PLAN DE TRATAMIENTO DE RIESGOS DESEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Versión 3

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

Contenido

INTRODUCC
ION

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 formación, 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 permite garantizar que los tipos de riesgos de seguridad informática seanprevenidos 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 básicoy 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 transparente, 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, confidencialidady disponibilidad de la información.

Objetivos Específicos:

- Identificar y conocer el estado actual de los riesgos durante la vigencia 2022 correspondiente a todos los procesos de integridad, confidencialidad y disponibilidadque existe 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 todos los procesos que afectan la integridad,confidencialidad y disponibilidad de la información.
- Identificar las debilidades y amenazas que afecten 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.
- Mejora 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 desdeel 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 1994” (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 sanación de actos de corrupción y la efectividad del control de la gestión pública”.
- Decreto 2641 de 2012 “por el cual se reglamentan el art. 73, plan Anticorrupción y de Atención al Ciudadano, y el art. 76, 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 protecciónde 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 Riesgo 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 delEstado”.
- Decreto 1008 de 2018, “por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga en 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 probabilidades 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 elimpacto 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 disposición de cualquier ciudadano, de forma libre y 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 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 riesgos 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 entedeterminado.

Integridad

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

Mapa de Riesgo

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 delos 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 20007).

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 infracción 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/IEC27000).

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 (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 de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Valoración de 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.

IDENTIFICACIÓN DEL RIESGO

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

- **Riesgos estratégicos**: 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 partede 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 de la articulación entre las 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 cobre los bienes.
- **Riesgos de Cumplimientos**: 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.

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

OBJETIVO DEL PROCESO: Identificar los riesgos y su valoracion.

									ANALISIS DE CONTROLES							PLAN DE ACCION	
N	RIESGO	TIPO DE RIESGO	CAUSA	CONSECUENCIAS	PROBABILIDAD		IMPACTO	EVALUACION PLAN DE ACCION (Zona de Riesgo)	ESTADO					DESCRIPCION DE CONTROLES	PERIODO DE SEGUIMIENTO	ACCION A IMPLEMENTAR	RESPONSABLE
1	Perdida de la informacion al realizar un mantenimiento	Tecnologico	Mal procedimiento al realizar un Backup	Perdida de informacion vital para la dependencia	Raro	1	mayor	4	Alto	ir	1	Raro	4	mayo	Seguir lista de contro de procedimiento para realizar mantenimiento	MENSUAL	Implementar procedimientos claros para mitigar el riesgo de perdida de información	Oficinas de las TIC
2	Sistemas de informacion desactualizados y sin licencias de uso	Tecnologico	Falta de compromiso por parte de la administracion para realizar los procesos de actualizacion	Acciones de responsabilidad 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	Proceso de contratacion claros y definidos	Anual	Actualizaciones y compra de licencias de uso	Oficinas de las TIC

3	Ataque cibernetico	Tecnologico	Sistemas de seguridad Desactualizadas	Perdida de informacion y exposicion del area financiera	Raro	1	Moderado	3	Moderado	ir	1	Raro	3	Moderado	Sistemas de Antivirus y Firewalls actualizados	Diario	Sistemas de informacion protegidos por Antivirus y Firewall actualizados	Oficinas de las TIC
4	Perdida y daños de equipos audiovisuales en préstamo	Tecnologico	Robo, mal uso de los dispositivos	Perdida de activos de Vallecaucana de Aguas S.A. E.S.P.	Raro	1	Menor	2	Bajo	ir	1	Raro	2	menor	Verificacion 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 salida de equipos informaticos	Oficina de las Tic

5	Uso inapropiado de los equipos Informaticos y apropiacion de TIC	Tecnologico	Falta de asistencia y compromiso por las capacitacion es. Sencibilizaci on de planes estrategicos y retroaliment acion de temas de innovación.	Falta de conocimiento en el manejo y uso de los recursos informaticos	improbab le	2	Menor	2	Bajo	ir	2	Imposible	2	menor	Plan de capacitacion es y procedimient o de las TIC para las diferentes dependencia s	Mensual	Ejecutar capacitacion a todos los funcionarios de una manera dinamica para el acceso y uso de las distintas herramientas informaticas	Oficina de las TIC
6	Inadecuada gestion en la implementacion de arquitectura de nuevos sistemas de informacion y servicios WEB	Tecnologico	Carencia de nuevas tecnologas y accesorios a los sistemas de informacion en linea	Insastisfaccion de los usuarios	improbab le	2	Menor	2	Bajo	ir	2	Imposible	2	menor	Implementac ion de una WEB service y servicios TIC	Anual	Disponibilida d de servicio en linea y pagos en linea	Oficina de las TIC
7	Infraestructura tecnologica insuficiente	Tecnologico	Recursos Economicos y equipos obsoletos	Deteriro, vida util menor y lentitud en las actividades laborales	Probable	4	Moderado	3	Alto	ir	4	Probable	3	Moderado	Mantenimien tos preventivos y correctivos	Anual	Alargar vida util de los equipos de computo existentes	Oficina de las TIC

8	Interaccion del Servivio de Internet	Tecnologico	Fallos constantes del proveedor del servicio, no cumple con lo contratado.	Traumas y atrasos en los procesos especialmente las areas 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 disponibilidadde la información.

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

Tecnológicos	- Fallos del 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 Riesgos	Amenaza	Valoración Riesgo
Gestión Administrativa	- Área Financiera - Área de Planeación y Desarrollo Económico - Área de infraestructura - Área TIC - Área 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 cómputo 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 disponibilidadde la información.

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

Tecnológicos	- Fallos del 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 Riesgos	Amenaza	Valoración Riesgo
Gestión Administrativa	- Área Financiera - Área de Planeación y Desarrollo Económico - Área de infraestructura - Área TIC - Área 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 cómputo y de oficina. Fallas de los equipos informáticos.	Alto

	Caracterización de los usuarios. - Interacción de las Aplicaciones institucionales	Interferencias. Mal funcionamiento del software. Virus (Malware, Troyano, gusano, etc.). Perdida de daos informáticos. La entidad requiere de sistemas 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 usuarios autenticación de usuarios. Contraseñas sin protección	Moderado
Comunicaciones y Redes Sociales	-Páginas Web -Email institucionales -Red telefónica	Eliminacion de satos. Alteración de red cableada (Router, Swich, etc.) Alteración de red inalámbrica (router,AP, etc.) 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	Bajo

Recursos Humanos y Conectividad	Red de Datos Puntos de Red Área de trabajo	Los puntos en la red no son suficientes. Existen cables de energía sulfatados, no están disponibles para la cantidad de funcionarios. La pérdida de datos es constate porque no cuentan con UPS para cuando son desconectados. El cuidado de los equipos de cómputo y de oficina no tienen 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 los funcionarios. El internet es muy lento y por tano la perdida 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 satos de los Backup.	

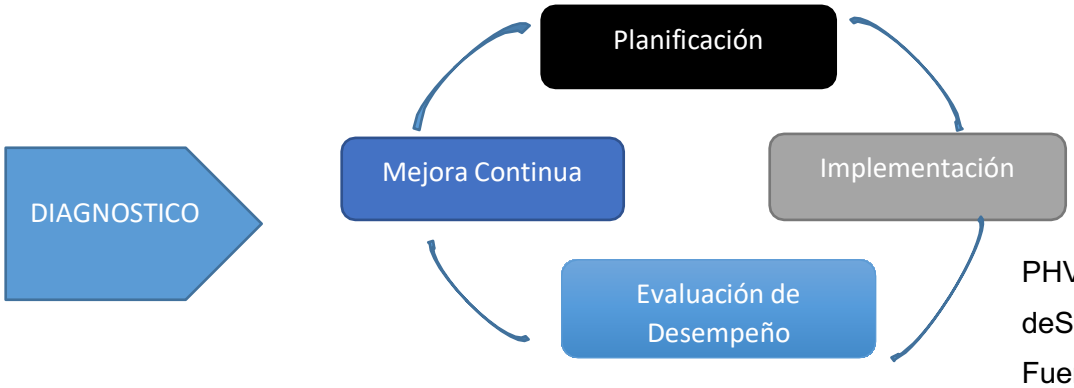
VALORACION DEL RIESGO

Niveles de Impacto:

Activo / Recursos	Valoración Riesgo	Ocurrencia
Servidores	3	Moderada
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 daos, documentos, aplicaciones, equipos tecnológicos, etc.



Ciclo PHVA deSGSIF 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 formación, con el fin de entregar resultados acordes con los 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 auditoria 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 plan de tratamiento de Riesgos de seguridad y Privacidad de la Información. Elaborar Inventario de Activos de Información de la Entidad. Realizar Diagnósticos de los Activos y su resultado	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. Realizar seguimiento de los riesgos identificados. Motivar al cumplimiento y aplicabilidad de los controles y acciones para minimizar los riesgos	Enero- Diciembre

MEDIDAS DEL 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 actualvigencia:

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

- Confirmar línea alterna de internet.

MEDIDAS DE CUMPLIMIENTO Y APLICABILIDAD

Para el cumplimiento y aplicabilidad del Plan estructurado, es importante la participación e integración de todos los funcionarios que hacen parte de la entidad directa e indirectamente. Mediante este modelo e aplicación de seguridad y privacidad de la información se establece una cultura donde interviene el ejercicio tecnológico dentro de sus actividades o funciones y así garantizar su fortalecimiento; implementando la estrategia de Gobierno Digital, se socializaran los planes y documentos institucionales en su página WEB www.vallecaucanadeaguas.gov.co, correo institucional contact@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 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 puedangenerar en el área de trabajo.
- Realizar acuerdos procedimientos con el uso de los equipos informáticos asignadosa su cargo.
- Desarrollar planes de contingencia para asegurar la continuidad de los procesos administrativos de la entidad (existe el Plan de Contingencia en la Oficina de las TIC).
- Evitar instalar aplicaciones desconocidas, ni permitir instalaciones de archivos noconfiables en su equipo de cómputo.
- Cuidar de golpe, alimentos y bebidas todos los equipos 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.

PLAN DE COTINUIDAD

- **OBJETIVO Y CONTEXTUALIZACIÓN**

- Establecer las estrategias y actividades que deben ser implementadas por la empresa Vallecaucana de Aguas S.A E.S.P. para proveer el

direccionamiento, soporte, equipamiento y metodologías para la continuidad de los servicios establecidos para la prestación del servido.

- **ALCANCE**

- Inicia estableciendo las pautas del plan y finaliza modificando los planes de acuerdo a las oportunidades de mejora que arrojen las pruebas, ensayos y las auditorías realizadas a Vallecaucana de Aguas S.A E.S.P.

- **RESPONSABLE**

- La definición de criterios, planes iniciales, valoración de análisis de impacto de negocios se dinamizan desde la empresa Vallecaucana de Aguas S.A E.S.P. bajo el liderazgo del director tecnología. No obstante, responde a la gerencia general la asignación de los recursos necesarios para el plan de continuidad de los servicios.

- **DEFINICIONES**

- **Activo de Información:** Se denomina activo a aquello que tiene valor para la organización y por lo tanto debe protegerse. De manera que un activo de información es aquel que contiene o manipula información.

- **Amenaza:** Evento que puede desencadenar un incidente dentro de la organización.

- **Análisis de Riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización. Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Análisis** de **Impacto al Negocio** (AIN): Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos

requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos. Proceso del análisis de actividades y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22301)

- **Centro de Alterno de Recuperación** (CAR): Sitio de alojamiento de equipos y canales de comunicación, diferentes al sitio normal de ubicación de los sistemas de cómputo, q u e se tiene preparado para operar en caso de un desastre total del sitio principal.

- **Cliente** (customer): persona u organización o parte de una organización que recibe el servicio o los servicios, destinados a esa persona u organización o requerido por ella. Hacen parte de esta definición: usuarios finales, clientes, receptor del producto o servicio del proceso interno.

- **Crisis:** Evento disruptivo con la capacidad de afectar negativamente las operaciones la integridad de los empleados, proveedores o la comunidad atraer la atención de medios de comunicación, autoridades regulatorias y en consecuencia afectar la reputación de la organización y los intereses de los accionistas.

- **Evento:** Situación o comportamiento inesperado que cause la interrupción en el ambiente de trabajo, recursos o personal de la organización generando como resultado la no disponibilidad de los servicios prestados a los clientes internos y/o externos.

- **Interrupción:** Es el período de tiempo en el cual un servicio no está disponible para el cliente o usuario. Si este tiempo no supera el tiempo establecido para RTO no se activa el plan de continuidad para el proceso de gestión de la Vallecaucana de Aguas S.A E.S.P Y se tratará como un incidente.

- **Punto Objetivo de Recuperación** - RPO (Recovery Point Objective): Indica la cantidad de información expresada en tiempo que la organización puede tolerar perder sin causar un impacto grave a su operación.

- **Tiempo Objetivo de Recuperación** — RTO (Recovery Time Objective): Tiempo que requiere el proceso/servicio/aplicación para restablecer la operatividad, después de un evento de desastre. Este tiempo representa la

expectativa del dueño del proceso para la recuperación de la misma y es un datode referencia para establecer estrategias de continuidad.

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

- **Disponibilidad** (Availabilify): Capacidad de un servicio o de un componente del servicio para llevar a cabo **su función requerida** en un instante determinado **o durante un** periodo de tiempo que ha sido acordado.

- **Seguridad de la Información:** Es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de Negocio. Adicionalmente se define como la preservación de la confidencialidad integridad y disponibilidad de la información. Tomado de NTC ISO/IEC 27002:2013.