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

PDA
PLAN DEPARTAMENTAL DE AGUAS
VALLE DEL CAUCA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 3

Vallecaucana de Aguas S.A. E.S.P.

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

PDA Plan Departamental de Aguas VALLE DEL CAUCA

Contenido

INTRODUCCION

Todos los riesgos de seguridad en torno a las tecnologías, se basan en la manipulación y tratamiento del recurso humano, esto debido a que se debe motivar en seguir la normatividad y los diferentes procedimientos que incurren en la seguridad y la privacidad de la información, el cual se les asigna teniendo en cuenta sus actividades y funciones dentro de la Entidad. La evaluación y seguimiento del presente plan se diseña y elabora mediante un proceso sistemático y con directrices de la metodología SGSI "Sistema de Gestión de Seguridad Informática" Norma ISO 27001.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Vallecaucana de Aguas S.A. E.S.P., es de gran importancia para la gestión del riesgo de la información y con esta herramienta los encargados de sistemas, tienen como principal alcance evitar y/o minimizar los riesgos que conllevan a procesos malintencionados que produzcan la pérdida o daño de los activos informáticos de la Entidad. Por tal motivo, se crean pautas que permitan garantizar que los tipos de riesgos de seguridad informática sean prevenidos y controlados eficientemente.

GENERALIDADES DE LA ENTIDAD

Misión:

Gestionar e implementar proyectos integrales de inversión regional y municipal sostenibles, que mejoren cobertura, calidad, continuidad, crecimiento y viabilidad empresarial de los servicios de agua potable, saneamiento básico y ambiental para el Departamento del Valle del Cauca, y sus actividades complementarias, de acuerdo con su conveniencia financiera y estratégica, generando rentabilidad sin detrimento de la calidad, para cumplir con su función social y contribuir a mejorar la calidad de vida de la comunidad, el desarrollo sostenible de la región y el bienestar de sus trabajadores.

Visión:

Ser la empresa Vallecaucana reconocida por el mayor impacto social en las condiciones de vida de los vallecaucanos, relacionadas con el sector de agua potable y saneamiento básico y el respeto por el medio ambiente.

Ser administrada con enfoque empresarial que la conduzca a lograr su sostenibilidad, rentabilidad y crecimiento dentro de un clima organizacional que propicie conductas éticas y actuaciones transparentes, que genere en sus empleados sentido de pertenencia, desarrollo profesional y técnico.

Objetivo General:

Implementar estrategias de gestión para el tratamiento de riesgos de seguridad de la información de la Entidad, a través de un Plan que garantice la integridad, confidencialidad y disponibilidad de la información.

Objetivos Específicos:

- Identificar y conocer el estado actual de los riesgos durante la vigencia 2021 correspondiente a todos los procesos de integridad, confidencialidad y disponibilidad que existen en la entidad.
- Establecer control en las políticas de la Seguridad de la información que garantice la, integridad, confidencialidad y disponibilidad.
- Definir el seguimiento a los riesgos de los todos los procesos que afectan la integridad, confidencialidad y disponibilidad de la información.
- Identificar las debilidades y amenazas que afectan los activos informáticos de la entidad.
- Garantizar los procesos misionales y administrativos dentro de la entidad.
- Minimizar los riesgos mediante recomendaciones estratégicas concientizando a todos los funcionarios de la Entidad.
- Mejorar continuamente los procesos con eficacia, eficiencia y efectividad.

Centro de Aseguramiento:

La Gestión del Riesgo de la Entidad y todos los procesos tecnológicos se llevan a cabo desde el encargado de sistemas de la entidad Vallecaucana de Aguas S.A. E.S.P.

NORMATIVIDAD:

- Ley 44 de 1993 "Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944." (Derechos de autor).

- Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

- Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "De la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

- Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

- Decreto 2641 de 2012: Por el cual se reglamentan el artículo 73, Plan Anticorrupción y de Atención al Ciudadano, y el artículo76, Oficina de Quejas, Sugerencias y Reclamos de la Ley 1474 de 2011.

- Ley 1581 de 2012, "Por medio de la cual se dictan disposiciones para la protección de datos personales".

- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- CONPES 3854 de 2016 – Política de Seguridad Digital del Estado Colombiano.

- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión. Guía para la administración del riesgo y el diseño de controles en entidades públicas.

- Norma Técnica Colombiana ISO27001:2013. Norma Técnica Colombiana ISO31000:2013. Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD).

- Decreto 612 de 2018 "Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado."

- Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015 decreto único reglamentario del sector de Tecnologías de la Información y Comunicaciones".

DEFINICIONES GENERALES:

Activo Informático:

Activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controla en su calidad de tal.

Amenaza:

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización (ISO/IEC 27000). Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Análisis de Riesgo:

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo (IS/IEC 27000).

Calificación del Riesgo:

Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Control:

Acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.

Datos Abiertos:

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y

sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Disponibilidad:

Propiedad de ser accesible y utilizable a demanda por una entidad. (2.10 ISO 27000).

Evaluación del Riesgo:

Resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.

Gestión del Riesgo:

Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Identificación del Riesgo:

Etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos.

Información:

Conjunto de datos, ya procesados y ordenados para su comprensión, que aportan nuevos conocimientos a un individuo o sistema sobre un asunto, materia, fenómeno o ente determinado.

Integridad:

Propiedad de salvaguardar la exactitud y el estado completo de los activos. (2.36 ISO 27000)

Mapa de Riesgos:

Documento que, de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.

Norma ISO 27001:

Es un estándar internacional que describe cómo implementar el Sistema de gestión de seguridad de la información de una empresa. Investiga como salvaguardar la información mediante una serie de estándares, lineamientos y procesos que facilitan la identificación de los riesgos.

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).

Privacidad:

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Seguridad de la Información:

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de la Información: Es la denominación convencional de un conjunto de procesos por los cuales se controla el ciclo de vida de la información,

desde su obtención (por creación o Captura), hasta su disposición final (su archivo o eliminación).

Sistema de Gestión de Seguridad de la Información SGSI:

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 y de mejora continua. (ISO/IEC 27000).

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).

Valoración del Riesgo:

Establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si se necesita.

IDENTIFICACION DEL RIESGO:

Dentro de la entidad pública se pueden presentar los siguientes riesgos:

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- **Riesgos de Imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **Riesgos Operativos:** Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

- **Riesgos de Tecnología:** Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

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

PDA

Mapa de Riesgos:

	Nombre de la entidad	Vallecaucana de Aguas S.A. E.S.P.	
	Nombre Del Proceso	Plan de Tratamiento de Riesgo y Privacidad de la Información	
OBJETIVO DEL PROCESO: Identificar los riesgos y su valoración.			

N	RIESGO	TIPO DE RIESGO	CAUSA	CONSECUENCIAS	PROBABILIDAD		IMPACTO	EVALUACIÓN PLAN DE ACCION (Zona de Riesgo)		ANALISIS DE CONTROLES						PERIODO DE SEGUMIENTO	PLAN DE ACCION	
										ESTADO					DESCRIPCION DE CONTROLES		ACCION A IMPLEMENTAR	RESPONSABLE
1	Perdida de Información al Realizar un Mantenimiento	Tecnológico	Mal procedimiento al realizar Backup	Perdida de información vital para la dependencia	Raro	1	Mayor	4	Alto	→Ir	1	Raro	4	Mayo	Seguir lista de control de procedimiento para realizar mantenimiento	Mensual	Implementar Procedimientos claros para mitigar el riesgo de perdida de información	Oficina de las TIC
2	Sistemas de información desactualizados y sin licencia de uso.	Tecnológico	Falta de compromiso por parte de la administración para realizar los procesos de actualización.	Acciones de responsabilidad administrativa por parte de entes de control y perdida de integridad por parte del sistema de información	Probable	4	Moderado	3	Alto	→Ir	4	Probable	3	Moderado	Procesos de contratación claros y definidos	Anual	Actualizaciones y compra de licencias de uso	Oficina de las TIC

3	Ataque Cibernético	Tecnológico	Sistemas de Seguridad Desactualizados	Perdida de información y exposición del área financiera	Raro	1	Moderado	3	Moderado	→Ir	1	Raro	3	Moderado	Sistemas de Antivirus y Firewalls actualizados	Diario	Sistemas de información protegidos por Antivirus y Firewall actualizados	Oficina de las TIC
4	Perdida y daño de equipos audiovisuales en préstamo	Tecnológico	Robo, mal uso de los dispositivos en préstamo	Perdida de activos de Vallecaucana de Aguas S.A. E.S.P.	Raro	1	Menor	2	Bajo	→Ir	1	Raro	2	Menor	Verificación de los dispositivos a prestar a través de una lista de chequeo y formato de salida de Talento Humano	Diario	Lista de chequeo y control de entradas y salidas de equipos informáticos	Oficina de las TIC

5	Uso inapropiado de los equipos informáticos y apropiación de TIC	Tecnológico	falta de asistencia y compromiso por las capacitaciones, sensibilización de planes estratégicos y retroalimentación de temas de innovación.	Falta de conocimientos en el manejo y uso de los recursos informáticos	Improbable	2	Menor	2	Bajo	→Ir	2	Imposible	2	Menor	Plan de capacitaciones y procedimiento de las TIC para las diferentes dependencias.	Mensual	Ejecutar capacitaciones a todos los funcionarios de una manera dinámica para el acceso y uso de las distintas herramientas informáticas	**Oficina de las TIC**
6	Inadecuada gestión en la implementación de arquitectura de nuevos sistemas de información y servicios WEB	Tecnológico	Carencia de nuevas tecnologías y accesos a los sistemas de información en línea	Insatisfacción de los usuarios	Improbable	2	Menor	2	Bajo	→Ir	2	Imposible	2	Menor	Implementación de un Web Service y servicios TIC	Anual	Disponibilidad de servicio en línea y pagos en línea	**Oficina de las TIC**
7	Infraestructura tecnológica insuficiente	Tecnológico	Recursos Económicos y equipos obsoletos	Deterioro, vida útil menor y lentitud en las actividades laborales.	Probable	4	Moderado	3	Alto	→Ir	4	Probable	3	Moderado	Mantenimientos preventivos y correctivos.	Anual	Alargar vida útil de los equipos de computo existentes	**Oficina de las TIC**

8	Interacción del Servicio de Internet	Tecnológico	Fallos constantes del proveedor del servicio, no cumple con lo contratado.	Traumas y atrasos en los procesos especialmente las áreas de Hacienda.	Probable	4	Moderado	3	Alto	→Ir	4	Probable	3	Moderado	Internet alterno	Diario	Contratar un servicio de internet de respaldo	**Oficina de las TIC**

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja. Reducir el riesgo
M: Zona de Riesgo Moderada. Asumir el riesgo, reducir el riesgo
A: Zona de Riesgo Alta. Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgo extrema. Reducir el riesgo, evitar, compartir o transferir

Factores de Riesgo:

Son todos aquellos riesgos que afectan la integridad, la confidencialidad y la disponibilidad de la información.

Factor	Riesgos
Humanos	- Fraudes - Hackers - Robo o Hurto - Accesos no Autorizados - Sabotaje
Ambientales	- Lluvias - Sismos - Humedad - Temperaturas altas - Incendios

Tecnológicos	- Fallos en el Hardware y Software - Ataques Informáticos (Virus) - Programas Maliciosos - Denegación de Servicios - Fraude Electrónico - Conectividad a Internet - Bloqueo de Aplicaciones
Eléctricos	- Falla del servicio eléctrico - Puntos sin servicio - Falta de Conexión

Análisis del Riesgo:

Sector	Descripción Riesgo	Amenaza	Valoración Riesgo
Gestión Administrativa	- Área Financiera - Área de Planeación y Desarrollo Económico - Área de Infraestructura - Área TIC - Área de Archivo Central	Daño en los Servidores por el área de humedad. Hacinamiento. Extintores Pasados de fecha. Red eléctrica inestable. Fuego. Agua. Fenómenos sísmicos. Fallas en el suministro del aire acondicionado.	Alto
Gestión Operativa	- Atención al Usuario - Diligenciamientos de Formatos de	Daños en los equipos de cómputos y de oficina. Fallas de los equipos informáticos.	Alto

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja. Reducir el riesgo
M: Zona de Riesgo Moderada. Asumir el riesgo, reducir el riesgo
A: Zona de Riesgo Alta. Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgo extrema. Reducir el riesgo, evitar, compartir o transferir

Factores de Riesgo:

Son todos aquellos riesgos que afectan la integridad, la confidencialidad y la disponibilidad de la información.

Factor	Riesgos
Humanos	- Fraudes - Hackers - Robo o Hurto - Accesos no Autorizados - Sabotaje
Ambientales	- Lluvias - Sismos - Humedad - Temperaturas altas - Incendios

Tecnológicos	- Fallos en el Hardware y Software - Ataques Informáticos (Virus) - Programas Maliciosos - Denegación de Servicios - Fraude Electrónico - Conectividad a Internet - Bloqueo de Aplicaciones
Eléctricos	- Falla del servicio eléctrico - Puntos sin servicio - Falta de Conexión

Análisis del Riesgo:

Sector	Descripción Riesgo	Amenaza	Valoración Riesgo
Gestión Administrativa	- Área Financiera - Área de Planeación y Desarrollo Económico - Área de Infraestructura - Área TIC - Área de Archivo Central	Daño en los Servidores por el área de humedad. Hacinamiento. Extintores Pasados de fecha. Red eléctrica inestable. Fuego. Agua. Fenómenos sísmicos. Fallas en el suministro del aire acondicionado.	Alto
Gestión Operativa	- Atención al Usuario - Diligenciamientos de Formatos de	Daños en los equipos de cómputos y de oficina. Fallas de los equipos informáticos.	Alto

	Caracterización de los Usuarios. - Interacción de las utilidades y Aplicaciones Institucionales	Interferencias. Mal funcionamiento del software. Virus (Malware, Troyano, gusano, etc.). Perdida de datos informáticos. La Entidad requiere de sistema de cámaras de vigilancia, alarmas contra incendios, etc. No se tiene los extintores adecuados.	
Aplicaciones	- Planes en general - App Adquiridos	Daño en las aplicaciones de los Sistemas Operativos. Eliminación de datos y de backup. Usos no autorizados de aplicaciones y equipos. Copias de software. Ausencia de identificación y autenticación de usuarios. Contraseñas sin protección.	Moderado
Comunicaciones y Redes Sociales	- Páginas WEB - Email Institucionales - Red telefónica.	Eliminación de datos. Alteración de red cableada (Router, Swich, etc.). Alteración de red inalámbrica (Router, AP, etc.).	Bajo

		Conexión deficiente del cableado. Falta de conciencia en la seguridad. No se cuenta con un cableado estructurado adecuado, tanto para red, datos y sistema eléctrico. La Entidad no cuenta con una red de internet alterna (Solo tiene un Proveedor) y no es la más adecuada	
Recurso Humano y Conectividad	- Red de Datos Puntos de Red Área de Trabajo	Los Puntos de red no son suficientes. Existen cables de energía sulfatados, no están disponibles para la cantidad de funcionarios. La pérdida de datos es constante porque no cuentan con UPS para cuando son desconectados. El cuidado de los equipos de cómputo y de oficina no tiene el mejor uso, acortando así su vida útil. Es muy común encontrar información personal, el cual comprueba la falta de	Alto

		confidencialidad y privacidad de la información personal. La información de la Entidad sale fácilmente con medios de almacenamiento por parte de sus funcionarios. El internet es muy lento y por tanto la pérdida de señal ha afectado las actividades administrativas constantemente. Los funcionarios incumplen las reglas básicas del cuidado de los equipos informáticos. No existen bancos de bases de datos de los Backup	

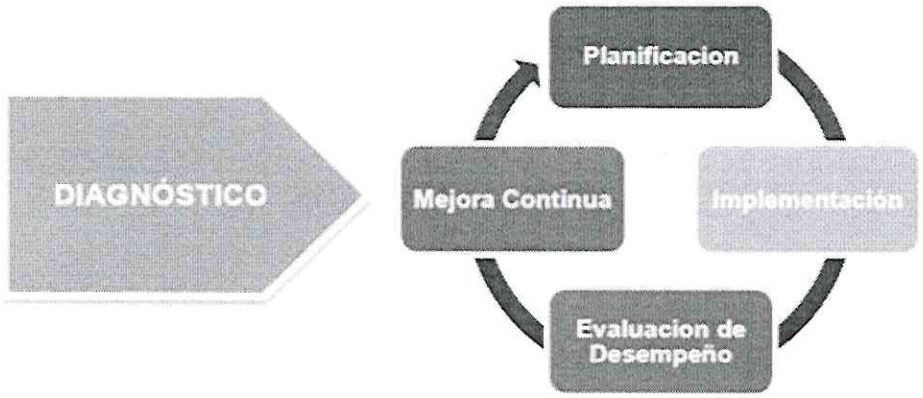
VALORACION DEL RIESGO:

Niveles de Impacto:

Activo / Recursos	Valoración Riesgo	Ocurrencia
Servidores	3	Moderado
Sistemas de Información	4	Alto
Fluido Eléctrico 3 Alta	3	Alto
Red de Datos	3	Moderado
Áreas de Trabajo	2	Bajo
Página Institucional – Gobierno Digital	2	Bajo
Internet	4	Moderado

MEDIDAS DE IMPLEMENTACION:

El plan se fundamenta en la metodología ISO 27001, mediante su ciclo continuo PHVA, este sistema establece una serie de lineamientos estandarizados, con el fin de asegurar la integridad, confidencialidad y disponibilidad de los activos informáticos de la entidad como son: las Bases de datos, documentos, aplicaciones, equipos tecnológicos, etc.:



Ciclo PHVA de SGSI

Fuente: NTC – ISO/IEC 27001

- **Planificar - Establecer el SGSI:** Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con objetivos globales de una organización.

- **Hacer - Implementar y utilizar el SGSI**: Implementar y operar la política, los controles, procesos y procedimientos del SGSI.

- **Verificar - Monitorizar y revisar el SGSI:** Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

- **Actuar - Mantener y mejorar el SGSI:** Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

CRONOGRAMA:

Ítem	Implementación	Actividades	Fecha Implementación
1	**Activos de Información**	Diseñar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Elaborar Inventario de Activos de Información de la entidad. Realizar Diagnostico de los activos y su estado.	Enero – Diciembre
2	**Riesgos de Seguridad de la Información**	Implementar Políticas de Seguridad de la Información. Identificar los riesgos. Analizar los riesgos (Internos y Externos). Valorar los riesgos. Implementar el tratamiento de los riesgos. Realizar seguimiento de los riesgos identificados. Motivar al cumplimiento y aplicabilidad de los controles y acciones para minimizar los riesgos.	Enero - Diciembre

MEDIDAS DE SEGUIMIENTO DEL RIESGO:

El seguimiento y evaluación propuestos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se realiza y establece las siguientes acciones para la actual vigencia:

- Reconocer los activos de la Entidad que requieren la protección por su valoración.
- Detectar riesgos diariamente en los activos físicos y lógicos de la información
- Realizar Backup periódicamente.
- Vacunar con un antivirus licenciado constantemente
- Implementar y proteger la red con Firewall.
- Realizar el mantenimiento en el sistema eléctrico y ubicar más puntos para conexión.
- Revisar la DOFA de la Entidad correspondiente a la Seguridad y la privacidad de la información.
- Socializar y capacitar a los funcionarios sobre las políticas de seguridad y privacidad de la Información.
- Crear usuarios y claves autorizadas a personal que administre información delicada y/o confidencial.
- Brindar soporte preventivo y correctivo a todos los equipos de cómputo, teniendo en cuenta el Plan de Mantenimientos de la Oficina de las TIC para la vigencia 2021.
- Monitoreo de las responsabilidades de los funcionarios y el tratamiento del equipo asignado.

- Confirmar línea alterna de internet.

MEDIDAS DE CUMPLIMIENTO Y APLICABILIDAD:

Para el cumplimiento y aplicabilidad del presente Plan estructurado, es importante la participación e integración de todos los funcionarios que hacen parte de la entidad directa e indirectamente. Mediante este modelo de aplicación de seguridad y privacidad de la información se establece una cultura donde intervienen el ejercicio tecnológico dentro de sus actividades o funciones y así garantizar su fortalecimiento; implementando la estrategia de Gobierno Digital, se socializarán los planes y documentos institucionales en su página WEB www.vallecaucanadeaguas.gov.co, correo institucional contacto@eva.gov.co

- Cumplir las normas y directrices de la Entidad relacionadas con el tratamiento de los riesgos informáticos.
- Crear conciencia y sentido de pertenencia frente a los beneficios de aplicar los controles y prendimientos en los riesgos que se presenten en su área.
- Reportar al área asignada o líder de las TIC, de los eventos de riesgo que se puedan generar en el área de trabajo.
- Realizar adecuados procedimientos con el uso de los equipos informáticos asignados a su cargo.
- Desarrollar planes de contingencia para asegurar la continuidad de los procesos administrativos de la entidad (existente el Plan de Contingencia en la Oficina de la TIC).
- Evitar instalar aplicaciones desconocidas, ni permitir instalaciones de archivos no confiables en su equipo de cómputo.
- Cuidar de golpes, alimentos y bebidas todos los quipos de cómputo.
- Conectar los equipos de cómputo a una conexión eléctrica con capacidad.

- Crear contraseñas personales para sus equipos y usos de archivos internos.
- Solicitar copias de seguridad (Backup) periódicamente.

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.