uesvalle
Unidad Ejecutora de Saneamiento del Valle del Cauca

Valle Invencible

GOBERNACIÓN VALLE DEL CAUCA
Secretaría de Salud

Plan de Seguridad y Privacidad de la Información

2021 -2023

TABLA DE CONTENIDO

INTRODUCCIÓN

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.

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 a través del 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.

Este documento se encuentra alineado al Y-GI-06 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2020 - 2023, teniendo en cuenta las mejores prácticas y estándares de implementación de los controles en relación con seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar) establecidos por el ministerio de la TICS y la ISO 27001.

En cumplimiento con la política de Participación Ciudadana en la Gestión Pública contenida en la segunda dimensión de Direccionamiento Estratégico y Planeación y en la tercera dimensión Gestión con Valores para Resultados, la entidad publicó en su portal web www.uesvalle.gov.co, el borrador de este documento con el fin de brindar de que la ciudadanía en general se incluyera en su construcción dentro del ejercicio de la democracia participativa.

1. OBJETIVO

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Y Privacidad de la información, establecidos en el Mapa de Procesos de la UESVALLE.

1.1 Objetivos Específicos

- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Establecer lineamientos para la metodología de gestión de activos de información acorde a los requerimientos mínimos del MINTIC y DAFP.
- Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

2. ALCANCE

El plan de seguridad y privacidad de la información será aplicado a los procesos estratégicos, misionales, de apoyo, y control de la UESVALLE, por tal motivo, deberá ser conocido y cumplido por todas las partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas.

3. DEFINICIONES

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).

Amenazas. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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

Auditoría. Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

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.

Activo de Información. En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza. causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

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).

Análisis de riesgos. proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Archivo. Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Auditoría. Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autenticación. provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autorización. Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales. Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberespacio. Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Ciberseguridad. capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Datos Abiertos. Son todos aquellos datos primarios o sin procesar, que se encuentran en

formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales. Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Mixtos. Es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Privados. Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Públicos. Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

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. (Decreto 1377 de 2013, art 3).

Encargado del Tratamiento de Datos. Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada. 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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada. 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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Plan de tratamiento de riesgos. Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Política. Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Plan de continuidad del negocio. Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

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

Riesgo. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

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

4. MARCO NORMATIVO

Ley 527de 1999. Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

Ley 1266 de 2008. 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 de 2009. 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 de 2012. Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

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

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

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

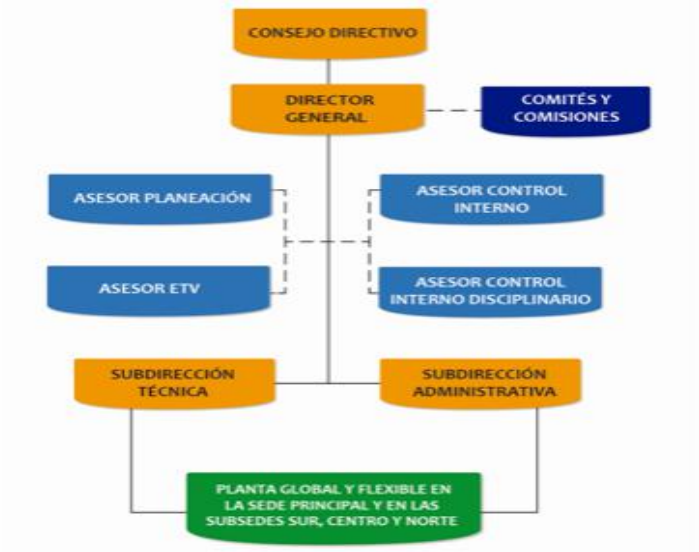
Normas Técnicas colombianas - NTC/IEC ISO 27001:2013

5. CONOCIMIENTO DE LA ENTIDAD

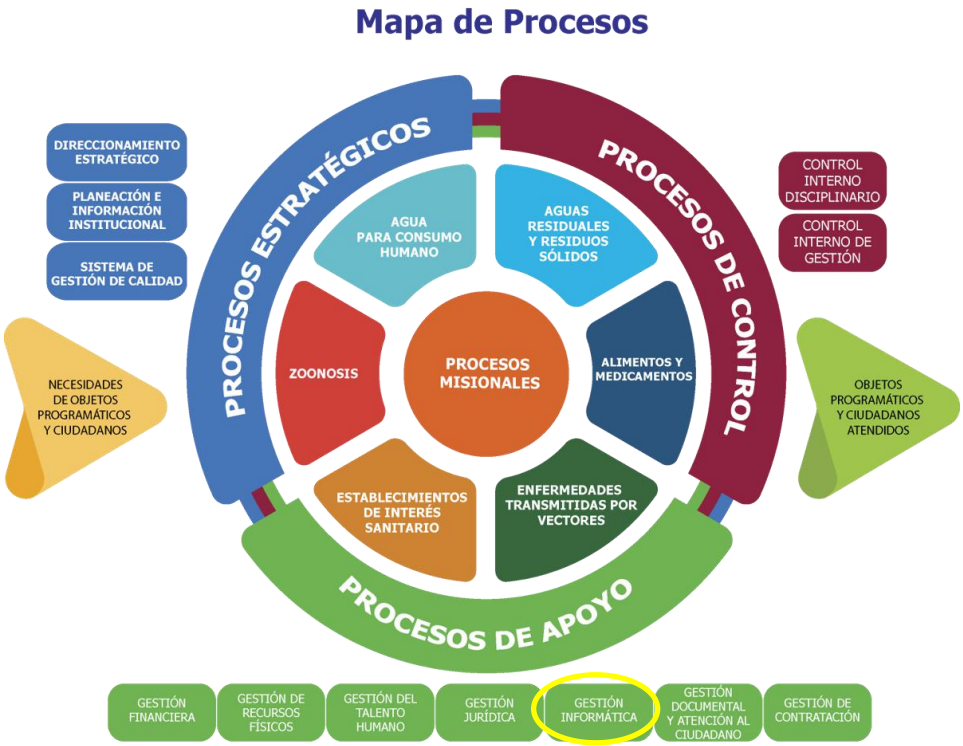
MISIÓN: Somos la Entidad, que apoya a la Secretaría Departamental de Salud en el cumplimiento de las funciones y competencias en Salud ambiental y Saneamiento ambiental; y desarrolla, programas y proyectos en alianza con otras instituciones públicas y organizaciones sin ánimo de lucro, contribuyendo al mejoramiento de la calidad de vida de la población Vallecaucana.

VISIÓN: La Unidad Ejecutora de Saneamiento del Valle del Cauca en el año 2032, será reconocida como una entidad referente a nivel regional y nacional por sus servicios en salud ambiental y saneamiento ambiental, que contribuirá de manera coordinada y participativa al mejoramiento de la calidad de vida de la población Vallecaucana.

ORGANIGRAMA:



MAPA DE PROCESOS



La UESVALLE, cuenta con el proceso Gestión Informática, el cual tiene a cargo los procedimientos, manuales, formatos y todo el tema documental correspondiente a seguridad y privacidad de la información.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la información fue aprobada por el Comité de gestión y desempeño de la UESVALLE, se encuentra publicada en el Sistema Integrado de Gestión identificada como: M-GI-05 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION UESVALLE 2020, y representa un documento de apoyo para el desarrollo de este plan.

6.1 Objetivos de la Política de Seguridad y Privacidad de la Información.

- Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la UESVALLE, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

- Definir los lineamientos a ser considerados para diseñar e implementar el Sistema de Gestión de Seguridad de la Información alineado con las necesidades, los procesos, los objetivos y la operación de la UESVALLE.

- Dar conformidad y cumplimiento a las leyes, regulaciones y normativas que le aplican a la UESVALLE en el desarrollo de su misión.

- Fortalecer la cultura de seguridad de la información en funcionarios, terceros y clientes de UESVALLE, mediante la definición de una estrategia de uso y apropiación de la política.

- Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la Información.

7. MODELO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El modelo del MSIP se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar.

Figura 1. **Ciclo de operación Modelo de Seguridad y Privacidad de la Información**
Fuente: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

7.1 Fase I – Diagnostico y Situación Actual

De acuerdo al modelo de seguridad y privacidad año 2020-2023, se establece para la vigencia 2020 las siguientes metas:

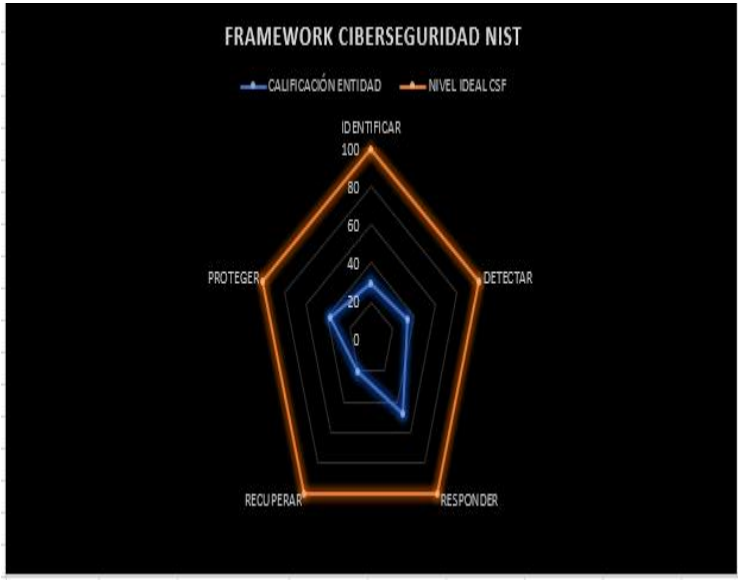
Metas	Actividades \ Instrumentos \ Resultados
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la UESVALLE.	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información. Diagnostico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos de la norma ISO 27001:2013. Valoración estado actual de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la UESVALLE.	Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo 'MODELO DE MADUREZ' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

7.1.1 Autodiagnóstico de Seguridad Y Privacidad De La Información Año 2020 Vs. 2021

A continuación, se presenta el resultado del autodiagnóstico realizado a la UESVALLE, durante la vigencia 2020 vs. 2021

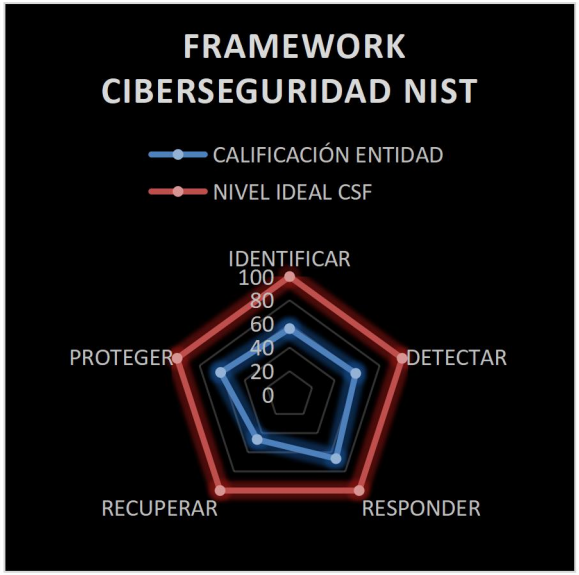
2020

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fi	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	29	100
DETECTAR	34	100
RESPONDER	48	100
RECUPERAR	20	100
PROTEGER	38	100



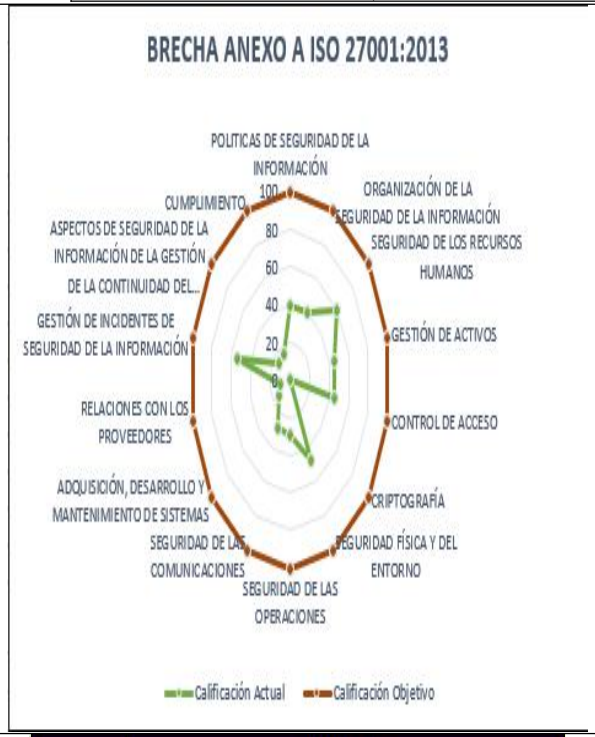
2021

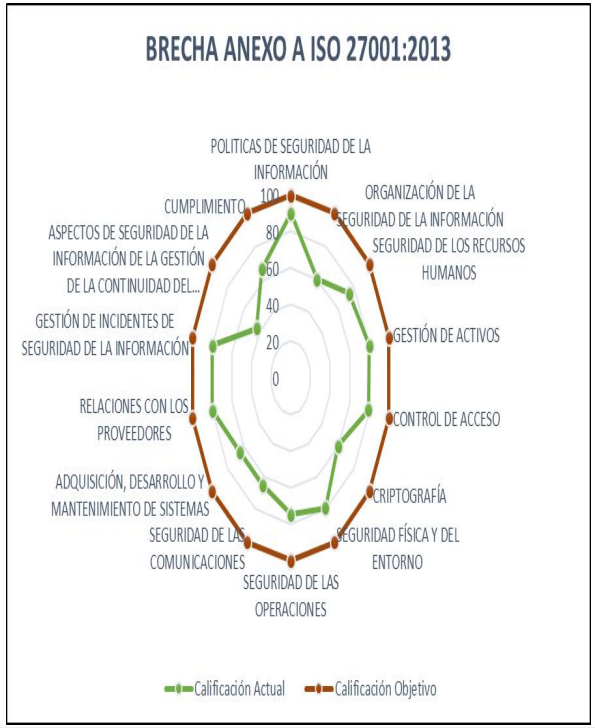
MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	56	100
DETECTAR	59	100
RESPONDER	67	100
RECUPERAR	47	100
PROTEGER	61	100



No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	46	100	EFECTIVO
A.9	CONTROL DE ACCESO	45	100	EFECTIVO
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	47	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	29	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	28	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	14	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	10	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	54	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	14	100	INICIAL
A.18	CUMPLIMIENTO	15	100	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		32	100	REPETIBLE

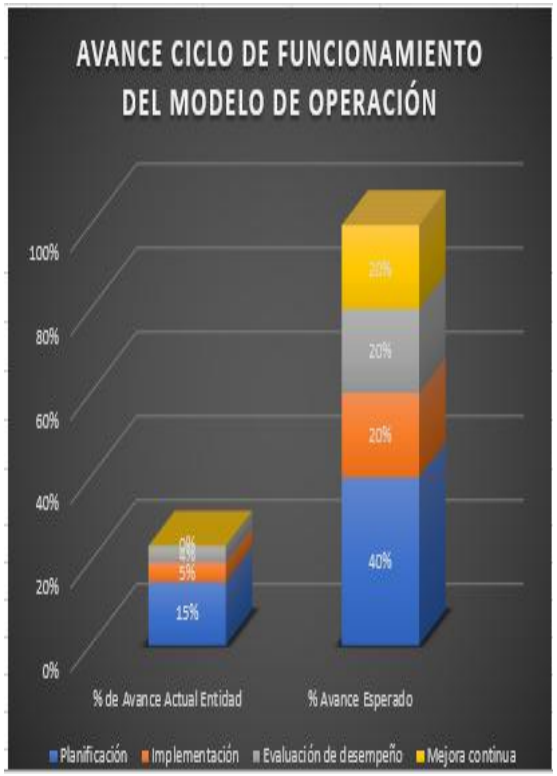
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	73	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	80	100	GESTIONADO
A.9	CONTROL DE ACCESO	64	100	GESTIONADO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	65	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	56	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	44	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	46	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	69	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	34	100	REPETIBLE
A.18	CUMPLIMIENTO	53,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		59	100	EFECTIVO

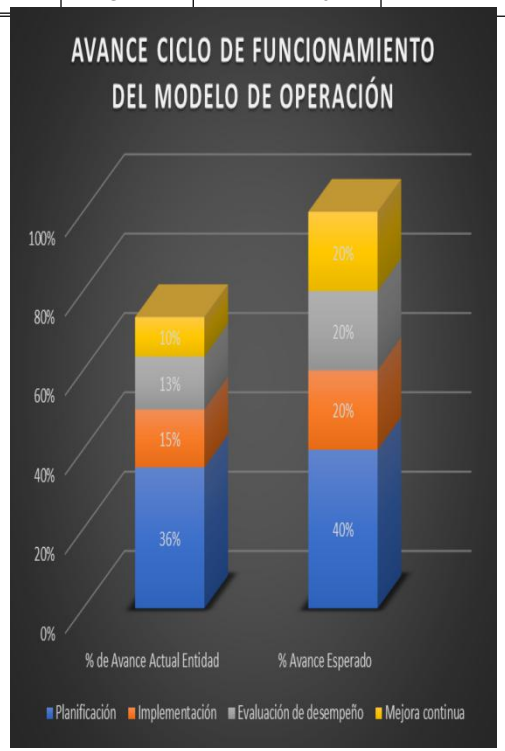




Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	15%	40%
2016	Implementación	5%	20%
2017	Evaluación de desempeño	4%	20%
2018	Mejora continua	0%	20%
TOTAL		24%	100%

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2021	Planificación	36%	40%
2021	Implementación	15%	20%
2021	Evaluación de desempeño	13%	20%
2021	Mejora continua	10%	20%
TOTAL		73%	100%


AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN
100%
80%
60%
40%
20%
0%
15%
5%
40%
20%
20%
% de Avance Actual Entidad
% Avance Esperado
Planificación
Implementación
Evaluación de desempeño
Mejora continua


AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN
100%
80%
60%
40%
20%
0%
36%
15%
13%
10%
40%
20%
20%
20%
% de Avance Actual Entidad
% Avance Esperado
Planificación
Implementación
Evaluación de desempeño
Mejora continua

Durante la vigencia 2021, se mejoraron lo indicadores en un 49% con respecto al año 2020, lo cual indica el crecimiento y empoderamiento del Modelo de Seguridad y Privacidad de la Información, documento Y-GI-06 adoptado por la UESVALLE.

De acuerdo con estos resultados, se continúa la etapa de planificación de acuerdo con el Modelo de Seguridad.

7.2 Fase II- Planificación

Durante la vigencia 2022, se continúa con la fase de planeación la cual permite definir la estrategia metodológica, el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas, a continuación, los documentos desarrollados para tal fin:

Metas	Actividades \ Instrumentos \ Resultados
Política de 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. M-GI-05 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION UESVALLE 2020 https://drive.google.com/file/d/11jwiV2KND9xJdmchuLAPWrVKPzZRW3VG/view
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional M-GI-05 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION UESVALLE 2020 https://drive.google.com/file/d/11jwiV2KND9xJdmchuLAPWrVKPzZRW3VG/view
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. M-GI-05 POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION UESVALLE 2020 https://drive.google.com/file/d/11jwiV2KND9xJdmchuLAPWrVKPzZRW3VG/view PAGINA 20
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. G-GI-02 METODOLOGIA GESTION DE ACTIVOS DE INFORMACION https://drive.google.com/file/d/19MskjH5nYQf71pPKYfnXskcTiGF-wakK/view Matriz con la identificación, valoración y clasificación de activos de información F-GI-13 ACTIVOS DE INFORMACION https://drive.google.com/file/d/1RUUz4bM5CmFYjw71MrhYBMUD6L-9QX3B/view
Integración del MSPI con el Sistema de Gestión documental.	Integración del MSPI, con el sistema de gestión documental de la entidad. SE INTEGRA CON EL SISTEMA DE GESTION, EN LA IMPLEMENTACION DE LAS POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION P-GI-01 PROCEDIMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION https://drive.google.com/file/d/1OTpxifGSWxzxfRcYmZGj2_CFMlYVIy9N/view

Metas	Actividades \ Instrumentos \ Resultados
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. M-DE-02 Política Administración de Riesgos https://drive.google.com/file/d/1jc3D_5wKYECt2o2frH89Qy23vXrIiO0L/view Documento con el análisis y evaluación de riesgos, Matriz riesgos de seguridad de la información. https://docs.google.com/spreadsheets/d/1YfRa1xyARxkNfzVGCNoq0ZsnVsTVn95s/edit?usp=sharing&ouid=107998174792122708495&rtpof=true&sd=true Documento con el plan de tratamiento de riesgos. Y-GI-03 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION https://drive.google.com/file/d/1pFkBGcaJrgBBtiF1akqeiv4BsiX_g9pU/view
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad. Y-GI-05 PLAN DE SENSIBILIZACION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION https://drive.google.com/file/d/1txogtF_ZMeCRs4ZgOiMxMcGcDhvylRTS/view
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. https://docs.google.com/document/d/1_TOLpR3V8tSs_RIpqsMrWEoncdm5MYcS/edit?usp=sharing&ouid=107998174792122708495&rtpof=true&sd=true

7.3 Fase III- Implementación

Durante la vigencia 2022, se llevará a cabo la implementación de la fase II de planeación, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la UESVALLE.

Metas	Actividades \ Instrumentos \ Resultados
Planificación y Control Operacional	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Todos los documentos son codificados y aprobados por el área Calidad, proceso estratégico de la Institución. La ejecución está a cargo del proceso de gestión informática, así como su socialización.
Implementación del plan de tratamiento de riesgos.	La matriz de riesgos de seguridad de la información está administrada por el área de planeación, con el seguimiento de controles y plan de acción a cargo de control Interno.
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. Se cuenta con el tablero de mando y ficha de indicadores para validar el cumplimiento del plan.
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. Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

7.4 Fase IV- Evaluación de Desempeño

Durante la vigencia 2023, se realizará el proceso de evaluación y cumplimiento de los planes de acuerdo a los instrumentos e indicadores de resultados que permitan determinar la efectividad de la implementación del SGSI.

Metas	Actividades \ Instrumentos \ Resultados
Plan de revisión y seguimiento, a la implementación del MSPI.	Establecer tablero de mando e indicadores de cumplimento de los planes de PSPSI y PTRPSI.
Plan de Ejecución de Auditorias.	Documento con el informe por parte de control interno, con los resultados de la auditoría interna. Socializado a la Alta Dirección.

7.5 Fases V - Mejora Continua

Para la vigencia 2023 se consolidarán los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el modelo de seguridad.

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

8. PLAN DE IMPLEMENTACION DEL MODELO DE SEGURIDAD DE LA INFORMACION.

El plan de implementación para la dimensión de seguridad y privacidad de la información establece el siguiente cronograma el cual tendrá seguimiento de manera trimestral.

FASES	Línea de Base Año 2020	2021	2022	2023
FASE I -Diagnóstico	X			
FASE II -Planificación		X	X	
FASE III –Implementación		X	X	
FASE IV –Evaluación				X
FASE V –Mejora Continua				X

A continuación, se detalla las actividades a desarrollar en la vigencia 2022, y cada año se proyectará las actividades siguientes actualizando solo la versión de este plan.

8.1 Cronograma de Actividades Año 2022

Gestión	Actividades	Responsable de la Tarea	Fecha Inicio	Fecha Final
Activos de Información	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad,	Gestión Informática	01-03-2022	30-06-2022
	Aprobar los Activos de información, mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.	Gestión Informática	01-07-2022	30-09-2022
Gestión de Riesgos	Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Gestión Informática	01-10-2022	31-12-2022
	Actualizar política y metodología de gestión de riesgos de seguridad digital.	Gestión Informática	01-06-2022	30-06-2022
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación.	Gestión Informática	01-05-2022	30-05-2022
Gestión de Incidentes de seguridad de la Información	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias.	Gestión Informática	01-02-2022	20-12-2022
Gestión de Infraestructura	Elaborar y ejecutar el plan anual de capacitación y sensibilización anual de seguridad de la información y ciberseguridad.	Gestión Informática	01-03-2022	20-12-2022
	Aprobar por la alta dirección, el diagnóstico para la transición de la entidad de IPv4 a IPv6.	Gestión Informática	01-06-2022	30-06-2022
Gestión de Monitoreo	Realizar y Documentar el Plan para la transición de IPv4 a IPv6.	Gestión Informática	01-07-2022	01-09-2022
Gestión de Monitoreo	Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la UESVALLE	Gestión Informática	01-02-2022	31-12-2022

8.2 Proyección de presupuesto PSPSI

La proyección estimada de presupuesto para la ejecución del PSPSI, se encuentra alineado con el PETI para cumplir con el Plan de Estratégico de la UESVALLE 2020-2023: "UN COMPROMISO SOCIAL Y RESPONSABLE POR LA SALUD AMBIENTAL", con sus dos líneas estratégicas "Gestión territorial compartida y eficiente por la salud ambiental" y "Por el mejoramiento de la gestión y el desempeño institucional" es:

PRESUPUESTO 2022	
NOMBRE DEL ACTIVO TECNOLÓGICO	**2022**
Mantenimiento y soporte técnico a sistemas de información.	170.000.000
Mantenimiento preventivo y correctivo.	107.000.000
Redes y seguridad de la información.	125.000.000
Software y equipos informáticos.	175.000.000
Gestión TI	102.000.000
TOTAL	**679.000.000**

9. NOTAS DE CAMBIO

Fecha	Versión inicial	Motivo del cambio y numerales modificados	Versión final
Ene. 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
Ene. 30 de 2020	1.0	Se incorpora Nuevas políticas de seguridad y privacidad de la información y se adiciona los procedimientos de gestión y clasificación de activos de información y gestión de incidentes de seguridad.	2.0
Ene. 27 de 2021	2.0	Se incorpora Nuevas el método de evaluación basado en el ciclo de mejoramiento continuo PHVA y Resultado inicial del autodiagnóstico del nivel de Madurez del MSPI.	3.0
Ene. 26 de 2022	3.0	Se realiza el avance comparativo de crecimiento de la vigencia 2021 vs 2020, se adiciona el ítem de proyección del presupuesto y se actualiza el cronograma de actividades para la vigencia 2022.	4.0

10. APROBACIÓN

	ELABORÓ	REVISÓ	APROBÓ
Nombre:	Yeny Aracelly Núñez	Julián Eduardo Montoya Ramírez	Diego Victoria Mejía
Cargo:	Profesional Universitaria Proceso de Gestión Informática	Subdirector Administrativo	Director General
Fecha:	Ene. 26 de 2022	Ene. 26 de 2022	Ene. 26 de 2022
Firma:	Documento Original Firmado.	Documento Original Firmado.	Documento Original Firmado.