietarios y su ubicación.

- Es responsabilidad del líder, el mantener actualizado el inventario de activos de información, el cual debe ser revisado con una periodicidad no mayor a un (1) año y actualizado cada vez que se requiera el ingreso de nuevos registros.

5.3.3. Clasificación de la información

Solo el propietario de la información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:
- Asignarle una fecha de efectividad.
- Comunicárselo al custodio del recurso.
- Realizar los cambios necesarios para que los usuarios conozcan la nueva clasificación.

5.4 SEGURIDAD FÍSICA Y DEL ENTORNO

5.4.1. Responsabilidades generales

- Es responsabilidad del funcionario y/o directores de área autorizar formalmente el trabajo fuera de las instalaciones con información de sus trabajos.

- Todo el personal de la EVA es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

- El uso inadecuado de los recursos tecnológicos o incumplimiento a alguna de las presentes políticas dará lugar en primera instancia a llamado de atención por parte del director Administrativo de EVA.

- El líder de sistemas de información es el encargado de revisar que el centro de procesamiento de datos y cuarto de equipos de TIC, deben de estar protegidos físicamente contra el acceso no autorizado, daño o interferencia.

- Todo equipo portátil, cámara fotográfica, USB propiedad de terceros contratistas y/o visitantes, deberá ser registrado en la entrada por la vigilancia contratada (recepción), así mismo deberá ser inspeccionado su contenido, si el mismo va a hacer conectado a la red de la EVA.

5.5 SEGURIDAD DE LAS OPERACIONES

5.5.1 Controles contra software malicioso

- El líder de sistemas debe definir controles de detección y prevención para la protección contra software malicioso.

- Es responsabilidad del proveedor contratista tercerizado del mantenimiento de los equipos y líder de sistemas gestionar la implementación de los controles contra software malicioso o solución informática equivalente.

- El manejo de la aplicación de antivirus - antimalware corporativo para estaciones de trabajo y servidores (instalación, configuración, administración y/o desinstalación)

debe ser realizado únicamente por el líder de sistemas o por el proveedor contratista tercerizado del mantenimiento de EVA.

- Todos los equipos informáticos de funcionarios, proveedores o terceros que sean autorizados para conectarse a la red de la empresa EVA deben contar con una aplicación de antivirus - antimalware con su base de datos actualizada.

5.5.2 Copias de respaldo y restauración de la información

Es responsable de líder de sistemas de información:

- Disponer y revisar la realización de copias de respaldo de la información, así como asegurar que se realicen pruebas periódicas de su restauración.
- Designar al proveedor contratista tercerizado del mantenimiento de sistemas para la administración y gestión de una solución de almacenamiento de información centralizada como implementación del servidor espejo con las condiciones necesarias de seguridad de información.
- Implementar controles documentados para la administración de medios informáticos removibles (USB, discos externos, cintas entre otros).
- Definir procedimientos para la eliminación segura de los medios de información que se necesiten eliminar, como es el caso de CD, DVD, blue ray, cintas magnéticas, discos duros o cualquier dispositivo que pueda tener información de la Entidad.

5.5.3 Registro de actividades y fallas

Es responsabilidad del líder de sistemas:

- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Asegurar el registro de las actividades realizadas en los sistemas, como parte de un incidente de seguridad de la información, incluyendo según corresponda:

- Errores del sistema y medidas correctivas tomadas.
- Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
- Ejecución de operaciones críticas.
- Cambios a información crítica.

5.6 SEGURIDAD DE LAS COMUNICACIONES

5.6.1 Responsabilidades generales

- El líder de seguridad de la información debe definir controles para garantizar la seguridad de los datos y los servicios conectados en las redes de EVA contra el acceso no autorizado.

- Salvo expresa autorización, ningún usuario está autorizado para, acceder o manipular directa o indirectamente los sistemas de información y de comunicaciones de la red de datos de EVA, e instalar nuevos sistemas de comunicaciones de redes que se conecten con la red de datos de la Institución.

5.6.2 Correo Electrónico y almacenamiento en la nube

- El líder de seguridad de la información debe definir y documentar el uso del correo electrónico que incluya los siguientes aspectos:

- El alcance del uso del correo electrónico y el almacenamiento en la por parte del personal de EVA.
- Protección contra ataques al correo electrónico e información en la nube, por ejemplo, virus, interceptación, entre otros.
- Protección de archivos adjuntos de correo electrónico.
- Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
- Aspectos operativos para garantizar el correcto funcionamiento del servicio.
- Es potestad de la Entidad, auditar los mensajes recibidos o emitidos por los funcionarios y contratistas, lo cual se incluirá en el "Compromiso de Confidencialidad".

- Los usuarios de correo electrónico no están autorizados a enviar información en forma masiva a múltiples direcciones de correo electrónico.
- Ningún usuario de correo electrónico debe modificar, falsificar o eliminar cualquier información que aparezca en cualquier lugar de un mensaje de correo electrónico, incluyendo el cuerpo del mensaje o encabezado.
- Ningún empleado puede usar cuentas gratuitas de correo electrónico en internet para el envío de mensajes corporativos de la Entidad. Todos los mensajes de carácter corporativo deberán ser enviados a través del sistema de correo electrónico corporativo o correo autorizado como medio alterno.
- Salvo que exista una autorización, ningún funcionario o contratista está autorizado para interceptar, revelar o contribuir en la interceptación de mensajes de correo electrónico a través de herramientas de escaneo.
- Los usuarios del servicio del correo electrónico de EVA no deben contestar mensajes spam.

- Ningún usuario del servicio de correo electrónico debe prestar atención a mensajes con falsos contenidos de virus, ofertas de premios, dinero, solicitudes de ayuda caritativa, venta de bienes (hardware o software) o financiamiento a muy bajo costo, productos medicinales, acceso gratuito a portales, advertencia de virus de fuentes desconocidas, entre otros.
- Para todos los funcionarios o usuarios del servicio de correo electrónico, está prohibido brindar servicios que, de manera directa o indirecta, faciliten la proliferación de spam, en esto se incluye casillas de correo, software para realizar spam, hosting de sitios de Web para realizar spam o que realicen spam, o bien que realicen bromas de mal gusto y/o fraudes, estos últimos definidos como un correo electrónico que atrae el interés del usuario y que esconde una maniobra deshonesta y brindar servicios que, de manera directa o indirecta, faciliten la proliferación de software malicioso o malware, software espía, spyware o phishing.
- A los usuarios que de acuerdo con sus funciones requieran una cuenta de correo, esta se les asignará en el servidor una vez sean vinculados.
- El buzón de correo es personal e intransferible y corresponde al funcionario o contratista velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico.

5.6.3 Conexiones a internet

- El proveedor contratista de sistemas es el responsable de revisar regularmente todos los logs y archivos de auditoría de la actividad en línea de los usuarios de internet. Esta información se considera reservada.
- Es responsabilidad del proveedor contratista de sistemas tercerizado, evaluar e implementar las nuevas herramientas tanto de software como de hardware para que la conexión a internet sea lo más eficaz, eficiente y segura posible.

- El uso de internet debe estar destinado exclusivamente a la ejecución de las actividades de la Entidad y deben ser utilizados por el usuario para realizar las funciones establecidas para su cargo.
- El usuario debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos y la utilización de los recursos para distribución o reproducción de este tipo de material, ya sea vía web o medios magnéticos.
- Queda prohibida la descarga o carga de música y videos excepto para los grupos definidos por el líder de seguridad de la información y que necesiten de este tipo de acciones para la ejecución de las funciones de su cargo (Área de Comunicaciones Estratégicas).
- Abstenerse de usar sitios que salten la seguridad del servidor de acceso a internet (proxy).
- Evitar coleccionar, almacenar, difundir, transmitir, solicitar, inducir o incitar en cualquier forma actos ilegales, inmorales, engañosos y/o fraudulentos es una responsabilidad de los usuarios de la Entidad; así como también amenazas, abusos, difamaciones, injurias, calumnias, escándalos, actos obscenos, pornográficos, profanos, racistas, discriminatorios, actos que invadan la privacidad de los demás u otro tipo de materias, informaciones, mensajes o comunicaciones de carácter ofensivo.

5.6.4 Carga y descarga de archivos

- El líder de sistemas y el proveedor contratista de sistemas de EVA están autorizados para realizar una evaluación de virus a los archivos descargados por medio de internet.
- Los usuarios deben cumplir los requerimientos de licencia y las restricciones de copia asociadas con cualquier archivo descargado.

- El personal técnico del EVA en el caso de un tercero que preste el soporte técnico, tendrá los permisos para instalar los archivos (ejecutables) absolutamente necesarios para las funciones de la entidad.

ORIGINAL FIRMADO

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

Elaboró y proyectó: Jesús Migdonio Mosquera Mena, CPS Sistemas de Información.
Revisó: Dr. Luís Eduardo Pineda – Director Jurídico.
Aprobó: Dr. Sebastián Sánchez – Director Administrativo.
Copia: Archivo.