Documento

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

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

Contenido

1. INTRODUCCION

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información

Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargados de velar por la protección y seguridad de sus recursos, infraestructura e información, contantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de Vallecaucana de Aguas S.A. E.S.P., el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno Digital y la norma ISO 27001 [1], los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo

2. OBJETIVOS

OBJETIVO GENERAL

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de Vallecaucana de Aguas S.A. E.S.P, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno digital, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

OBJETIVO ESPECIFICOS

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno Digital.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad

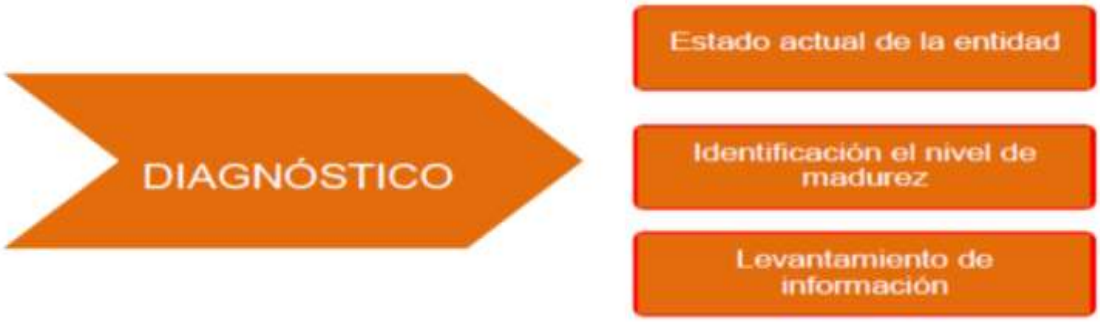
3. METODOLOGIA IMPLEMENTACION MODELO DE SEGURIDAD

3.1 CICLO OPERACIÓN

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno Digital contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información

3.2 FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información



3.3 INSTRUMENTOS DE LA FASE ETAPAS PREVIAS A LA IMPLEMENTACIÓN

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad
- Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad
- Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación

En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad

3.4 FASE DE PLANIFICACIÓN

Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad.

Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

Resultados e Instrumentos de la Fase de Planificación

Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

DESCRIPCIÓN DE FASE DE PLANIFICACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Política de seguridad y privacidad de la información. La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.

La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.

La política debe ser aprobada y divulgada al interior de la entidad.

Políticas de Seguridad y Privacidad de la Información. Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información. En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

Procedimientos de Seguridad de la Información.

En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad. Esta actividad describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

Roles y Responsabilidades de Seguridad y Privacidad de la Información.

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

Inventario de activos de información.

La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios

Identificación, Valoración Y Tratamiento de Riesgos.

La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, asi como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por Vallecaucana de Aguas S.A. E.S.P respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad. Para definir la metodología, la entidad puede hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC.

Plan de Comunicaciones.

La Entidad debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad.

Plan de transición de IPv4 a IPv6.

Para llevar a cabo el proceso de transición de IPv4 a IPv6 en las entidades, se debe cumplir con la fase de planeación establecida en la Guía No 20 - Transición de IPv4 a IPv6 para Colombia que indica las actividades específicas a desarrollar.

3.5 FASE DE IMPLEMENTACIÓN

Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

Metas, Resultados e Instrumentos de la Fase de Implementación

Metas	Resultados
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.

Con base a los resultados de la fase de planeación, en la fase de implementación deberá ejecutarse las siguientes actividades:

Planificación y Control Operacional.

La entidad debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos. La entidad debe tener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado, adicionalmente, deberá llevarse un control de cambios que le permitan tomar acciones para mitigar efectos adversos cuando sea necesario.

Implementación del plan de tratamiento de riesgos.

Se debe implementar el plan de tratamiento de riesgos de seguridad de la información, en el cual se identifica el control a aplicar para llevar cada uno de los riesgos a un nivel aceptable para la entidad.

Es preciso tener en cuenta que la aplicación del control sobre los riesgos detectados deben estar aprobados por el dueño de cada proceso.

Indicadores De Gestión.

La entidad deberá definir indicadores que le permitan medir la efectividad, la eficiencia y la eficacia en la gestión y las acciones implementadas en seguridad de la información. Los indicadores buscan medir:

- Efectividad en los controles.
- Eficiencia del MSPI al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones y la mejora continua.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumo al plan de control operacional.

Plan de Transición de IPv4 a IPv6.

Se deberá generar el documento detallado con el plan de transición e implementación del protocolo IPv6 en la entidad. Las guías de apoyo para esta labor son “Guía de Transición de IPv4 a IPv6 para Colombia” y “Guía de Aseguramiento del Protocolo IPv6”

3.6 FASE DE EVALUACIÓN DE DESEMPEÑO

El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Metas	Resultados
Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.
Plan de Ejecución de Auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

Plan de revisión y seguimiento a la implementación del MSPI.

En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

- Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
- Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.
- Seguimiento a la programación y ejecución de las actividades de autorías internas y externas del MSPI.
- Seguimiento al alcance y a la implementación del MSPI.
- Seguimiento a los registros de acciones y eventos / incidentes que podrían tener impacto en la eficacia o desempeño de la seguridad de la información al interior de la entidad.
- Medición de los indicadores de gestión del MSPI
- Revisiones de acciones o planes de mejora (solo aplica en la segunda revisión del MSPI)

Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas; deben ser medibles permitiendo analizar causas de desviación y su impacto en el cumplimiento de las metas y objetivos del MSPI

Plan de Ejecución de Auditorias

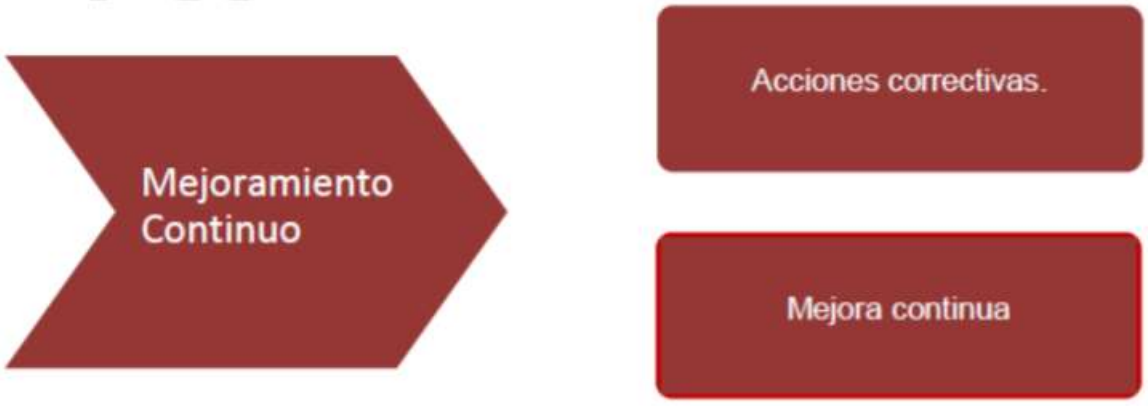
La entidad debe generar un documento donde se especifique el plan de auditorías para el MSPI, donde especifique la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Se debe llevar a cabo auditorías y revisiones independientes a intervalos planificados que permitan identificar si el MSPI es conforme con los requisitos de la organización, está implementado adecuadamente y se mantiene de forma eficaz; así mismo es necesario difundir a las partes interesadas, los resultados de la ejecución de las auditorías.

Es importante conservar la información documentada como evidencia de los resultados de las auditorías.

3.7 FASE DE MEJORA CONTINUA

En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas



Metas, Resultados e Instrumentos de la Fase de Mejora Continua

Metas	Resultados
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.

En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

- Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.
- Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

Utilizando los insumos anteriores, la entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.

4. MODELO DE MADUREZ

Este esquema permite identificar el nivel de madurez del MSPI en el que se encuentran las entidades, midiendo la brecha entre el nivel actual de la entidad y el nivel optimizado. Características de los Niveles de Madurez

Nivel	Descripción
Inexistente	Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad. No se reconoce la información como un activo importante para su misión y objetivos estratégicos. No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	Se han identificado las debilidades en la seguridad de la información. Los incidentes de seguridad de la información se tratan de forma reactiva. Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sob
Repetible	Se identifican en forma general los activos de información. Se clasifican los activos de información. Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión. La entidad cuenta con un plan de diagnóstico para IPv6.

Definido	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. La Entidad tiene procedimientos formales de seguridad de la Información. La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. La Entidad ha realizado un inventario de activos de información aplicando una metodología. La Entidad trata riesgos de seguridad de la información a través de una metodología. Se implementa el plan de tratamiento de riesgos. La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	Se revisa y monitorea periódicamente los activos de información de la Entidad. Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. Se utilizan indicadores de efectividad para establecer si la entidad.

PRIVACIDAD DE LA INFORMACIÓN

Uno de los objetivos del modelo de seguridad y privacidad de la Información es el de garantizar un adecuado manejo de la información pública en poder de las entidades destinatarias, la cual es uno de los activos más valiosos para la toma de decisiones, el modelo propende por un doble enfoque a saber: a nivel de seguridad marcando un derrotero para que las entidades destinatarias construyan unas políticas de seguridad sobre la información a fin de salvaguardar la misma a nivel físico y lógico, de manera que se pueda en todo momento garantizar su integridad, disponibilidad y autenticidad. En esa línea el aseguramiento de los procesos relacionados con los sistemas de información debe complementarse con un enfoque de privacidad para garantizar tanto la protección de los derechos a la intimidad y el buen nombre o la salvaguarda de secretos profesionales, industriales o de información privilegiada de particulares en poder de la

administración como el acceso a la información pública cuando esta no se encuentre sometida a reserva.

Para ello se requiere dotar al modelo de seguridad de la información de un componente específico relacionado con la privacidad. Para que los servidores públicos entiendan mejor el concepto de privacidad, hay que tener claro que diferentes procesos relacionados con la recolección y uso de información son susceptibles de ser objeto de implementación de medidas de privacidad, como puede ser:

- La Implementación de un sistema de información que tenga la posibilidad de recolectar datos personales, tal como un sistema de seguridad a través de video vigilancia que capture imágenes, datos biométricos, etc.
- El Diseño y ejecución de un sistema de gestión documental
- El Desarrollo de políticas que impliquen la necesidad de recolectar y usar información personal, como por ejemplo políticas de atención de PQR´s
- La Transferencia de información a terceros (otras entidades o países). Para ello la entidad debe tener en cuenta los siguientes temas.

Contar con una herramienta de análisis sobre impacto en la privacidad El MSPI es el instrumento que se pone a disposición de las entidades con el fin de realizar el análisis de impacto que en la privacidad de la información pueda presentarse a partir del desarrollo de las funciones administrativas o el desarrollo misional de cada entidad, teniendo como referente:

- El marco legal vigente.
- Las necesidades de los clientes internos y externos de la entidad.
- La identificación de los posibles problemas recurrentes relacionados con la privacidad.

Descripción de los flujos de información La descripción de los flujos de información sirve para saber qué información está siendo recolectada, con qué propósito, cómo, en qué cantidad y si la misma es objeto de divulgación. La fase de diagnóstico de privacidad puede servir como insumo al poder identificar qué información se tiene, dónde y en cabeza de quién. Este ejercicio tiene que ser complementado con la documentación de los procesos relacionados con gestión de la información que la entidad haya levantado, para poder hacer una valoración sobre la circulación de la información, identificando que en la misma no se afecten derechos de los titulares de información o se ponga en riesgo su privacidad.

Identificar los riesgos de privacidad

Los riesgos en relación con la privacidad pueden ser de varios tipos:

En relación con la información personal de los individuos

- Se expone información clasificada (datos personales no públicos) sin que medie autorización para ello.
- Uso de sistemas de información o aplicaciones en la interacción con los ciudadanos que pueden ser intrusivos sobre su privacidad sin advertir previamente a los usuarios sobre ello (geolocalización)
- Información que permanece en poder de la entidad por más tiempo de la vigencia que tiene la base de datos o en contra del ejercicio de derecho de supresión por parte del titular-ciudadano.

En relación con la información de usuarios institucionales

- Se divulga información que puede ser clasificada como secreto industrial o que pone en riesgo la imagen corporativa.

En relación con los sistemas de información y programas usados o los procedimientos y procesos relacionados con la gestión administrativa a cargo.

- Procesos no ajustados al sistema de gestión documental que garanticen medidas de protección sobre la información.
- Adquisición de programas que no garanticen un nivel adecuado de privacidad, por ejemplo que permitan recolección masiva de datos sin conocimiento de los usuarios.
- Indebida utilización de datos personales en ejercicios de divulgación tales como procesos de rendición de cuentas, publicación de información en la página web, etc.

El análisis debe reflejarse en una matriz de riesgos ponderando la probabilidad de su ocurrencia (ejemplo: baja-intermedia-alta) y el impacto que puede generar su causación (se sugiere utilizar una tabla numérica, por ejemplo - 1 ningún impacto a 10 impacto considerable).

La implementación del componente de privacidad sigue el mismo ciclo de operación adoptado para seguridad de la información consistente en cinco fases o etapas así: diagnóstico, planeación, implementación, gestión y mejora continua.

FASE DIAGNÓSTICO

En esta fase es necesario que las entidades identifiquen cómo se está garantizando la privacidad sobre todo el ciclo de la información que tienen en su poder verificando la implantación o no de medidas que den cumplimiento a los requerimientos de las normas sobre protección de datos personales y que, adicionalmente contribuya a identificar la información pública sometida a reserva o clasificada en los términos de la Ley.

Para ello se pone a disposición de las entidades, el instrumento de diagnóstico y seguimiento a la implementación. A través del diligenciamiento de este instrumento se podrá conocer la realidad de la información relacionada con el manejo de los activos de la información que reposen en bancos de datos o archivos y a partir de allí determinar las medidas a nivel procedimental que deben adelantar las entidades para otorgar un nivel adecuado de protección a esta información.

Metas, Resultados e Instrumentos de la Fase de Diagnostico

Metas	Resultados
Diagnostico	• Realizar el diagnóstico de las condiciones en que se encuentran los activos de información administrados por la entidad. • Diligenciamiento de la herramienta. • Documento con el resultado del diagnóstico realizado por la entidad con la clasificación y distinción de los activos de información teniendo en cuenta la información con datos personales y aquellos que no lo son identificando la criticidad de la información clasificada o reservada.

Con el resultado del diagnóstico se puede contar con un insumo frente a la identificación de aquella información que debe ser manejada como privada (clasificada en los términos de la Ley) para a partir de allí incorporar las medidas de seguridad proporcionales a su naturaleza como los procedimientos que lleven al cumplimiento de la normatividad de protección de datos, transparencia y acceso a la información pública soportado todo ello en la incorporación de un sistema de privacidad por diseño que responda a la realidad presupuestal, humana y técnica de cada entidad

FASE PLANIFICACIÓN

En esta segunda etapa se debe trazar la estrategia con el objetivo de organizar el trabajo adelantado por la entidad a partir de las características recogidas en la fase de diagnóstico, para acercarlas a un nivel de cumplimiento adecuado para salvaguardar la información privada y de manera concomitante responder a los retos de disponibilidad a la información pública por parte de la ciudadanía, así como para ajustar los roles del personal designado para cumplir con las responsabilidades de seguridad y privacidad de la información.

Metas, Resultados e Instrumentos de la Fase de Planificación

Metas	Resultados
Planificación	• Documento con la política de privacidad, debidamente Manual de políticas de seguridad y privacidad de la información, aprobada por la alta dirección y socializada al interior de la entidad. • Documento con el plan de gestión de la privacidad sobre la información, aprobado por la alta dirección de la entidad. • Definición de roles en relación con la Información. • Procedimientos de privacidad. • Plan de capacitación al interior de la entidad aprobada por la alta dirección y socializada al interior de la entidad

FASE DE IMPLEMENTACIÓN

En esta fase se deben ejecutar las acciones trazadas en la etapa previa de planeación de manera que la entidad diseñe un modelo de privacidad que le permita cumplir con los mínimos legales y generar una política privacidad que le permita la correcta gestión de la información.

Metas, Resultados e Instrumentos de la Fase de Implementación

Metas	Resultados
Implementación	• Documento con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del plan de gestión de la privacidad de la información • Documento que evidencie el registro de las Bases de datos, • Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados

FASE DE EVALUACIÓN DEL DESEMPEÑO

Una vez implementadas las anteriores actividades el modelo de privacidad se evalúa, para medir la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI y la aplicación de la Ley de Transparencia y Acceso a la Información Pública.

Metas, Resultados e Instrumentos de la Fase de Evaluación de Desempeño

Metas	Resultados
Evaluación del desempeño	• Documento con los resultados del plan de seguimiento · Documento con el Plan de auditoría interna y resultados revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces • Comunicación de los indicadores al público a través de la rendición de cuentas, informe a la PGN y al Congreso de la República.

FASE DE MEJORA CONTINUA

Una vez se tengan los resultados del componente de evaluación del desempeño se toman los resultados obtenidos y se preparan los correctivos necesarios que permitan a la misma crecer en el nivel de responsabilidad demostrada.

Metas	Resultados

Mejora Continua	• Documento con los resultados del plan de seguimiento • Documento con los resultados del plan de mejoramiento revisado y aprobado por el Comité de Gestión Institucional o el que haga sus veces. • Documento con el consolidado de las auditorias.

ADOPCIÓN DEL PROTOCOLO

IPv6 En el presente capitulo se relacionan las fases para el proceso de transición del protocolo IPv4 a IPv6 que orientará a las entidades del gobierno y a la sociedad en general en el análisis, la planeación y la implementación del protocolo IPv6.

FASE DE PLANEACIÓN

En esta fase, se debe definir el plan y la estrategia de transición de IPv4 a IPv6, en procura de los resultados que permitan dar cumplimiento con la adopción del nuevo protocolo.

Metas, Resultados e Instrumentos de la Fase de Planeación

Metas	Resultados
Plan y estrategia de transición de IPv4 a IPv6.	• Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de cada Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones , de cómputo y almacenamiento con el cumplimiento de IPv6, plan de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (Readiness) de los sistemas de comunicaciones, bases de datos y aplicaciones. • Documento que define la estrategia de para la implementación y aseguramiento del protocolo IPv6 en concordancia con la política de seguridad de las entidades.

FASE DE IMPLEMENTACIÓN

En esta fase se realizan actividades tales como habilitación del direccionamiento de IPv6, montaje, ejecución y corrección de configuraciones para pruebas piloto, activar las políticas de seguridad de IPv6, validar la funcionalidad de los servicios y aplicaciones de las entidades, entre otras.

Metas, Resultados e Instrumentos de la Fase de Implementación

Metas	Resultados
Implementación del plan y estrategia de transición de IPv4 a IPv6.	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

PRUEBAS DE FUNCIONALIDAD

En esta fase se hacen pruebas de funcionalidad y/o monitoreo de IPv6, en sistemas de información, de almacenamiento, de comunicaciones y servicios; frente a las políticas de seguridad perimetral, de servidores de cómputo, equipos de comunicaciones, de almacenamiento, entre otros. Tener en cuenta que se debe elaborar un inventario final de servicios y sistemas de comunicaciones, bajo el nuevo esquema de funcionamiento de IPv6.

Metas, Resultados e Instrumentos de la Fase de Pruebas de Funcionalidad.

Metas	Resultados
Plan de pruebas de funcionalidad de IPv4 a IPv6.	Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II de Implementación. Acta de cumplimiento a satisfacción de la Entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II de la implementación. Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo IPv6.

5. CLASIFICACION DE LA INFORMACION

OBJETIVO

Brindar a los funcionarios de Vallecaucana de Aguas S.A E.S.P, que tienen bajo su responsabilidad la clasificación de la información, un instrumento para determinar el nivel de criticidad y el valor de la información, con el fin de identificar los controles de seguridad requeridos para salvaguardarla adecuadamente, así como los controles y autorización de acceso por parte de los funcionarios y terceras personas que apoyan las actividades de Vallecaucana de Aguas S.A E.S.P.

ALCANCE

Se aplica a todos los procesos de la institución.

DEFINICIONES

Titular de la información: Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la normatividad vigente ley.

Usuario: El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos.

Dato personal: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados.

Dato público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato Reservado: Es reservado el dato que no tiene naturaleza íntima, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Datos personales sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Información: Hace referencia a los datos tratados que se encuentran en forma digital o no digital Se empleará como base para esta metodología la definición de la familia de normas ISO 27000 y la Información en forma digital o no digital creada, procesada, almacenada, archivada o borrada durante la ejecución de procesos misionales; por ejemplo: Bases de datos, registros, correos

electrónicos, código fuente, documentos en papel, diseños, datos procesados, listas de contactos, calendarios, imágenes y toda aquella información que se considere con valor para el Vallecaucana de Aguas S.A. E.S.P .

Por otra parte, la ley 1712/2014, la define como: "Un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen".

Información pública reservada: De acuerdo a la ley 1712/2014 se define como: "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley".

Información pública clasificada: De acuerdo a la ley 1712/2014 se define como: "Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley".

Información privada: La jurisprudencia de la Corte Constitucional, en Sentencia T-729 de 2002, hace referencia a la información privada de la siguiente manera:

> *"La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio* ".

RESPONSABILIDAD

Titular de la Información.

- Actualizar y rectificar sus datos personales frente al Responsable del Tratamiento o Encargados del Tratamiento, cuando sea necesario.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato, cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

Responsable del Tratamiento.

- Decidir sobre las bases de datos y/o el tratamiento de los datos.
- Dar a conocer, actualizar y rectificar los datos personales de los titulares de acuerdo con los requerimientos de los mismos.
- - Entregar las pruebas de la autorización otorgada por el titular de los datos, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el Artículo 10 de la Ley 1581 de 2012.
- Informar al propietario de la información del tratamiento de sus datos personales, previa solicitud.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la Ley 1581 de 2012, copia de la respectiva autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al encargado del tratamiento sea verás, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley 1581 de 2012.
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados, en los términos señalados en la Ley 1581 de 2012.
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos, cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Responsable de la producción de la información

- Tiene responsabilidad aprobada por el nivel directivo del VALLECAUCANA DE AGUAS S.A. E.S.P para controlar la generación, clasificación, desarrollo, mantenimiento, uso y protección adecuada de la información.
- Identificar todas las fuentes de información, concientizar a sus funcionarios sobre la importancia de la clasificación de la información para la adecuada operación del VALLECAUCANA DE AGUAS S.A. E.S.P.
- Asegurar que se cumplan los controles para preservar la confidencialidad, la integridad y la disponibilidad de la información.
- Tomar decisiones esenciales de costo beneficio para lograr el cumplimiento de los objetivos de la entidad.
- Mantener un nivel apropiado de protección física y lógica sobre la información.
- Revisar periódicamente la clasificación de la información.
- Asegurar la disponibilidad de la información en todo momento.
- Revisar periódicamente la efectividad de los controles sobre la información.
- Definir y revisar periódicamente las restricciones de acceso y niveles de clasificación de la información, considerando las políticas definidas por el Comité de Sistemas del VALLECAUCANA DE AGUAS S.A. E.S.P.
- Determinar y revisar periódicamente el esquema de respaldo y restauración de la información.

Encargado del Tratamiento

- Tiene la responsabilidad de tratar los datos personales sobre las bases de datos y/o fuentes de información.
- Dar a conocer, actualizar y rectificar los datos personales de los titulares de acuerdo con los requerimientos de los mismos y lo indicado por el responsable del tratamiento.
- Informar al propietario de la información del tratamiento de sus datos personales previa solicitud, de acuerdo con lo indicado por el responsable del tratamiento.
- Garantizar al titular, en todo tiempo el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos personales en los términos de la Ley 1581 de 2012.
- Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- Tramitar las consultas y los reclamos sobre datos personales formulados por los titulares en los términos señalados en la Ley 1581 de 2012

- Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley 1581 de 2012.
- Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información, únicamente a las personas que pueden tener acceso a ella de acuerdo con los procedimientos establecidos
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

Consultado.

- Verificar los niveles, categorías o tipos de clasificación de la información y sus actualizaciones.
- Definir los criterios para la clasificación de la información y los procedimientos de manejo en conjunto con los propietarios de la información.
- Decidir sobre casos en los que se tengan dudas sobre la clasificación de un cierto tipo de información.
- Apoyar a los Propietarios de la Información en la determinación de los requerimientos de protección y mecanismos de control de cada categoría de clasificación.

Informado.

- Conocer los tipos de clasificación de la información y las normas concernientes a él.
- Divulgar y aplicar las normas de clasificación de la información establecidas por el VALLECAUCANA DE AGUAS S.A. E.S.P.

Responsable de la Información.

- Responsable de proteger la información, manteniendo los controles definidos por el dueño de la información.
- Obtener aprobación del propietario de la información antes de realizar la divulgación de la misma.
- Realizar y aprobar las copias de respaldo de la información para garantizar su disponibilidad.
- Realizar restauraciones de las copias de respaldo.
- Implementar los controles de acceso definidos o aprobados por el propietario de la información.

- Realizar las tareas administrativas propias de su cargo con la información bajo su custodia.

Usuario Final (Funcionarios VALLECAUCANA DE AGUAS S.A. E.S.P).

- Recibir y dar un buen uso al activo de información asignado.
- Orientar a los jefes de dependencia en la clasificación de la información.
- Garantizar la confidencialidad de la información que conoce, de acuerdo a sus responsabilidades y funciones.
- Firmar las actas y documentos relacionados con los activos de información.
- Colaborar con los jefes de dependencia a mantener actualizada la matriz de activos de información, las aplicaciones asociadas y la clasificación de la información a su cargo.
- Contribuir con la disposición final de la información, acorde con el manual de gestión de correspondencia y archivos oficiales y con las Tablas de Retención Documental.

GENERALIDADES

Las áreas del VALLECAUCANA DE AGUAS S.A. E.S.P deberán clasificar su información de acuerdo a su valor y criticidad. Esta clasificación debe realizarse de acuerdo a las necesidades que tiene el área de compartir o restringir la información, los requerimientos de seguridad en términos de confidencialidad, integridad y disponibilidad, y con base al impacto que pudiera provocar en términos económicos, operativos, legales e imagen institucional.

El dueño o propietario de la información, será el responsable de definir la categoría en la que cada activo de información se encuentra, así como determinar si es necesario un proceso de reclasificación y los controles requeridos para su protección.

Para la clasificación de la información el VALLECAUCANA DE AGUAS S.A. E.S.P adoptará el siguiente esquema:

- Pública: El VALLECAUCANA DE AGUAS S.A. E.S.P establece que la información pública es aquella que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica. Esta información puede ser entregada o publicada sin restricciones a terceros, funcionarios o cualquier persona sin ocasionar daños a terceros ni a los procesos de negocio del VALLECAUCANA DE AGUAS S.A. E.S.P.

- Confidencial: El VALLECAUCANA DE AGUAS S.A. E.S.P establece que la información confidencial es toda aquella que no es pública. Y a la información pública solo pueden tener acceso las personas que han sido declaradas usuarios legítimos de esta información con privilegios asignados, como se expresa en los activos de información.

Los niveles de confidencialidad de los activos de información del VALLECAUCANA DE AGUAS S.A. E.S.P son los siguientes:

- Uso Interno: Es la información que es utilizada por el VALLECAUCANA DE AGUAS S.A. E.S.P para realizar sus labores en los procesos y que no puede ser utilizada por terceros sin autorización del propietario del activo de información. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera leve a los procesos de la entidad.
- Restringida: Información que es utilizada por solo un grupo de funcionarios del VALLECAUCANA DE AGUAS S.A. E.S.P para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin previa autorización del propietario del activo de información. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera importante a los procesos de la entidad.
- Altamente Restringida: Información que es utilizada por solo un grupo de funcionarios del VALLECAUCANA DE AGUAS S.A. E.S.P para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin previa autorización del VALLECAUCANA DE AGUAS S.A. E.S.P. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera grave a los procesos de la entidad.

Toda la información que se maneja dentro de cada una de las Áreas tendrá carácter de CONFIDENCIAL hasta que se apruebe otro tipo de clasificación.

Etiquetado y manejo de la información:

- Los documentos con información del tipo “restringida” deberán ser controlados por medio de copias individuales perfectamente numeradas y registro de las personas que han tenido acceso.
- La copia o transferencia de información “restringida” por cualquier medio (electrónico, magnético, en papel) deberá estar autorizada y controlada.
- Todos los documentos del tipo “Altamente Restringida” se deberán conservar bajo llave y en lugares seguros.
- El envío de documentos con clasificación Confidencial (De Uso Interno, Restringida y Altamente Restringido), se deberá hacer por medio de canales seguros tales como mensajería privada, correo electrónico cifrado o entrega personal. En caso de hacerse por

medio de forma física, los paquetes deberán estar debidamente cerrados y que sea imposible observar su contenido.

- Toda recepción de información confidencial deberá solicitar acuse de recibo.
- En caso de ser necesario, se considerará un procedimiento o centro de destrucción de documentos y activos de información que garantice la no reutilización de la información. La destrucción de registros e información del VALLECAUCANA DE AGUAS S.A. E.S.P debe ser formalmente autorizada por el responsable.
- La información Confidencial (De Uso Interno, Restringida y Altamente Restringido) deberá reflejar por medio de una leyenda, la clasificación a la que pertenece
- El VALLECAUCANA DE AGUAS S.A. E.S.P, a través de sus instancias correspondientes, se reserva el derecho de iniciar denuncias, y procesos disciplinarios para sancionar a los funcionarios que divulguen o destruyan ilícitamente la información de la entidad.

Se deben tener en cuenta los siguientes lineamientos o controles para el manejo y transporte de información confidencial.

- Política de control de acceso a la información
- Proceso Disciplinario
- Propiedad de los activos
- Devolución de Activos
- Clasificación de la información
- Etiquetado de la información
- Manejo de Activos
- Transferencia de medios físicos

NORMATIVIDAD

TIPO	NUMERO	NOMBRE	FECHA
Ley	1712	Ley de Transparencia y Acceso a la Información Pública Objeto. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.	6 Marzo / 2014
		Ley Habeas Data La cual "dicta disposiciones generales del Habeas Data y se	

Ley	1266	regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países"	31 Dic. / 2008
Ley	1581	Ley de Protección de Datos Por la cual se desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.	31 Oct / 2012

6. SEGURIDAD EN LA RED DE DATOS

Introducción

- Disponibilidad: Se requiere que la información esté disponible en el momento exacto para quienes están autorizados a acceder a ella

Ataques a la seguridad de la red

Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos a saber:

Ataques pasivos: Son oidores o monitores de las transmisiones. El objetivo de quienes realizan ese tipo de ataque es obtener la información que se está transmitiendo. En este tipo de ataque se pueden encontrar:

- Divulgación del contenido de un mensaje: es un tipo de ataque pasivo por medio del cual el atacante se entera de la información transmitida; como por ejemplo escuchar una llamada telefónica, leer un correo electrónico abierto.
- Análisis de Tráfico: Este tipo de ataque pasivo se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que está siendo transmitido aun cuando esté protegido por medio de cifrado.

Ataques activos: Suponen modificación de los datos o creación de flujos de datos falsos. Dentro de este tipo de ataques se pueden encontrar:

Norma ISO 17799

- Enmascaramiento: Es un tipo de ataque activo que tiene lugar cuando una entidad pretende suplantar a otra para obtener información confidencial.
- Repetición: Se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.
- Modificación de Mensajes: Se modifican los mensajes para producir efectos no autorizados.
- Denegación de Servicios: Previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin específico o para obtener perturbaciones sobre la red desmejorando su rendimiento o incluso inhabilitando la misma.

Herramientas de seguridad

Existen métodos o herramientas tecnológicas que ayudan a las organizaciones a mantener segura la red. Estos métodos, su utilización, configuración y manejo dependen de los requerimientos que tenga la organización para mantener la red en un funcionamiento óptimo y protegido contra los diferentes riesgos. Los más utilizados son:

Autenticación: Identifica quien solicita los servicios en una red. Esta no hace referencia solo a los usuarios sino también a la verificación de un proceso de software.

Autorización: Indica que es lo que un usuario puede hacer o no cuando ingresa a los servicios o recursos de la red. La autorización otorga o restringe privilegios a los procesos y a los usuarios.

Auditoria: Para analizar la seguridad de una red y responder a los incidentes de seguridad, es necesario hacer una recopilación de datos de las diferentes actividades que se realizan en la red, a esto se le llama contabilidad o auditoria. Con normas de seguridad estrictas la auditoria debe incluir una bitácora de todos los intentos que realiza un usuario para lograr conseguir la autenticación y autorización para ingresar a la red. También debe registrarse los accesos anónimos o invitados a los servidores públicos, así como registrar los intentos de los usuarios para cambiar sus privilegios.

Cifrado: Es un proceso que mezcla los datos para protegerlos de su lectura, por parte de otro que no sea el receptor esperado. Un dispositivo de cifrado encripta los datos colocándolos en una red. Esta herramienta constituye una opción de seguridad muy útil, ya que proporciona confidencialidad a los datos. Se recomienda el cifrado de datos en organizaciones cuyas redes se conectan a sitios privados a través de Internet mediante redes privadas virtuales.

Filtros de paquete: Se pueden configurar en routers o servidores para rechazar paquetes de direcciones o servicios concretos. Los filtros de paquete ayudan a proteger recursos de la red del uso no autorizado, destrucción, sustracción y de ataques de denegación del servicio. Las normas de seguridad deben declarar si los filtros implementan una de las siguientes normas:

- Denegar tipos específicos de paquetes y aceptar todo lo demás
- Aceptar tipos específicos de paquetes y denegar todo lo demás.

Firewalls: Es un sistema o combinación de sistemas, que exige normas de seguridad en la frontera entre dos o más redes.

Vlan: En una red LAN se utilizan los switches para agrupar estaciones de trabajo y servidores en agrupaciones lógicas.

En las redes, las VLAN se usan para que un conjunto de usuarios en particular se encuentre agrupado lógicamente.

Las VLAN permiten proteger a la red de potenciales problemas conservando todos los beneficios de rendimiento.

Detección de Intrusos: Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar debilidades en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación. . Una intrusión significa:

- Acceder a una determinada información.
- Manipular cierta información.
- Hacer que el sistema no funcione de forma segura o inutilizarlo.
- Un routers (*enrutador*) es un dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI.
- Un firewall (cortafuegos), es un elemento de hardware o software utilizado en una red de computadores para prevenir algunos tipos de comunicaciones prohibidos según las política de red que se hayan definido en función de las necesidades de la organización responsable de la red.
- Un switche (conmutador) es un dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Seguridad de redes: Es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos:

Esto puede incluir:

- Evitar que personas no autorizadas intervengan en el sistema con fines malignos
- Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema
- Asegurar los datos mediante la previsión de fallas
- Garantizar que no se interrumpan los servicios

Las causas de inseguridad: Generalmente, la inseguridad puede dividirse en dos categorías:

Estado de inseguridad activo: es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita).

Estado pasivo de inseguridad: es decir, cuando el administrador (o el usuario) de un sistema no está familiarizado con los mecanismos de seguridad presentes en el sistema.

El objetivo de los atacantes (también denominados "piratas" o "hackers"):

- La atracción hacia lo prohibido
- El deseo de obtener dinero (por ejemplo, violando el sistema de un banco)
- La reputación (impresionar a sus amigos)
- El deseo de hacer daño (destruir datos, hacer que un sistema no funcione)

El comportamiento del atacante: Frecuentemente, el objetivo de los atacantes es controlar una máquina para poder llevar a cabo acciones deseadas. Existen varias formas de lograr esto:

- Obteniendo información que puede utilizarse en ataques
- Explotando las vulnerabilidades del sistema
- Forzando un sistema para irrumpir en él

¿Cómo es posible protegerse?

- Manténganse informado
- Conozca su sistema operativo
- Limite el acceso a la red (firewall)
- Limite el número de puntos de entrada (puertos)
- Defina una política de seguridad interna (contraseñas, activación de archivos ejecutables)
- Haga uso de utilidades de seguridad (registro)

Control de Seguridad de la Red

Control de uso de puntos de red de datos (Red de Área Local – LAN).

Objetivo: Asegurar la operación correcta y segura de los puntos de red.

Aplicabilidad: Estas son reglas que aplican todos los procesos del Vallecaucana de Aguas S.A. E.S.P.

Directrices:

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar.
- Los equipos de uso personal, que no son de propiedad del VALLECAUCANA DE AGUAS S.A. E.S.P. solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Área de la Oficina de Información del VALLECAUCANA DE AGUAS S.A. E.S.P .
- La instalación, activación y gestión de los puntos de red es responsabilidad de la Oficina de Información.

Seguridad del centro de datos y centros de cableado

Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Aplicabilidad: aplican a los funcionarios, contratistas, colaboradores del VALLECAUCANA DE AGUAS S.A. E.S.P actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática, Data Center.

Directrices:

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- El Área de Información y Sistemas debe garantizar que el control de acceso al centro de datos del VALLECAUCANA DE AGUAS S.A. E.S.P, cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.

- La Oficina de Informacion deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de un funcionario de la Oficina de Información del VALLECAUCANA DE AGUAS S.A. E.S.P.
- El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

El centro de datos debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- Pisos elaborados con materiales no combustibles.
- Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el Comité de Seguridad Informática y de Sistemas y exclusivamente con fines institucionales.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado del VALLECAUCANA DE AGUAS S.A. E.S.P.
- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
- Cuando se requiera realizar alguna actividad sobre algún armario (*rack*), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

Seguridad de los Equipos de Computo

Objetivo: Asegurar la protección de la información en los equipos.

Aplicabilidad: Aplican todos los procesos del Vallecaucana de Aguas S.A. E.S.P.

Directrices:

- Protecciones en el suministro de energía: A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el área Administrativa.

- Seguridad del cableado: Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- Deben existir planos que describan las conexiones del cableado.
- El acceso a los centros de cableado (Racks), debe estar protegido.
- Mantenimiento de los Equipos**:** El VALLECAUCANA DE AGUAS S.A. E.S.P debe mantener contratos de soporte y mantenimiento de los equipos críticos.
- Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
- Los equipos que requieran salir de las instalaciones del VALLECAUCANA DE AGUAS S.A. E.S.P para reparación o mantenimiento, deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo a los niveles de clasificación de la información.
- Para que los equipos puedan salir fuera de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior del VALLECAUCANA DE AGUAS S.A. E.S.P.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

Ingreso y retiro de activos de información de terceros.

- El retiro e ingreso de todo activo de información de propiedad de los usuarios del VALLECAUCANA DE AGUAS S.A. E.S.P, utilizados para fines personales, se realizará mediante los procedimientos establecidos por la Administración del Edificio.
- El VALLECAUCANA DE AGUAS S.A. E.S.P no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica del Departamento.
- El retiro e ingreso de todo activo de información de los visitantes que presten servicios al VALLECAUCANA DE AGUAS S.A. E.S.P (consultores, pasantes, visitantes, etc.) será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información.
- El traslado entre dependencias del VALLECAUCANA DE AGUAS S.A. E.S.P de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

Establecimiento, uso y protección de claves de acceso.

Objetivo: Controlar el acceso a la información.

Aplicabilidad: Aplican todos los procesos del Vallecaucana de Aguas S.A. E.S.P.

Directrices:

- Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le signen para la utilización de los equipos o servicios informáticos de la Entidad.
- Los usuarios deben tener en cuenta los siguientes aspectos:
  - No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo, almacenadas en un macro o en una clave de función.
  - El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.

- Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
- Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.
- La clave de acceso será desbloqueada sólo por el PUC (Punto Único de Contacto, luego de la solicitud formal por parte del responsable de la cuenta. Para todas las cuentas especiales, la reactivación debe ser documentada y comunicada al PUC.
- Las claves o contraseñas deben: Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Tener mínimo diez caracteres alfanuméricos.
- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Cambiarse obligatoriamente cada 30 días, o cuando lo establezca el Área de la Oficina de Información.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- No ser reveladas a ninguna persona, incluyendo al personal del Área de Información y Sistemas.
- No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

Vallecaucana de Aguas S.A. E.S.P. en cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 que regulan la recolección y tratamiento de los datos de carácter personal, y establece las garantías legales que deben cumplir todas las personas en Colombia para el debido

tratamiento de la información, expide la siguiente norma que desarrolla la política de seguridad de la información para el manejo y preservación de datos personales dentro de la entidad.

Definición de Términos:

Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P: red de comunicaciones que conecta todos los ordenadores y dispositivos de red del VALLECAUCANA DE AGUAS S.A. E.S.P entre ellos y con Internet.

Usuarios de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P: estudiantes, profesores, investigadores, personal, usuarios de las instituciones conectadas y en general cualquier persona que por su relación con el VALLECAUCANA DE AGUAS S.A. E.S.P tenga derecho a usar la Red de datos.

Normas de Uso Aceptable y Seguridad: documento que recoge la normativa orientada a lograr el uso correcto y seguro de una red en un determinado ámbito.

Instituciones conectadas a través de la red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P: toda institución que se encuentre directamente conectada a la red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P.

La Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P conecta los ordenadores y otros dispositivos susceptibles de ser conectados dentro de su plataforma entre ellos y con otras redes de investigación y comerciales como por ejemplo Internet.

La finalidad de esta interconexión es dotar a los usuarios de la red de los medios necesarios para la realización de las tareas misionales, de investigación, docente y administrativa.

Oficina coordinadora de Gestión de la Información, previa petición del usuario, proporciona conexión a la Red de Datos del VALLECAUCANA DE AGUAS S.A. E.S.P y a los servicios que en ella se ofrecen como pueden ser, correo electrónico, acceso a internet, etc.

El uso de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P deberá:

- Respetar los fines para los que ha sido creada.

- Evitar la interrupción de los servicios que ofrece o de otros equipos que forman parte de la infraestructura de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P
- Evitar interferencias e interrupciones en el trabajo de otros usuarios de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P
- Evitar situaciones que afecten a la seguridad de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P y a sus usuarios.
- Respetar el contenido de las leyes y demás disposiciones normativas y legales a nivel nacional.
- Respetar dentro del campus del VALLECAUCANA DE AGUAS S.A. E.S.P el rango de radiofrecuencias entre los 2.4 y 5 GHz para uso de la red inalámbrica

Ámbito de aplicación**:** Las normas contenidas en este documento serán de aplicación a todos los usuarios e instituciones de la red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P en tanto en cuanto hagan uso de la red y de los servicios ofrecidos.

Las instituciones conectadas a la red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P deben tener sus propias Normas de uso y seguridad de la red dentro del contexto de los servicios que ofrece a sus usuarios. Dichas Normas deberán ser compatibles con las condiciones y términos expresados en el presente documento.

Los usuarios e instituciones serán informados de estas Normas de Uso Aceptable y Seguridad y aceptan que la oficina coordinadora de Gestión de la Información sea el ente, responsable del cumplimiento de las mismas.

La Oficina de Información podrá proponer al Consejo de Administración del VALLECAUCANA DE AGUAS S.A. E.S.P modificaciones a este documento para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades para los que se creó la red y que se describen en el punto de *Seguridad de la información en la Red*. Los usuarios e instituciones serán puntualmente informados de cualquier modificación que fuera preciso introducir.

Términos y condiciones**:** Para garantizar y optimizar el funcionamiento de la Red de Datos del VALLECAUCANA DE AGUAS S.A. E.S.P, es necesaria una serie de compromisos entre los usuarios y los responsables de la red.

La Oficina Coordinadora de Gestión de la Información debe asegurar:

- Conectividad a la Red de Datos del VALLECAUCANA DE AGUAS S.A. E.S.P a todos los usuarios de la institución, cumpliendo siempre con las normas de uso y seguridad.
- Acceso a los servicios que están detallados en el Catálogo de Servicios ofrecidos por Oficina de Información en los términos recogidos en el mismo.
- La salvaguardia del espectro de radiofrecuencias entre 2.4 y 5 GHz que utiliza la red inalámbrica.

Los compromisos por parte de los usuarios de la Red de Datos del VALLECAUCANA DE AGUAS S.A. E.S.P son los siguientes:

- Hacer buen uso de la Red de datos institucional.
- No interferir con el espectro de radiofrecuencias entre 2.4 y 5 GHz que utiliza la red inalámbrica.
- Cumplir las normas de seguridad definidas en el punto de **Seguridad de la información en la Red**.
- No utilizar su conexión a la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P para proporcionar tráfico a terceras personas o entidades, salvo por expreso consentimiento de los organismos responsables de la red.
- No solicitar más recursos de los que a corto o medio plazo vayan a ser utilizados.
- Comunicar los problemas que surjan al HelpDesk de la Oficina de Información para su resolución.
- Utilizar correctamente los recursos que se le suministran.

Normas de seguridad: La conexión de un ordenador a la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P conlleva ciertos riesgos desde el momento en que dicho equipo se conecte a Internet.

Desde Internet llegan diariamente ataques, virus, gusanos, etc., y para minimizar los riesgos los usuarios del VALLECAUCANA DE AGUAS S.A. E.S.P deben cumplir las siguientes normas de seguridad:

- Todo computador o dispositivo móvil conectado a la red del VALLECAUCANA DE AGUAS S.A. E.S.P deberá estar protegido por una contraseña suficientemente robusta, es decir, no trivial o evidente.
- Deben aplicarse periódicamente todas las actualizaciones de seguridad para el sistema operativo que esté usando. Esta tarea es fácilmente automatizable en la mayoría de los casos.
- Si su sistema operativo es Windows o Macintosh, debe instalarse el antivirus institucional proporcionado por el Vallecaucana de Aguas S.A. E.S.P.
- No compartir carpetas sin contraseña.

Además de las anteriores normas, se recomienda:

- Instalar solo el software que vaya a necesitar.
- En la medida de lo posible sustituir los protocolos que no encriptan las contraseñas por otros que si las encripten. Por ejemplo, si se usa telnet, sustituirlo por ssh.
- No instalar servicios de red que no se vayan a usar.

Uso aceptable: Los usuarios de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P utilizarán la infraestructura de la red de esta institución para el intercambio de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa.

Los usuarios de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P deberán utilizar eficientemente la red con el fin de evitar, en la medida de lo posible, la congestión de la misma.

Uso no aceptable**:** La infraestructura y servicios ofrecidos por la red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P no deben usarse para:

- Cualquier transmisión de información o acto que viole la legislación vigente.

- Fines privados, personales o lúdicos (Juegos, música, videos).
- La creación o transmisión de material que cause cualquier tipo de molestia a los usuarios del VALLECAUCANA DE AGUAS S.A. E.S.P.
- La circulación de información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Distribución de material que viole derechos de propiedad intelectual.
- Desarrollo de actividades que produzcan:
    - La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
    - La destrucción o modificación premeditada de la información de otros usuarios.
    - La violación de la privacidad e intimidad de otros usuarios.
    - El deterioro del trabajo de otros usuarios.
    - Destrucción, manipulación o apropiación indebida de la información que circula por la red.
    - Uso y obtención de cuentas de ordenador ajenas.
    - Comunicación de contraseñas u otro tipo de información que permita a otros usuarios entrar en el sistema.
    - Proporcionar accesos externos a la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P distintos de los que la Oficina de Información ofrece.
    - La conexión de equipos de red activos (hubs, switches, routers, módems, firewalls, puntos de acceso inalámbricos, etc.) que previsiblemente perturbe el correcto funcionamiento de la misma o comprometa su seguridad, salvo expresa autorización de la Oficina de Información.
    - Conexión, desconexión o reubicación de equipos sin la autorización expresa de la Oficina de Información.
    - El alojamiento de dominios distintos de Vallecaucana de Aguas S.A. E.S.P es salvo expresa autorización de la Oficina de Información.

Responsabilidades: Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, la Oficina de Información procederá a la interrupción del servicio en el computador o dispositivo de red, dependiendo de la gravedad y reiteración del incidente.

Suspensión temporal o de emergencia del servicio: Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de la red y/o implique al VALLECAUCANA DE AGUAS S.A. E.S.P en algún tipo de responsabilidad.

La acción consistirá en la desconexión física de la red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P, del computador o dispositivo móvil causante del incidente, hasta resolver la causa que ha llevado a tomar esta medida.

Donde no fuera posible la desconexión física se procederá al filtrado del tráfico del computador o dispositivo implicado.

Suspensión indefinida del servicio: Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por parte del personal de la Oficina de Información. El servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable del computador o dispositivo causante del incidente garantizan un uso aceptable en el futuro.

Cualquier usuario del VALLECAUCANA DE AGUAS S.A. E.S.P que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta de la infraestructura de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P.

Cuando a un usuario de la Red de datos del VALLECAUCANA DE AGUAS S.A. E.S.P se le haya aplicado alguna de las limitaciones en el servicio, podrá recurrir la suspensión ante la Oficina de Información.

(Original se encuentra firmado)

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

Elaboró y proyectó: Dr. Luis Eduardo Pineda Álzate – Director Administrativo.
Aprobó: El Firmante.

Copia. Archivo.