uesvalle
Unidad Ejecutora de Saneamiento
del Valle del Cauca

Plan de Seguridad y Privacidad de la Información

TABLA CONTENIDO

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.

La UESVALLE debe apoyarse en las Tecnologías de Información y de comunicaciones (TIC), sobre el entendido de que son recursos, herramientas, equipos (hardware), aplicaciones o programas informáticos (software), redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recibo de información como: voz, datos, texto, vídeo e imágenes, o procesar información para poder calcular resultados y elaborar informes para la toma de decisiones.

Con el fin de garantizar el manejo eficaz de la información la UESVALLE por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información y la integridad, su privacidad y/o confidencialidad.

Esto se logra por medio de un Sistema de Gestión de Seguridad de la Información acorde con referentes nacionales e internacionales como la norma ISO 27001:2013, que permite la evaluación de riesgos, el establecimiento de controles, la evaluación de la conformidad de las partes interesadas, tanto internas como externas y contribuye en la ejecución de un plan de seguridad y privacidad adecuado para la Entidad, donde se de tratamiento de incidentes y planes de contingencia a la Entidad, como medida preventiva ante cualquier eventualidad a la cual se pueda ver expuesta.

1. JUSTIFICACION

Actualmente la seguridad y confidencialidad de la información juega un papel muy importante dentro de las empresas y por consiguiente se deben construir planes y procedimientos que nos permitan manipular la información de forma segura.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante para el sector público que está cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno Digital, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y aplicativos de la UESVALLE, se hace necesario levantar una línea de base sobre la cual se articulen diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

Esta normativa se debe aplicar progresivamente teniendo en cuenta los lineamientos solicitados y dando victorias tempranas sucesivas hasta lograr la mejor implementación.

La seguridad de la información debe estar caracterizada por su:

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

2. GLOSARIO:

1. **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
2. **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
3. **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
4. **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)
5. **Activo**: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
6. **Amenaza:** causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
7. **Amenaza informática:** la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).
8. **Análisis de riesgos**: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
9. **Anonimización del dato**: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.
10. **Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta.
11. **Autenticidad:** propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).
12. **Ciberseguridad:** capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
13. **Dato privado:** es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
14. **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.

3. OBJETIVO

Establecer un plan para desarrollar los mecanismos necesarios para darle disponibilidad, confidencialidad y seguridad a los datos y activos de información de la Entidad.

3.1. Objetivos específicos

- Realizar un plan de trabajo para iniciar la implementación del plan de seguridad y privacidad de la información.
- 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.

4. ALCANCE

El alcance del documento es mejorar los niveles de seguridad de los activos de información de los procesos de la Entidad para el año 2019, teniendo en cuenta la normatividad vigente.

5. Marco normativo

Decreto 1008 de 2018. Establece los lineamientos generales de la política de Gobierno Digital. Deroga el Decreto 2573 de 2014.

Ley 1266/08 Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países información

Ley 1273/09. Por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Ley 1581/12 Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

La Ley 850/03 establece en su artículo 9º Principio de Transparencia

Ley 594/00 Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones

Ley 527/99 Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos

Decreto 1499 de 2017. Modelo Integrado de Planeación y Gestión y Manual operativo.

6. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Reconocemos que los Activos de Información que soportan los procesos de la Entidad, contribuyen a la generación de la memoria institucional y gestión del conocimiento por lo que es necesario avanzar en su Seguridad y Privacidad, por lo que se propiciará los recursos necesarios para apoyarlo, de acuerdo con la disponibilidad presupuestal y la priorización institucional.

En la UESVALLE se debe asegurar de implementar la política, para asegurar el cumplimiento de los objetivos de seguridad de la información, como son:

a) Establecer las políticas, procedimientos e instructivos en materia de Seguridad de la información.
b) Mitigar los riesgos de la entidad
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Proteger los activos de información.
g) Fortalecer la cultura de seguridad de la información en los funcionarios y usuarios de los diferentes aplicativos.

Las responsabilidades frente a la seguridad de la información serán definidas, compartidas y publicadas por cada uno de los usuarios de información de la Entidad. de ellos se intuye que la Entidad protege la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de la misma. Para ello es fundamental

la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

Dadas las condiciones de seguridad y privacidad la UESVALLE estará en capacidad de:

- Proteger la integridad de información de las amenazas originadas por parte del personal.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de los procesos garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información y las debilidades asociadas.
- Garantizar la disponibilidad de información y la continuidad en el servicio que la proporciona.

Implementación de políticas de seguridad de la información

Este plan de Seguridad y Privacidad de la información deberá realizarse para el año 2019.

6.2. **DESCRIPCIÓN DE LAS POLÍTICAS**

Generalidades

Este plan tiene como fin garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en la UESVALLE.

Entre los temas a tratar están:

6.2.1. **Gestión de activos**

Política para la identificación, clasificación y control de activos de información.

En la UESVALLE a través de La mesa de trabajo de gobierno digital se realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a los procesos de Gestión informática, gestión de recursos físicos y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El responsable del proceso de Gestión de Recursos Físicos con apoyo del técnico operativo de gestión informática tienen la responsabilidad de mantener el inventario completo y actualizado de los recursos de hardware y software de la entidad.

Procedimientos a tener en cuenta:

a) Los usuarios deben acatar los lineamientos de clasificación de la Información para el acceso, almacenamiento, copia, transmisión, etiquetado y Eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

b) La información física y digital de la Entidad debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, envíen correos y saquen copias: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras o dejar abierto el correo electrónico para asegurarse que no quedaron documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y

resguardo, para los documentos digitales debe estar implementada una plataforma para el acceso personal a los mismos (control de usuario).

6.2.2. **Control de acceso**

6.2.2.1 Política de acceso a redes y recursos de red

El proceso de gestión informática de la UESVALLE, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Pautas para tener en cuenta

a) El proceso Gestión Informática debe asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.

b) El proceso Gestión Informática debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de la UESVALLE, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

c) Los funcionarios y personal provisto por contratistas externos, antes de contar con acceso lógico por primera vez a la red de datos de la UESVALLE, deben contar con el formato de creación de cuentas de usuario debidamente autorizado.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

6.2.2.2. Política de administración de acceso de usuarios

El proceso de Gestión Informática establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

a) El proceso de Gestión Informática, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la UESVALLE; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b) El proceso de Gestión Informática debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

c) El proceso Gestión Informática debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

d) Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso de Gestión Informática, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

e) Los propietarios de los activos de información deben verificar y ratificar anualmente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

6.2.2.3. **Política de control de acceso a sistemas de información y aplicativos.**

La UESVALLE como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El proceso Gestión Informática, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Normas de atención:

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

b) Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

c) El proceso Gestión Informática, debe establecer un procedimiento para la administración de usuarios en los sistemas y aplicativos de la UESVALLE.

d) Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos acceder a los recursos y configuración en la página web.

f) Los funcionarios no deben dejar escritas contraseñas en “notas” junto a los PC´s para su recordación, es responsabilidad de cada uno que se cumpla.

6.2.3. Políticas de seguridad física.

La UESVALLE proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso de Gestión Informática administrará las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso de Gestión Informática autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.

b) El proceso de Gestión Informática debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

c) El Director General debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la UESVALLE.

d) El Subdirector administrativo debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

e) Los ingresos y egresos de personal a las instalaciones de la UESVALLE en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por contratistas externos deben cumplir completamente con los controles físicos implantados.

6.2.4. **Política de seguridad para los equipos.**

La UESVALLE para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Puntos clave:

a). El proceso de Gestión Informática y Gestión de recursos físicos debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la UESVALLE.

b). El proceso de Gestión Informática debe realizar soportes técnicos (presenciales o virtuales) y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la entidad.

c). El proceso Gestión de Informática en conjunto con el facilitador del proceso Gestión de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.

d) El proceso de Gestión Informática debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.

e) El proceso de Gestión Informática debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la Red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

f) El proceso Gestión de Informática y recursos físicos deben generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.

g) El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la UESVALLE cuente con la autorización documentada y aprobada previamente por el área.

h) El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad se realicen de forma segura y posean las pólizas de seguro.

i) El proceso de Gestión Informática es el único autorizado para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la UESVALLE.

j) Los equipos portátiles y dispositivos móviles deben allegarse al área de gestión informática para recibir su mantenimiento preventivo, correctivo o ajustes necesarios para su mejor funcionamiento, es responsabilidad de cada funcionario que tenga a cargo el dispositivo.

k) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la UESVALLE, el usuario responsable debe informar al facilitador del proceso de Gestión Informática, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

l) La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los profesionales universitarios o técnicos de apoyo del proceso de Gestión Informática.

m) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

n) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

6.2.5. **Política de uso adecuado de internet.**

La UESVALLE consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para

asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad en cualquiera de sus oficinas (sede principal, ARO Cali, ARO Tuluá, Aro Buga, ARO Cartago, oficina de yumbo).

Puntos clave:

a). El proceso de Gestión Informática debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación SEGURA del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

b). El proceso de Gestión Informática debe contar con niveles de servicio contratados eficientes que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

c). El proceso de Gestión Informática debe monitorear continuamente el canal o canales del servicio de Internet.

d) El proceso de Gestión Informática debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

e) El proceso de Gestión Informática debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.

f) Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

g) No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

h) Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la UESVALLE.

I) En la UESVALLE no está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura

tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el facilitador del proceso Gestión de TIC o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

j) No está permitido el intercambio no autorizado de información de propiedad de la UESVALLE, de los funcionarios, con terceros.

7. PRIVACIDAD Y CONFIDENCIALIDAD

7.1. Política de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la UESVALLE, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Esta política contiene una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente y deberá ser conocido y aplicado por usuario, funcionarios, proveedores o terceros que intercambien información con la Entidad.

Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras deben:

- Obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

- Asegurar que solo aquellas personas que tengan una necesidad laboral legítima Puedan tener acceso a dichos datos.

- Acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

El proceso de gestión informática debe:

- Establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de la UESVALLE de los cuales reciba y administre información.

- Implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la Entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

Los usuarios y funcionarios, deben verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico o por correo certificado.

Los usuarios del portal de la UESVALLE deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

En el portal de la UESVALLE deben estar publicadas las Políticas de protección de datos personales.

8. DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN

La UESVALLE con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, debe crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

8.1. Política de continuidad, contingencia y recuperación de la información.

La UESVALLE proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

8.2. **Copias de Seguridad.**

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos establecidos en el portal de Sistema de Gestión de Calidad. Dicho procedimiento deberá incluir las actividades de almacenamiento de las copias en sitios seguros.

El proceso de Gestión Informática deberá realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deberán ser guardados en una base de datos creada para tal fin.

El proceso de Gestión Informática deberá proveer las herramientas para que las dependencias puedan administrar la información y registros de copias de seguridad. La (el) profesional especializado con funciones de Control Interno debe efectuar auditorías aleatorias que permitan determinar el correcto funcionamiento de los procesos de copia de seguridad.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

El proceso de gestión informática deberá:

a) Reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

b) Liderar los temas relacionados con la continuidad del Entidad y la recuperación ante desastres

c) Realizar los análisis de impacto a la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d) Asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

9. ANEXOS

P-GI-04 Procedimiento para administración de usuarios del proceso de gestión Informática.
P-GI-05 Procedimiento para la realización de copias de seguridad

10. NOTAS DE CAMBIO

FECHA	VERSION INICIAL	CREACION O MOTIVO DEL CAMBIO Y NUMERALES MODIFICADOS	VERSIÒN 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

	ELABORÒ	REVISÒ	APROBÒ
Nombre:	Robert Andrey Fernández de Córdoba Flórez	Fernando Girón Vanderhuk / Constanza Ivette Hernández	Diego Victoria Mejía
Cargo:	Profesional Universitario Proceso de Gestión Informática	Subdirector Administrativo / Asesora de Planeación	Director General
Fecha:	Enero 21 de 2019	Enero 21 de 2019	Enero 21 de 2019
Firma:	Documento original firmado	Documento original firmado	Documento original firmado