Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

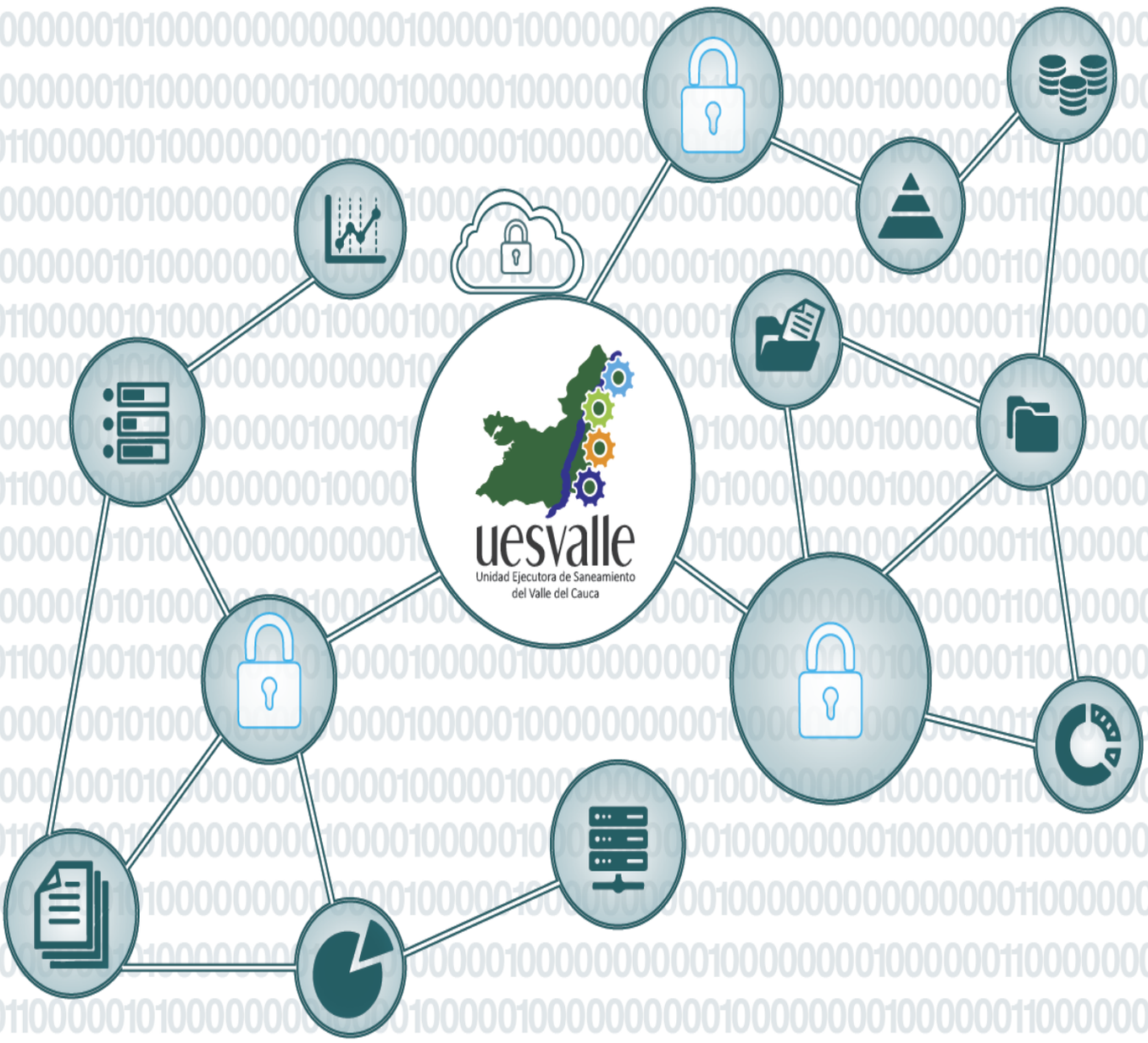

TABLA CONTENIDO

12. INTRODUCCION

La Unidad Ejecutora de Saneamiento del Valle del Cauca - UESVALLE, durante muchos años, ha acumulado datos e información originados por las experiencias y ejecución de los diferentes planes y programas, pero debe asegurar su permanencia en el tiempo, con una verdadera gestión del conocimiento, teniendo como insumo el capital intelectual y el banco de información como activo intangible de alto valor que puede mejorar la productividad, la especialización dentro del sector, la ratificación de ser un referente y su sostenibilidad.

En el pasado al hablar de manejo de los riesgos, se entendía que debía asumirse básicamente con la compra de seguros que cubrieran las posibles pérdidas, universalmente esto está cambiando, en la actualidad la administración de riegos se lleva de forma más extensa y coherente y se le vincula con el proceso de planeación estratégica que establece la gerencia de la empresa.

Administración de riesgos es el conjunto de técnicas y procedimientos usados para el análisis, identificación, evaluación y control de aquellos efectos adversos consecuencia de los riesgos o eventualidades a los que se expone una empresa, de esta manera se lograr reducirlos, evitarlos, retenerlos o transferirlos.

La información es crucial para el desarrollo de las actividades misionales y administrativas en la UESVALLE, por tal razón debe ser protegida de cualquier posibilidad de ocurrencia de eventos de riesgo de seguridad y que pudiese significar un impacto indeseado generando una consecuencia negativa para el normal progreso de las actividades de la entidad.

Glosario:

1. Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
2. Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
3. Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
4. Adware: Es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.
5. Advertencia: Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.
6. Alarma: Sonido o señal visual que se activa cuando se produce una condición de error.
7. Alerta: Notificación automática de un suceso o un error.
8. Administración de riesgos: conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
9. Amenaza: situación externa que no controla la entidad y que puede afectar su operación.
10. Análisis del riesgo: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
11. Asumir el riesgo: opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
12. Causa: medios, circunstancias y/o agentes que generan riesgos.
13. Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
14. Debilidad: situación interna que la entidad puede controlar y que puede afectar su operación.
15. Evaluación del riesgo: resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
16. Evitar el riesgo: opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
17. Frecuencia: ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
18. Identificación del riesgo: etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos

1. OBJETIVO

Establecer acciones que permitan la identificación, evaluación y control de los riesgos de forma tal que no afecten el objetivo misional de la entidad.

2. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Riesgo se puede definir como la probabilidad de que una amenaza pueda afectar una vulnerabilidad o debilidad de una entidad para causar una pérdida o daño en un activo de información. El objetivo general de este plan es gestionar el riesgo para identificar y establecer controles efectivos que garanticen la confidencialidad, integridad y disponibilidad de la información, donde se busca diseñar una metodología ágil enfocada en la identificación, gestión y tratamiento de los Riesgos de Seguridad y Privacidad de la Información.

2.1. Riesgos de seguridad de la información:

Riesgos que resultan de la combinación de amenazas y vulnerabilidades en el ambiente digital y dado su naturaleza dinámica incluye también aspectos relacionados con el entorno físico.

En la tipificación de dichos riesgos, se encuentran los siguientes:

a. Pérdida de la Información: Información que hace que esta llegue a personas no autorizadas, sobre la que su responsable pierde el control o el estado que genera una condición irreparable en el tratamiento y procesamiento de la Información. Ocurre cuando un sistema de información o proceso diseñado para restringir el acceso sólo a sujetos autorizados revela parte de la información que procesa o transmite debido a errores en la ejecución de los procedimientos de tratamiento, las personas o diseño de los Sistemas de Información.

b. Pérdida de la Confidencialidad: Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.

c. Pérdida de la Integridad: Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

d. Pérdida de la Disponibilidad: Pérdida de la cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2.2. Riesgos de Privacidad de la información:

Riesgos que afectan a las personas cuyos datos son tratados y que se concreta en la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por una utilización ilícita o fraudulenta de los mismos. Como riesgo tipificado se cuenta con lo siguiente:

a. Inadecuado Tratamiento de Datos Personales: Uso no adecuado de la información que identifica a las personas, lo que repercute en una violación de los derechos constitucionales.

3. Incidente de Seguridad de la Información

De acuerdo con lo descrito en la norma GTC-ISO/IEC 27035, un incidente de seguridad de la información está definido como “Evento o serie de eventos no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y vulnerar la seguridad”; por consiguiente, se representarían en Riesgos de Seguridad y Privacidad de la Información.

4. Factores de Riesgo

Se entiende por factores de riesgo aquellos que pueden afectar la confidencialidad, la integridad o la disponibilidad de la información de la UESVALLE. Entre los factores de riesgos que se encuentran identificados dentro de la entidad están los siguientes:

Personas: Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.

Procesos: Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.

Tecnología: Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.

Infraestructura: Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.

Factores Externos: Condiciones generadas por agentes externos, las cuales no son controlables por la Entidad y que afectan de manera directa o indirecta algún proceso.

5. TIPOS DE ACTIVOS

Activos Esenciales:

- Datos importantes o vitales para la Administración de la Entidad: Aquellos que son esenciales, imprescindibles para la continuidad de la entidad; es decir que su carencia o daño afectaría directamente a la entidad, permitiría reconstruir las misiones críticas o que sustancian la naturaleza legal de la organización o de sus usuarios.

- Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su intimidad personal y familiar (Ley 1581 de 2012).

- Datos Clasificados o Calificados: Aquellos sometidos a normativa específica de control de acceso y distribución o cuya confidencialidad es tipificada por normativa interna o legislación nacional (Ley 1712 de 2014)

Datos / Información: Que es almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.

Hardware / Infraestructura: Medios físicos, destinados a soportar directa o indirectamente los servicios que presta la entidad, siendo depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

Software / Aplicaciones Informáticas: Que gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

Servicios: Funciones que permiten suplir una necesidad de los usuarios (del servicio).

Personas: Usuarios Internos, Usuarios Externos, Operadores, Administradores de Sistemas, Administradores de Comunicaciones, Administradores de Bases de Datos, Administradores de Seguridad, Programadores, Contratistas, Proveedores.

Soportes de Información: Dispositivos físicos electrónicos o no que permiten almacenar información de forma permanente o durante largos periodos de tiempo

Redes de Comunicaciones: Instalaciones dedicadas como servicios de comunicaciones contratados a terceros o medios de transporte de datos de un sitio a otro

Claves Criptográficas: Esenciales para garantizar el funcionamiento de los mecanismos criptográficos

Equipos Auxiliares: Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos

Instalaciones: Lugares donde albergan los sistemas de información y comunicaciones.

La Valoración del Activo de Información se realiza mediante la identificación del impacto para la UESVALLE por la pérdida de las propiedades, principios o fundamentos de la Seguridad de la Información, teniendo en cuenta la siguiente tabla de criterios:

Criterio	**Valor**
Crítico	**= 5**
Alto	**= 3 y < 5**
Medio	**= 1 y < 3**
Bajo	**= 0 y < 1**

6. CONFIDENCIALIDAD.

Impacto que tendría para la UESVALLE, la pérdida de confidencialidad sobre el activo de información:

(5) Crítico: Es la existencia de información más crítica (Calificada, Vital o Esencial) a nivel de pérdida de su confidencialidad que cualquier otra y que por ende debe tener una mayor protección. A la información (Calificada, Vital o Esencial) sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de esta información, y con los privilegios asignados. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente a la UESVALLE.

(4) Alto: Es la información que es utilizada por los funcionarios del UESVALLE para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al proceso evaluado y/u otros procesos de Entidad.

(3) Medio: Es la información que es utilizada por los funcionarios de la Entidad para realizar sus labores en los procesos y que puede ser conocida por terceros con la autorización del propietario del activo. El conocimiento o divulgación no autorizada de la información que gestiona este activo impacta negativamente al proceso evaluado y/u otros procesos.

(2) Bajo: Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada con ciertas restricciones dadas por el propietario del activo a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos de la Entidad. El conocimiento o divulgación no autorizada de la información que gestiona este activo no tiene ningún impacto negativo en los procesos de la UESVALLE.

(1) Mínimo: Es la información que ha sido calificada como de conocimiento público. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que implique daños a terceros ni a las actividades y procesos de la UESVALLE.

(0) Nulo. Esla información que ha sido calificada como de conocimiento público y su divulgación no implica impacto negativo en los procesos del UESVALLE.

7. INTEGRIDAD.

Impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de la información y métodos de procesamiento fueran alterados.

(5) Crítico: La pérdida de exactitud y estado completo del activo impacta negativamente la prestación de servicios de tecnología y de información en la UESVALLE.

(4) Alto: La pérdida en la exactitud de algún dato o estado del activo impacta negativamente la prestación de servicios de tecnología y de información en la Entidad.

(3) Medio: La pérdida posible de en la exactitud de algún dato o estado completo del activo puede impactar negativamente al proceso que gestiona la información y/o a otros procesos de la UESVALLE.

(2) Bajo: La pérdida posible de en la exactitud de algún dato o estado completo del activo puede tener algún impacto negativo en los procesos.

(1) Mínimo: La pérdida de exactitud y estado completo activo no tiene ningún impacto negativo en los procesos de la UESVALLE.

(0) Nulo: La pérdida de exactitud y estado no genera situación negativa alguna en los procesos de la Entidad.

8. DISPONIBILIDAD.

Impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

(5) Crítico: La falta o no disponibilidad de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en la Entidad.

(4) Alto: La falta o no disponibilidad parcial de la información que posea el activo de información o el mismo impacta negativamente la prestación de servicios de tecnología y de información en la UESVALLE.

(3) Medio: La falta o no disponibilidad de algún dato que posea el activo de información o el mismo impacta negativamente al proceso que gestiona la información y/o a otros procesos.

(2) Bajo: La falta o no disponibilidad del activo de información en su componente puede tener algún impacto negativo en los procesos de la UESVALLE.

(1) Mínimo: La falta o no disponibilidad del activo de información no tiene ningún impacto negativo en los procesos de la Entidad.

(0) Nulo: La falta o no disponibilidad de algún dato que posea el activo de información no afecta los procesos

Se identifican los responsables y dueños de la información con base en la oficina o dependencia productora, así mismo se le asocian a su responsabilidad, el tratamiento de los riesgos de seguridad identificados.

Se consideran los factores de riesgo, las vulnerabilidades de los activos de información, las causas o amenazas que puedan determinar la materialización de un evento, sus posibles consecuencias o afectación, relacionándolos con la identificación del riesgo de seguridad o privacidad de la información.

Todo lo anterior se realiza mediante la documentación de fuentes como: Entrevistas no estructuradas con los responsables de los activos y el desarrollo del flujo de la información en el proceso, fuentes estadísticas y tendencias de los riesgos de seguridad y privacidad, observaciones de expertos y analistas, estudio de los procedimientos, guías y diagramas de información, establecimiento de la criticidad del activo y su tratamiento por parte de las personas, los procesos y la tecnología, gestión de riesgos realizados anteriormente y detección de áreas o dependencias sensibles.

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

9.1. Actividades

a. Realizar Diagnóstico.
b. Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información.
c. Realizar la Identificación de los Riesgos con los responsables de Proceso.
    - Entrevista con los responsables del Proceso.
d. Valoración del riesgo y del riesgo residual
e. Realizar matriz de riesgos de seguridad y privacidad de la información

f. Plantear el plan de tratamiento de riesgos aprobado por los responsables de los procesos.

9.2. Cumplimiento de implementación

De acuerdo a las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo a lo establecido por la UESVALLE.

1. Revisión y/o Modificación de la actual Política de Seguridad.
2. Aspectos organizativos de la seguridad de la información
3. Seguridad Ligada a los recursos humanos
4. Revisión del Control de acceso
5. Seguridad en la operatividad
6. Seguridad en las telecomunicaciones
7. Gestión de Incidentes de Seguridad de la Información
8. Aspectos de seguridad de la información en la gestión de continuidad del negocio.

9.3. Cronograma de actividades del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información

CRONOGRAMA DE ACTIVIDADES DEL PLAN DE TRATAMIENTO - 2019										
Actividad	Mar	Abril	Mayo	Jun	Julio	Ago.	Sept.	Oct.	Nov	Dic
Realizar diagnostico										
Realizar inventario de activos										
Identificar riesgos con responsables de procesos										
Elaborar matriz de valoración de activos y análisis de riesgos.										
Valoración del riesgo residual										
Seguimiento y control										

Con base en el resultado del análisis de riesgos de seguridad y privacidad de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de la misma, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

El Plan de Tratamiento de Riesgos de Seguridad de la Información se integra a la presente Guía Metodológica y a la Matriz de Valoración de Activos y Análisis de Riesgos de Seguridad de la Información, contribuyendo al fortalecimiento de los mecanismos de Gestión de Riesgos del Sistema Integrado de Gestión de la UESVALLE.

La formulación de actividades de tratamiento de riesgos de seguridad de la información y su aplicación de acuerdo con la valoración del riesgo inherente documentado, buscando integrar la implementación de la presente Guía Metodológica.

10. NOTAS DE CAMBIO

Fecha	Versión inicial	Creación o motivo del cambio y numerales cambiados	Versión final
Enero 21 de 2019	0.0	Creación del documento. Decreto 1078 de 2015. Decreto Único Reglamentario del sector de Tecnologías de la información y las comunicaciones	1.0

11. APROBACION

	Elaboró	Revisó	Aprobó
Nombre:	Robert Andrey Fernández de Cordoba Flórez	Fernando Girón Vanderhuk	Diego Victoria Mejía
Cargo:	Profesional Universitario Proceso de Gestión Informática	Subdirector Administrativo	Director General
Fecha:	Enero de 2019	Enero de 2019	Enero de 2019
Firma:	Documento original firmado	Documento original firmado	Documento original firmado