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

PDA
PLAN DEPARTAMENTAL DE AGUAS
VALLE DEL CAUCA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 3.0

Vallecaucana de Aguas S.A E.S.P.
Seguridad y Privacidad de la Información
Enero 2021

Contenido

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

PDA
PLAN DEPARTAMENTAL DE AGUA
VALLE DEL CAUCA

CONTROL DE CAMBIO

VERSIÓN	FECHA	CAMBIO REALIZADO
1.0	Enero 2019	Inicio
1.1	Enero 2020	Actualización
1.2	Enero 2021	Actualización

1. OBJETIVO

Procurar ofrecer servicios tecnológicos y de comunicaciones de calidad, confiables, íntegras, garantizando su disponibilidad y eficiencia, optimizándolos para asegurarnos que funcionen correctamente bajo parámetros de seguridad óptimos que permitan:

- Disminuir amenazas de seguridad en los datos y la información de Vallecaucana de Aguas S.A. E.S.P.
- Evitar comportamiento y uso inapropiado de los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P.
- Proteger y cuidar 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

Los lineamientos del presente documento de seguridad informática de Vallecaucana de Aguas S.A. E.S.P., aplican para funcionarios, contratistas y terceros no vinculados directamente a Vallecaucana de Aguas S.A. E.S.P., pero que presten su servicio y usen los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., y también para los equipos de funcionarios, contratistas y terceros no vinculados que se conecten a la red de Vallecaucana de Aguas S.A. E.S.P.

La revisión de este manual, tanto como sus objetivos, debe hacerse anualmente, o cuando se realicen cambios en Vallecaucana de Aguas S.A. E.S.P., que afecten los servicios de la empresa, o durante las revisiones periódicas ejecutadas para asegurar la continuidad de los servicios tecnológicos de la entidad.

3. RESPONSABILIDADES

Principios Generales: Todos los secretarios, Jefes de Oficina 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 de TI.

A continuación, se definen responsabilidades puntuales para la operación, administración y control de los planes de seguridad informática.

Oficina TIC's: Serán los responsables de la Seguridad Informática de Vallecaucana de Aguas S.A. E.S.P., y se encargará 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 las 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 trabajaos de Vallecaucana de Aguas S.A. E.S.P.
- Definir planes y políticas de acceso para usuarios autorizados por la dependencia correspondiente y según el nivel asignado a los datos, la red y sistemas de información necesarios 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.S.P.

- Determinar políticas procedimientos para monitorear y detectar accesos no autorizados, registrar eventos que sirvan de soporte en caso de presentarse incidentes relacionados con la seguridad informática.
- Mantener actualizada la documentación de procedimientos de accesos a los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., para los terceros autorizados.
- Proporcionar herramientas de protección tales como antivirus,
- Antimalware, antispam, antispyware, 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 servicios que se 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.

Los Colaboradores: Son responsabilidades de todos los funcionarios y contratistas (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 las indicaciones 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 al 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 lineamientos e indicaciones establecidos en este documento.

El director administrativo, Talento Humano y Oficina de Contratación:

Informar al encargado de sistemas toda novedad de personal de nómina o de prestación de servicios, para la creación de usuarios de red 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 instrumentos 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.

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.

4. DEFINICIONES

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

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: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización (ISO/IEC 27000).

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000).

Amenaza Externa: Amenaza originada fuera de la organización.

Amenaza Interna: Amenaza originada dentro de la organización.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos (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, pone en cuarentena o elimina los virus según lo indique el usuario. Tener un antivirus actualizado es parte de las estrategias de seguridad.

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: Practica 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: Intrusiones que inicial 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.

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

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

Blacklist (Lista Negra): Proceso mediante el cual se identifican y se proceden 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: Red de bots bajo el control de un bot maestro por medio de un canal de control. Dichos equipos se distribuyen por medio de internet y se usan para actividades mal intencionadas como envío de paquetes maliciosos o ataques distribuidos de denegación de servicio. Se crean al infectar varias computadoras con malware para dar acceso al atacante a dichas máquinas. En la mayoría de los casos, los propietarios ignorar que sus máquinas son parte de esta red pues no cuentan con software de seguridad actualizados.

Caballo de Troya (Troyano): Tipo de código malicioso que no infecta archivo ni se propaga automáticamente, al activarse causan pérdida o robo de información; generalmente tiene códigos de puertas traseras que permiten al atacante controlar o descargar amenazas adicionales en el equipo infectado. Por lo general, se propagan por correo o mediante la descarga y ejecución de archivos de internet enviados al usuario después de utilizar ingeniería social para convencer al usuario de ejecutarlos.

Certificado: Sistema criptográfico usado como prueba de identidad, contiene el nombre del usuario y su clave pública.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este

tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo (ISO/IEC 27000).

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.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados (ISO/IEC 27000).

Contraseña: Cadena exclusiva de caracteres asignada por el usuario como forma de identificación para acceder a equipos o archivos de forma exclusiva. El sistema comparará el código introducido con la lista de usuarios autorizados, en caso de ser correcto, se permitirá el acceso en el nivel de seguridad autorizado para el propietario de la contraseña.

Control: Media por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardar o contramedida son utilizados frecuentemente como sinónimos de control (ISO/IEC 27000).

Control Correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige (ISO/IEC 27000).

Control Detectivo: 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 esté 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, p.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 interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa (ISO/IEC 27000).

Directiva o Directriz: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas (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 usuarios no autorizados accedan o manipulen la información contenida, solamente los usuarios con contraseña podrán hacerlo. En algunos casos el malware usa encriptación para ocultarse de los programas de seguridad.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede ser una o más ocurrencias y puede tener varias causas. Un evento puede consistir en que algo no suceda. Un evento a veces puede ser referido como un "incidente" o "accidente" (ISO/IEC 27000).

Evento de Seguridad de la Información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad (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: Nueva forma de abuso y acoso hacia menores de edad que se ha venido presentando con la expansión de la tecnología, se presenta principalmente en redes sociales y chats; inicia con una sencilla conversación en la que un adulto se hace pasar por otro menor para ganar su confianza y empezar intercambios de fotos e imágenes a través de la cámara web.

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 riesgos puede involucrar datos históricos, análisis teóricos, opiniones informadas y de 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 que ejecutar acciones que no harían 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).

Keystroke 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 maliciosos o no deseados, como virus, gusanos, troyanos y puertas traseras. Se propagan usando herramientas comunes como correo, 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 el 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 servicio a una misma máquina o dirección IP, que aumenta el consumo de los recursos del servicio hasta agotar su capacidad de respuesta lo que se refleja en 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 su probabilidad (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 seguridad de la información, para lograr resultados específicos (ISO/IEC 27000).

Objetivo de Control: Declaración que describe lo que se debe lograr como resultado de la implementación de los controles (ISO/IEC 27000).

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

Parte Interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad (ISO/IEC 27000).

Pharming: Forma de ataque que busca redirigir el tráfico de un sitio web hacia un sitio web falso, 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 usada en estafas bancarias y de tarjetas de crédito.

Plan de Tratamiento de Riesgos: Documento 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 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.

Riesgo: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización (ISO/IEC 27000).

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo. El riesgo residual puede contener un riesgo no identificado. El riesgo residual también puede denominarse "riesgo retenido" (ISO/IEC 27000).

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 máquinas como los virus, solo proveen un ambiente indetectable para la ejecución de los códigos maliciosos.

Sistema de Detección de Intrusos: Servicio de monitoreo y análisis de los eventos presentados en los sistemas informáticos, con los cuales se busca encontrar y proporcionar advertencias en tiempo real de intentos de acceso no autorizados a los recursos; esta revisión se hace por medio del registro de eventos y toda información disponible en la red, este sistema de detección debe estar incluido en la estrategia de seguridad de la organización.

Sistema de Gestión de Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una

organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua (ISO/IEC 27000).

Sistema 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 supervisar la 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 difunden con el fin de obtener más direcciones de correo electrónico para continuar enviando malware adjuntos y en propagación de 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 y contraseñas; estos programas por lo general se liberan de forma remota al equipo local.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad (ISO/IEC 27000).

Virus: Programa escrito para distorsionar o alterar el funcionamiento de la máquina, sin conocimiento ni 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 remplazando o alterando archivos en el equipo infectado, se puede propagar en equipos de escritorio y servidores de la red; algunos están programados para operar de forma secreta con el fin de robar información y usarla con fines delictivos.

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

5. LINEAMIENTOS DEL MANUAL DE SEGURIDAD INFORMÁTICA

Los lineamientos contenidos en este manual se publican con el fin de gestionar de forma adecuada los recursos de TI y los sistemas informáticos de Vallecaucana de Aguas S.A. E.S.P.

BUEN USO

De los activos tecnológicos: Entregados por la persona encargado de sistemas de Vallecaucana de Aguas S.A. E.S.P.; los cuales son:

- Computadores de escritorio y portátiles.
- Impresoras.
- Escáneres.
- Proyectores.
- Accesorios para reuniones virtuale

Todo esto de propiedad de Vallecaucana de Aguas S.A. E.S.P.

El encargado de sistemas, asignará mediante acta a los colaboradores y a las áreas los activos informáticos según las necesidades para el desarrollo de sus labores y funciones, la persona a la que se le asigne el activo será el único responsable del uso y de la información contenida en el dispositivo, por lo que, debe evitar compartirlos; en caso de requerir uso compartido, debe ser solamente para cuestiones de índole laboral y mantenerlo bajo su supervisión.

Los computadores portátiles y de escritorio se entregarán con el software necesario para su funcionamiento y para el cumplimiento de las labores asignadas.

Cada vez que el funcionario requiera mover el activo dentro o fuera de las instalaciones de Vallecaucana de Aguas S.A. E.S.P., será responsabilidad del tenedor asignado mediante acta del encargado de sistemas; en caso de presentarse algún incidente que afecte de forma directa un activo informático de Vallecaucana de Aguas S.A. E.S.P., como robo, pérdida o daño físico, debe ser notificado de inmediato al encargado de sistemas para recibir las indicaciones de los pasos a seguir.

Únicamente el encargado de sismas o proveedor contratista de mantenimiento de los computadores se encuentra autorizado para hacer reparaciones y cambios en los activos informáticos de Vallecaucana de Aguas S.A. E.S.P.

El encargado de sismas o proveedor contratado de mantenimiento actualizará periódicamente los sistemas operativos, parches de seguridad, antivirus y aplicaciones instaladas en los computadores y activos informáticos de Vallecaucana de Aguas S.A. E.S.P., para lo cual se hará necesario la colaboración del usuario reiniciando los equipos para la aplicación de dichas actualizaciones.

Todos los activos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., estarán incluidos dentro del dominio establecido para la organización y se les aplicarán las políticas de seguridad definidas por el encargado de sistemas, tales como: fondo de pantalla institucional, acceso a la información según perfil y cargo, bloqueo de las configuraciones del sistema, entre otros. Los equipos de terceros que necesiten conectarse a la red informática de Vallecaucana de Aguas S.A. E.S.P., serán evaluados por el encargado de sistemas para verificar que cumplan con los requisitos mínimos de seguridad para no vulnerar ni poner en peligro la red de Vallecaucana de Aguas S.A. E.S.P.

Del Internet: El encargado de sistemas, proveerá el servicio a los colaboradores de Vallecaucana de Aguas S.A. E.S.P., para trabajar exclusivamente en las tareas asignadas al cargo de forma eficiente y austera.

No revelar información relevante de Vallecaucana de Aguas S.A. E.S.P., sin importar su formato (Excel, Word, PDF, Power Point, mp3, AVI, mp4 o algún otro formato actual o nuevo) ni su nivel de clasificación de confidencialidad en sitios web no permitidos por la Vallecaucana de Aguas S.A. E.S.P., discos duros, discos extraíbles, carpetas virtuales, la nube o sistemas de publicación de información no permitido dentro y fuera de la organización.

Evitar el uso de aplicaciones cuyo fin sea evadir controles implementados Vallecaucana de Aguas S.A. E.S.P.

La navegación en sitios web con contenidos inapropiados está restringida en la red de Vallecaucana de Aguas S.A. E.S.P.; en caso de ser necesario y según la naturaleza del cargo requieran acceso a sitios de contenido controlado, se solicitará a la oficina de las TIC's para su justificación y posterior aprobación del jefe inmediato.

Evitar la descarga de fotografías, música, sonidos y vídeos, así como la descarga de archivos e instalación de programas no autorizados desde sitios web gratuitos o desconocidos, ya que la puede generar saturación en el canal de comunicaciones o incurrir en piratería al instalar software no licenciado.

El encargado de sistemas se reserva el derecho a bloquear sitios web detectados o identificados como peligrosos y con contenidos no autorizadas, en pro de velar por la seguridad de los activos informáticos de Vallecaucana de Aguas S.A. E.S.P.

Cada usuario es responsable de dar un manejo adecuado a las credenciales de autenticación al momento de ingresar a los diferentes componentes del sistema de información de Vallecaucana de Aguas S.A. E.S.P.

Del Correo Electrónico: El correo institucional es para uso exclusivo de los funcionarios activos y dependencias de Vallecaucana de Aguas S.A. E.S.P., y sus sistemas de

información, por lo tanto, únicamente se usará para el ejercicio de las actividades relacionadas a sus funciones.

6. DERECHOS DE AUTOR

Está prohibida, la inspección, búsqueda, copiado y almacenamiento de software y otras fuentes que violen la ley de derechos de autor, por lo cual, todos los funcionarios deben estar comprometidos a no usar ningún tipo de estos programas que violen la ley de derechos de autor y que no estén licenciados por Vallecaucana de Aguas S.A. E.S.P.

Con el fin de evitar y asegurarse de no incurrir en violación de derechos de autor, no se permite a los funcionarios y colaboradores de Vallecaucana de Aguas S.A. E.S.P., copiar ningún programa instalado en los activos tecnológicos de la entidad bajos ninguna circunstancia sin autorización escrita de el encargado de sistemas; así como tampoco está permitido la instalación de ningún programa en los equipos sin dicha autorización o la verificación de que la entidad posee una licencia que cubre esa instalación.

- No se autoriza la descarga de internet Software que no esté previamente revisado y autorizado por el encargado de sistemas, en caso de ser necesario, debe solicitarse al encargado de sistemas la validación de dicho programa.
- No se permiten las copias no autorizadas de programas informáticos, bases de datos o cualquier tipo de información Vallecaucana de Aguas S.A. E.S.P., por parte de ningún funcionario o contratista.
- No se permite que los funcionarios carguen o descarguen programas no autorizados a internet para el uso de sistemas Peer-to-peer (P2P) los cuales pueden ser usados en la comercialización de trabajos protegidos por los derechos de autor.
- Se prohíbe el intercambio o descarga de archivos digitales de música (MP3, MP4, AVI, WAV, etc.) por parte de los funcionarios de Vallecaucana de Aguas S.A. E.S.P., si no son los autores o no tienen los derechos de distribución de esos archivos.
- En caso de evidenciar que algún funcionario o contratista de Vallecaucana de Aguas S.A. E.S.P., ha hecho alguna copia de programas informáticos o música de forma ilegal, la oficina de las TIC's le comunicará al jefe inmediato o supervisor del contrato, para que se tomen las medidas necesarias.

- En caso de evidenciar que algún funcionario o contratista de Vallecaucana de Aguas S.A. E.S.P., ha hecho alguna copia de bases de datos, sistemas de información o cualquier archivo propiedad de la institución de forma ilegal para ser entregado a un tercero, la oficina de las TIC's le comunicará al jefe inmediato o supervisor del contrato, para que se tomen las medidas necesarias.
- Las licencias que provee Vallecaucana de Aguas S.A. E.S.P., son para el desempeño de sus labores y no podrán ser cedidas, vendidas o alquiladas.
- El encargado de sistemas de Vallecaucana de Aguas S.A. E.S.P., hará revisiones periódicas en los activos informáticos con el fin de determinar que los funcionarios estén usando las aplicaciones licenciadas instaladas en los equipos. En caso de encontrar programas no licenciados, licencias gratuitas o no autorizados, dichas aplicaciones serán eliminadas y si son necesarias, se reemplazarán por los programas con licencias que cuenta Vallecaucana de Aguas S.A. E.S.P.
- Los funcionarios usarán los programas instalados según los acuerdos de licencias y no podrán instalar copias no autorizadas de programas informáticos comerciales.
- Según las leyes vigentes de derechos de autor, los funcionarios involucrados en la reproducción ilegal de software pueden estar sujetos a sanciones civiles y penales que incluyen multas y prisión; no está permitida la duplicación ilegal de cualquier programa informático.
- Los funcionarios que hagan, adquieran o usen copias ilegales no autorizadas de software estarán sujetos a sanciones disciplinarias internas según las circunstancias; estas sanciones podrán incluir desde suspensiones hasta despidos justificados.

7. CONTROL DE ACCESOS

Gestión de acceso de usuarios para bases de datos, sistemas de información, red y correo electrónico, toda solicitud de creación de usuario para acceder a los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., será hecha formalmente a través del formato destinado para tal fin.

Creación de Usuarios en Bases de Datos y Sistemas de Información: Toda solicitud de creación de usuarios en bases de datos debe ser aprobada por el jefe inmediato de la persona solicitante.

Creación de usuarios de Red: El encargado de sistemas establece el procedimiento de solicitud a través del formato en donde se especificará la creación, modificación o eliminación de usuarios del directorio activo de Vallecaucana de Aguas S.A. E.S.P.

El sistema de administración de contraseñas para los usuarios de red, correo, bases de datos y sistemas de información de Vallecaucana de Aguas S.A. E.S.P., deben cumplir como mínimo con los siguientes lineamientos de seguridad:

- El uso de las credenciales de acceso individuales (usuario y contraseña) son obligatorias con el fin de determinar responsabilidades.
- Los usuarios deben seleccionar y cambiar sus contraseñas una vez cumplido el plazo mínimo de expiración o a voluntad cuando consideren que ha sido comprometida la seguridad en la cuenta.
- Los usuarios deben cambiar las contraseñas temporales, asignadas al momento de crear la cuenta por el administrador del sistema de información.
- No compartir las contraseñas con los demás usuarios de la red.
- La longitud mínima de la contraseña debe ser de ocho (8) caracteres, debe incluir números, mayúsculas, minúsculas y un símbolo (*, /, -, +, &, etc.).

Uso, Creación y Eliminación de Usuarios: El administrador de los sistemas de Vallecaucana de Aguas S.A. E.S.P., es el encargado de crear, modificar o eliminar usuarios en los diferentes sistemas de información.

El buen uso y la administración de las credenciales asignadas será responsabilidad de cada usuario y deben estar regidas por la política de contraseñas seguras de la entidad, los casos para solicitar al encargado de sistemas el cambio o actualización de las contraseñas de las credenciales de accesos cualesquiera de los sistemas de información, son:

- Cumplimiento del periodo de vida establecido por el encargado según la política definida en el Directorio Activo.
- Cambio de contraseña decido por el usuario.
- Cambio por olvido, pérdida o sospecha de que su contraseña anterior fue comprometida o compartida sin su autorización.
- Cambio de contraseña temporal asignada por el administrador de sistemas.
- El único responsable de iniciar un procedimiento de cambio de contraseña, será el usuario dueño de la cuenta o en casos de olvido el administrador del encargado de sistemas de Vallecaucana de Aguas S.A. E.S.P.

El encargado de los sistemas de Vallecaucana de Aguas S.A. E.S.P., establece que todos los usuarios incluidos los administradores de sistemas, tendrán un identificador único para su uso personal de forma exclusiva, con el fin de garantizar la confiabilidad y trazabilidad de los procesos y de la información manejada por cada uno.

Responsabilidades de los Usuarios: El encargado de sistemas considera las siguientes responsabilidades de los usuarios de los sistemas informáticos de Vallecaucana de Aguas S.A. E.S.P.:

- Son responsables de las acciones realizadas en los sistemas informáticos a los que se les asignó acceso, así como de las credenciales entregadas para tal fin.
- Los funcionarios no deben compartir los datos de acceso a sus cuentas con otros funcionarios ni con personal contratista o terceros.
- Los funcionarios a los que se les asignó una cuenta y contraseña para el ejercicio de sus funciones, deberán cumplir con la política de seguridad informática de Vallecaucana de Aguas S.A. E.S.P., así como las políticas de seguridad de la entidad asignadora de cuentas.
- Los funcionarios y contratistas con acceso a los sistemas de información de la Vallecaucana de Aguas S.A. E.S.P., deben acogerse a las políticas y lineamientos establecidos para usuarios y contraseñas Vallecaucana de Aguas S.A. E.S.P., para garantizar una buena administración y gestión de las contraseñas y cuentas de usuarios.

Las cuentas del Directorio Activo de la Vallecaucana de Aguas S.A. E.S.P., asignadas se ajustarán a los siguientes lineamientos en caso de inactividad o desuso:

- Después de inactividad de treinta (30) días se procederá a bloquear la cuenta.
- Serán eliminadas las cuentas después de sesenta (60) días de inactividad.
- Las cuentas serán administradas por la oficina de las TIC's.

Acceso a las Bases de Datos y a los Sistemas de Información: Toda la información de Vallecaucana de Aguas S.A. E.S.P., contenida en los servidores y equipos, deberá estar centralizada con el fin de que se le puedan aplicar los mismos mecanismos de integridad, seguridad y recuperación de la información en el evento que se llegase a presentar alguna falla.

- Para acceder a la información de Vallecaucana de Aguas S.A. E.S.P., se debe contar con privilegios y niveles de acceso suficientes que garanticen la seguridad de la información; estos niveles de accesos serán controlados por un administrador único y serán otorgados a través del directorio activo.

- Se delimitarán las responsabilidades en cuanto a los permisos de lectura y escritura de la información o solamente consulta de la información.
- La información contenida en los recursos compartidos, serán respaldados según la frecuencia de actualización de los datos, haciendo respaldos históricos periódicos, será indispensable llevar una bitácora de las copias de seguridad hechas.
- En cuanto a la información contenida en los equipos de los funcionarios, la información que será respaldada será la que ellos copien en el servidor de archivos y en la unidad asignada para copias de seguridad.

Acceso a las Redes: El acceso a las redes por parte de los funcionarios y contratistas de Vallecaucana de Aguas S.A. E.S.P., no deberá comprometer la seguridad de los servicios de la red y debe garantizar:

- Aplicación de mecanismos adecuados de autenticación para equipos y usuarios.
- Control de acceso de los usuarios a los servicios de información.
- Mantener habilitados únicamente los puertos y servicios utilizados por los programas y servicios informáticos de la entidad.
- El acceso a las redes de Vallecaucana de Aguas S.A. E.S.P., es de uso exclusivo y únicamente para la infraestructura tecnológica de la entidad.

Roles y Perfiles de Usuarios:

Acceso a Servidores: El encargado de sistemas, define que los servidores tanto físicos como virtuales, estarán bajo un solo administrador perteneciente a su oficina y se accederá a los mismos por consola o escritorio remoto, haciendo los trabajos iniciales en ambientes de prueba y una vez se asegure su correcto funcionamiento se pasará al ambiente productivo.

Control de Accesos para Usuarios de la Entidad: El encargado de sistemas define los siguientes lineamientos como control de acceso para los funcionarios:

- Los usuarios de Vallecaucana de Aguas S.A. E.S.P., solamente tendrán permisos de acceso a las aplicaciones y bases de datos para los que estén específicamente autorizados por el jefe inmediato.
- Todos los accesos y conexiones remotos a los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P., deben ser controlados por medio de autenticación.

Autenticación de Usuarios de Red para Conexiones Externas: Las conexiones externas deberán ser previamente autorizadas por el jefe inmediato para la creación de los perfiles con dichos privilegios.

Cada uno de los funcionarios de Vallecaucana de Aguas S.A. E.S.P., será responsable del uso adecuado de los recursos de red y del seguimiento de los procedimientos definidos para el acceso a las redes.
Los sistemas de información de Vallecaucana de Aguas S.A. E.S.P., deben estar configurados de tal forma que solo puedan acceder a las funciones permitidas; los privilegios y niveles de acceso serán asignados al momento de crear el usuario y se mantendrá actualizada según las funciones del cargo, registrando las modificaciones que se produzcan en los niveles de acceso autorizados hasta la eliminación del usuario.

Trabajo y Conexiones Remotas: El trabajo desde conexiones remotas solo podrá ser autorizado por el director administrativo al funcionario que lo solicite; los permisos serán dados por el encargado de sistemas, una vez sean verificadas las condiciones de seguridad del ambiente remoto.

El uso de conexiones remotas será autorizado solo para servicios como aplicativos, servidor de archivos o infraestructura que sea inalcanzable desde redes externas.

El encargado de sistemas entregará e instalará las herramientas necesarias para hacer las conexiones de forma segura, de igual modo mantendrá monitoreo de estas conexiones, así como el tráfico y consumo de los recursos de red de Vallecaucana de Aguas S.A. E.S.P., de forma permanente.

Los usuarios que realicen conexiones remotas, deben tener las aprobaciones de la oficina de las TIC, para acceder remotamente a los recursos tecnológicos de Vallecaucana de Aguas S.A. E.S.P. Solamente podrán establecer dichas conexiones a través de VPN seguras y computadores previamente identificados en la red, es ideal que no use conexiones públicas de hoteles o de café internet con baja seguridad.

Los administradores de los sistemas realizarán monitoreos periódicos con el fin de detectar ingresos no autorizados, registrando eventos que servirán como evidencias en caso de producirse incidentes de seguridad.

Uso y creación de contraseñas seguras: Los funcionarios y contratistas Vallecaucana de Aguas S.A. E.S.P., deberán proteger sus contraseñas siguiendo estas recomendaciones:

- No escribir su contraseña en ningún lugar, papel o documento en el que quede expuesta.
- No enviar la contraseña por mensajes de texto, redes sociales o correo electrónico.
- No mencionar la contraseña en comunicaciones o conversaciones de ningún tipo.
- No usar contraseñas dadas en los ejemplos de creación de contraseñas robustas.
- No ingresar sus contraseñas en equipos de cómputo de los que no se está seguro de su nivel de seguridad y son monitoreados por terceros, como bibliotecas, cibercafés, entre otros.
- El uso de la contraseña es personal e intransferible, no se debe compartir con nadie.
- No se debe usar la opción "Recordar Contraseña" en programas de aplicación ni navegadores web.

- Informar al encargado de sistemas cualquier evento o incidente de seguridad que ponga en riesgo su contraseña.
- Informar encargado de sistemas si alguien dentro o fuera de la entidad le solicita revelar sus contraseñas.
- No permita que nadie le observe mientras usted escribe la contraseña.
- Siempre debe cambiar la contraseña dada por defecto por los desarrolladores o fabricantes.
- Luego de 3 intentos fallidos de ingreso de contraseña, la cuenta será bloqueada y el usuario tendrá que solicitar su desbloque al encargado de sistemas.
- Cuando un usuario inicie sesión por primera vez, el sistema exigirá el cambio de la contraseña.

El encargado de sistemas ha definido algunas recomendaciones al momento de crear una contraseña segura:

- No se debe usar información personal en la contraseña, como su nombre o el de algún familiar, ni su fecha de nacimiento, cuentas o números de tarjetas.
- Se debe usar mínimo 8 caracteres para crear la contraseña.
- Las contraseñas deben usar combinaciones aleatorias de los siguientes tipos de caracteres:
  - Minúsculas
  - Mayúsculas
  - Números
- Caracteres especiales (+ " @ # ¡ $ & % - /)
- Evitar el uso de secuencias básicas del teclado, por ejemplo: "1234", "98765", "Qwerty", entre otras.
- La contraseña no debe ser ni contener el nombre del usuario asociado a la misma.
- No se deben asignar contraseñas en blanco ni usar datos relacionados con el usuario que sean fácilmente deducibles como apodos, colores preferidos, por ejemplo.

- No usar fechas en las contraseñas.
- La contraseña no podrá ser la misma cuando el sistema solicite cambio.
- En caso de no cambiar la contraseña, la política de contraseñas le exigirá cambiarla cada cuarenta y cinco (45) días.
- Las contraseñas tendrán un histórico de 10 claves para que pueda volver a repetirse alguna de las usadas.

Uso de Medios Extraíbles: Para un uso adecuado de medios extraíbles, se deben tener en cuenta las siguientes recomendaciones:

- La información crítica o sensible de Vallecaucana de Aguas S.A. E.S.P., cuyo tiempo de vida sea mayor al tiempo del medio en el que se encuentra almacenado, tendrá que ser almacenada en el servidor de archivos para ser incluida dentro de la programación de copias de seguridad de la entidad.
- El uso de medios extraíbles como USBV, CD, o Discos Duros Externos; serán monitoreados y bloqueados para todos los usuarios, solamente se asignarán permisos su uso con previa autorización del jefe inmediato y por periodos de tiempo limitados.

8. SEGURIDAD

Antivirus:

Los funcionarios de Vallecaucana de Aguas S.A. E.S.P., deberán ejecutar el examen con el antivirus en los archivos y/o documentos que son abiertos por primera vez en el dispositivo, sobre todo los que se encuentren en medios de almacenamiento extraíble.

- Los funcionarios de Vallecaucana de Aguas S.A. E.S.P., procurarán que los archivos enviados por correo, descargados de internet o copiados a cualquier medio de almacenamiento de la red, provengan de sitios confiables o fuentes conocida y seguras con el fin de evitar contagios y propagación de virus informáticos o malware en los recursos tecnológicos de la entidad.
- Los usuarios que detecten o sospechen de alguna actividad por software malicioso deben notificar de inmediato al encargado de sistemas, para tomar las acciones pertinentes y evitar su propagación a través de la red.
- Permitir las actualizaciones del sistema operativo, firmware, servicios de red, bases de datos y sistemas de información que conforman los activos informáticos de la entidad.

Red:

- El propósito principal de la red es servir en la transformación e intercambio de la información dentro de Vallecaucana de Aguas S.A. E.S.P., entre funcionarios y colaboradores, departamentos y oficinas.
- La oficina de las TIC's no será responsable del tráfico ni de los contenidos de los datos compartidos en la red, toda la responsabilidad recaerá sobre el funcionario que la genere.
- Nadie podrá ver, copiar, manipular o destruir la información contenida en los equipos de Vallecaucana de Aguas S.A. E.S.P., sin autorización del responsable del mismo.

- Se prohíbe el uso de los recursos de red para labores que no sean propias de sus funciones dentro de Vallecaucana de Aguas S.A. E.S.P.
- Las credenciales de acceso a los servicios de red de Vallecaucana de Aguas S.A. E.S.P., son propiedad de la entidad y se usarán únicamente para actividades asociadas al desarrollo de las funciones del cargo.
- Cuando se encuentre un uso inapropiado de la red, se procederá a desconectar temporalmente la cuenta de red involucrada hasta que se considere que el uso no aceptable se ha suspendido.

Servidores:

- El encargado de sistemas es el único responsable de verificar la instalación, configuración e implementación de las políticas de seguridad en los servidores de la red.
- La configuración de todo servidor conectado a la red será responsabilidad del encargado de sistemas en compañía del operador del servicio prestado.
- El encargado de sistemas debe garantizar durante la configuración de los servidores que se cumplan las normas de seguridad para el uso de recursos compartidos y la restricción de accesos a directorios, servicios de información y programas ejecutas por los usuarios.
- Los servidores que proporcionen servicios a través de la red e internet deben:
  - Funcionar las 24 horas al día los 365 días del año.
  - Recibir mantenimiento preventivo por lo menos dos veces al año.
  - Mantenimiento semestral con depuración de logs.
  - Incluir la revisión de la configuración en el mantenimiento anual.
- La información de los servidores debe ser incluida en la política de copias de seguridad establecida por el encargado de sistemas.
- El acceso a internet solo podrá concederse a través de los servidores autorizados por el encargado de sistemas.

Seguridad Perimetral:

Es uno de los métodos principales de protección de la red, se basa en establecer recursos de seguridad en el perímetro externo de la red a diferentes niveles; lo cual permite establecer distintos niveles de confianza para permitir el acceso a determinados usuario internos o externos a servicios determinados y denegando servicios a otros.

- El encargado de sistemas, debe implementar soluciones lógicas y físicas que garanticen la protección de la información Vallecaucana de Aguas S.A. E.S.P., de posibles ataques externos o internos.
- Rechazar conexiones a servicios comprometidos.
- Tener definido el tráfico permitido (correo, http, https).
- Proporcionar un punto único de conexión con servicios en el exterior.
- Redirigir el tráfico entrante a través de los dispositivos de seguridad perimetral de Vallecaucana de Aguas S.A. E.S.P.
- Ocultar servicios y sistemas de fácil acceso desde internet.
- Auditar el tráfico entre el interior y el exterior de la entidad.
- Ocultar información como: nombres de sistemas, topologías de red, tipos de dispositivos de la red y cuentas de usuarios internos.

Sistemas de Detección de Intrusos:

Es una aplicación usada para detectar el acceso no autorizado a un servidor, a una red. Estos accesos pueden ser ataque hechos por usuarios malintencionados con conocimientos de seguridad o a través de bots.

- El encargado de sistemas implementará soluciones lógicas o físicas que impidan el acceso no autorizado a la red de Vallecaucana de Aguas S.A. E.S.P.
- Detección de ataques en momento real o poco después del suceso.

- Búsqueda automática de nuevos patrones de ataque usando herramientas de análisis de tráfico anómalo.
- Análisis detallado de logs y de tráfico de la red con el fin de encontrar máquinas o cuentas de usuario comprometidas en posibles intrusiones a la red.

Redes Privadas Virtuales: Los usuarios móviles y remotos de Vallecaucana de Aguas S.A. E.S.P., podrán acceder a la red interna cuando se encuentren fuera de la entidad con accesos a internet público usando redes privadas VPN habilitadas por el encargado de sistemas.

- El encargado de sistemas, será el encargado de la instalación y configuración de las aplicaciones necesarias y asignar los usuarios y claves para la conexión remota.
- El funcionario que solicite un acceso remoto por VPN, es responsable del mismo y del uso que se le dé.
- Para proceder con la asignación de la VPN a un funcionario o contratista para el acceso a aplicaciones, servidores u otros equipos de la red interna, debe cumplir con el siguiente procedimiento:
  - Solicitar la conexión VPN usando el formato establecido para tal fin.
  - La solicitud hecha, deberá incluir la justificación para el acceso remoto y el tiempo durante el cual tendrá vigencia; esto aplica para todos los funcionarios y contratistas que requieran desempeñar labores fuera de las instalaciones o en circunstancias especiales que así lo ameriten.
  - El encargado, procederá a revisar la solicitud, en caso de ser aprobada, se procede con la creación del perfil, asignación de usuario y contraseña e instalación de la aplicación VPN; en caso de no ser aprobada, se regresará al solicitante con las razones de la negación.
  - Una vez terminada la configuración y la instalación de la aplicación, se procederá a capacitar al usuario para conectarse a la VPN.

Seguridad Física y Ambiental del Centro de Cómputo:

- Las instalaciones diseñadas específicamente para los equipos de procesamiento, conectividad, servidores y demás elementos de tecnología, requieren una mayor protección que la proporcionada en las demás instalaciones; teniendo en cuenta que todas las funciones de TI y el material relacionado se clasifica como confidencial, debe protegerse de forma acorde.
- El acceso al centro de cómputo y centros de cableado será restringido y solo podrá ingresar personal autorizado por el encargado de sistemas.
- Únicamente el personal autorizado del área de sistemas, tiene acceso a gabinetes, en donde se encuentren ubicados elementos de infraestructura de procesamiento, almacenamiento, redes y seguridad; en caso de que alguna área requiera acceso a los gabinetes, debe solicitarlos a la oficina de las TIC para su análisis y aprobación.
- No se permite tomar fotografías o grabar vídeos en las áreas de procesamiento de información o en los lugares donde se encuentre dispositivos informáticos de almacenamiento de información que puedan comprometer la seguridad de la entidad a menos que tenga autorización del encardo de sistemas.

Vulnerabilidades:

Con el fin de estar preparados para cualquier evento que se pudiese presentar de pérdida de comunicación o daños en la infraestructura tecnológica, se deben tener en cuenta varios aspectos, a continuación:

- Contar con un inventario actualizado de sistemas de información, bases de datos e infraestructura instalada en Vallecaucana de Aguas S.A. E.S.P.
- Disponer de fuentes de información técnica a cerca de las vulnerabilidades descubiertas.
- Las vulnerabilidades se dividen en 4 grupos:
  - **Críticas:** Incluyen riesgos que podrían comprometer equipos e incluso interrumpir el servicio de algunas aplicaciones.

- **Alto:** Incluyen el riesgo de compromiso de equipos con degradación en el servicio de algunas aplicaciones.
- **Medio:** Incluyen riesgos de compromiso de equipos sin afectar el servicio de las aplicaciones.
- **Bajo:** Incluyen riesgos de daños locales a nivel de equipos de usuario sin pérdidas de información.

- La priorización de la atención de vulnerabilidades se encuentra definida así:
  - **Crítica**: Inmediata
  - **Alta**: 4 horas
  - **Media**: 8 horas
  - **Baja**: 24 horas

Gestión de Vulnerabilidades: Para este fin, se contemplan las siguientes actividades:

Identificación:

- Identificar el grado de riesgo que representa el evento.
- Recibir las alertas desde fuentes externas o herramientas internas de monitoreo.
- Revisión y ponderación de las alertas.
- Uso de herramientas de seguimiento.

Administración:

- Asignar nivel de riesgo al evento con base en el impacto que podría tener sobre Vallecaucana de Aguas S.A. E.S.P.
- Identificar los sistemas y equipos afectados.
- Asignar la revisión del evento al responsable de la aplicación.

Aplicación o Recuperación:

- Determinar el procedimiento a seguir según el nivel de riesgo detectado.
- Deshabilitar los sistemas o equipos expuestos si es necesario.
- Determinar el tipo de solución a aplicar.
- Probar la solución en ambiente de pruebas.
- Implementar la solución en los equipos productivos.
- Reportar la recuperación al encargado de sistemas.

Reporte:

Documentar las lecciones aprendidas durante el proceso de resolución del evento, para evitar que se repita o se presenten eventos similares en ocasiones futuras o que se puedan resolver de forma más eficiente.

Cumplimiento:

Una vez se haya resuelto el evento, se debe verificar su solución efectiva y que la vulnerabilidad presentada haya sido eliminada según lo esperado.

Gestión de seguimiento:

Realizar análisis de las acciones propuestas y tomadas para la mitigación de vulnerabilidades.

Gestión de LOGs: Aplica para toda plataforma tecnológica que cuente con cualquier sistema operativo, dispositivos de red, dispositivos de seguridad de Vallecaucana de Aguas S.A. E.S.P., como:

- Equipos de seguridad perimetral
- Servidores
- Equipos de Networking
- Aplicaciones
- Controles de accesos

Para la gestión de Logs, el encargado de sistemas, define los siguientes roles:

Responsable de Seguridad de la Información: Velar por el cumplimiento de las directrices dadas para conservar el nivel de confidencialidad de la información y mantener actualizado el plan según las necesidades de la entidad.

Responsable de TI: Encargado de sistemas debe ser el primero en enterarse de las actividades o eventos inusuales o consecuencias de accesos no autorizados. Analizará y coordinará la recolección de evidencias respecto a los eventos, teniendo cuidad de cumplir con los estándares respecto a manipulación, mecanismos de obtención y retención de evidencias. Será el encargado del registro de eventos ocurridos y su documentación.

Administrador de Plataforma: Monitoreo de la plataforma, debe revisar y extraer información de los Logs, debe evitar la propagación de eventuales actividades o consecuencias asociadas a los incidentes.

Sistemas Generadores de Logs:
Sistemas Operativos (servidores y equipos de red)

- Logs de sistemas
- Logs de audibilidad
- Logs de accesos de usuarios

- Logs de antivirus

Dispositivos perimetrales

- Logs de servidor de autenticación
- Logs de VPN y Firewall
- Logs de Malware
- Logs de accesos de usuarios

Aplicaciones

- Logs de Servidor de correo
- Logs de servidor web
- Logs de servidor de archivos
- Logs de servidor de base de datos
- Logs de accesos de usuarios

Rango de Criticidad de Logs: Estará clasificado de la siguiente manera:

- **Alto**: Son los Logs generados por dispositivos críticos como firewall, servidores y aplicaciones.
- **Medio**: Logs generados por dispositivos no tan críticos como equipos de red y algunas aplicaciones locales.
- **Bajo**: Generados por dispositivos de poco impacto como estaciones de trabajo y sus aplicaciones.

Conectividad: La autorización para acceder a internet, se concederá únicamente para actividades relacionadas con las funciones asociadas al cargo; todos los funcionarios y contratistas de Vallecaucana de Aguas S.A. E.S.P., y tendrán las mismas responsabilidades en cuanto al uso del internet.

- El acceso a internet estará restringido exclusivamente a la red establecida para tal fin, es decir, a través del sistema de seguridad perimetral por medio del firewall de la red.
- No se podrá acceder a internet buscando un proveedor de servicio directamente o usando algún navegador específico o con algún otro tipo de herramientas como módems.

Red inalámbrica: La red inalámbrica es un servicio que permite la conexión a Internet de la entidad sin la necesidad de cableado. Esta conexión, permitirá el acceso a los servicios de red internos como servidor de archivos, aplicaciones, bases de datos, además del acceso controlado a internet.
El encargado de sistemas, es el encargado de la administración, habilitación e incluso la eliminación de usuarios dentro de la red inalámbrica de Vallecaucana de Aguas S.A. E.S.P., por lo cual debe tener en cuenta el buen uso de los dispositivos Wireless (computadores portátiles, celulares, tabletas, etc.) conectados a la red. Para hacer uso de la red institucional, el dispositivo deberá estar dentro del dominio de la entidad para su autenticación en la red.

Evaluación de Riesgos de Seguridad Informática: Se deben aplicar las técnicas de gestión de riesgos a todos los sistemas informáticos y componentes de las redes en el momento oportuno y conveniente.

Esta evaluación de riesgos debe tener en cuenta:

- Importancia de la información, programas y activos del sistema informático.
- Las actividades, productos y servicios de Vallecaucana de Aguas S.A. E.S.P., respaldados en las copias de seguridad.
- Tener en cuenta los posibles daños causados por una seria violación de la seguridad informática de la entidad, los impactos reales y potenciales que esto conlleve, como

el daño en la reputación de la entidad ante el estado colombiano y el público en general, la mala prensa y el potencial incumplimiento de las labores de la entidad.

- Contemplar las posibilidades de que ocurra una violación de seguridad, según los controles que se tienen en la red y las amenazas latentes, teniendo en cuenta el entorno en el que funciona el sistema y la vida útil de la información en el posible riesgo.
- Prever los controles adicionales que se requieran para reducir los riesgos a los niveles mínimos aceptables.
- Implementar las acciones necesarias para aplicar los nuevos controles correspondientes; en caso de encontrar niveles de riesgo inaceptables o que no se puedan reducir con los controles actuales, se debe plantear e implementar mejoras en la seguridad informática.

Gestión de Borrado Seguro: El encargado de sistemas verificará las siguientes condiciones antes de realizar un procedimiento de borrado seguro:

- Acta de entrega del equipo de cómputo al encargado de sistemas.
- Realizar una copia de seguridad del dispositivo y copiarla al servidor de información histórica para ser consultada únicamente con permisos de lectura a quien los solicite y el jefe del área autorice.
- EL procedimiento de borrado seguro se aplicará sobre todos los equipos de propiedad de Vallecaucana de Aguas S.A. E.S.P.

9. EXCEPCIONES

No hay excepciones en el lineamiento de seguridad definido.

10. REFERENCIAS A OTRAS POLÍTICAS, LINEAMIENTOS Y NORMAS DE SOPORTE

- Lineamientos de Gobierno en Línea.
- Mejores Prácticas Cobit, Togaf
- Norma ISO 27001

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. Andrés Felipe Solórzano Gómez – Director Jurídico.
Aprobó: Dr. Luis Eduardo Pineda Álzate – Director Administrativo.
Copia: Archivo.