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

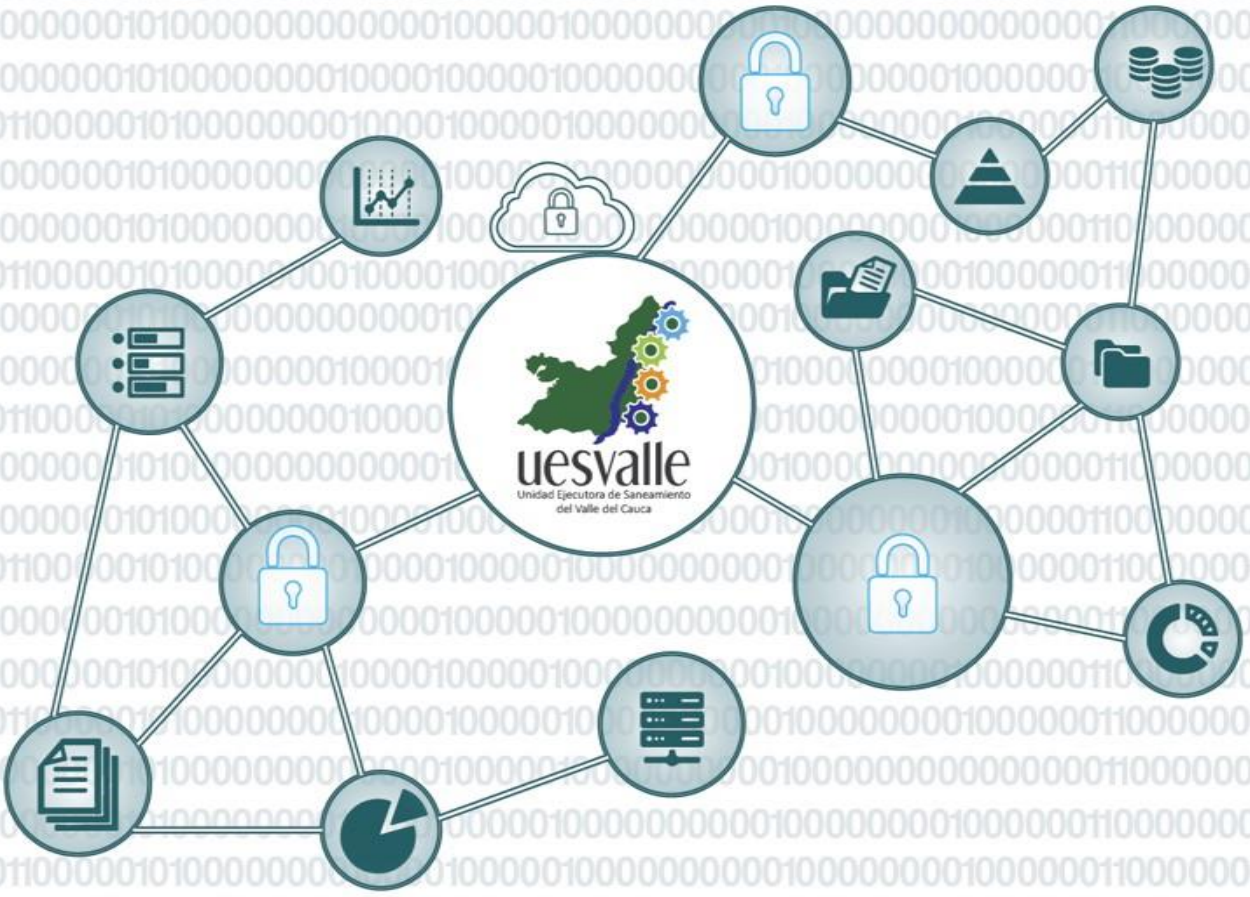


TABLA CONTENIDO

.

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.

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 UESVALLE.

Es importante resaltar que para la evaluación de riesgos en seguridad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación – (ver Tabla No.1 criterios de Clasificación y la Tabla No 2 Niveles de Clasificación) :

Tabla No.1 Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla No 2 Niveles de Clasificación

Alta	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
Media	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
Baja	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

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, 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.

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 UESVALLE 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).- Uso sistemático de la información para identificar las fuentes y estimar el riesgo. [ISO/IEC Guía 73:2002]

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 UESVALLE 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

19. Activo: Cualquier cosa que tenga valor para la organización. [NTC 5411- 1:2006]

20. Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

21. SEGURIDAD DE LA INFORMACIÓN. Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

22. Política: Toda intención y directriz expresada formalmente por la Dirección.

23. Riesgo: Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guía 73:2002]

24. Valoración del Riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo. [ISO/IEC Guía 73:2002]

25. Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. [ISO/IEC Guía 73:2002]

26. Tratamiento del Riesgo: Proceso de selección e implementación de medidas a para modificar el riesgo. [ISO/IEC Guía 73:2002]

1. OBJETIVO

Establecer una metodología que permitan la gestión del riesgo de seguridad de la información basados en los criterios de Confidencialidad, Integridad y Disponibilidad, que permitan la protección de los activos de información y que estos no afecten el objetivo misional de la UESVALLE.

1.1 OBJETIVOS ESPECÍFICOS:

Establecer lineamientos para la implementación y/o adopción de mejores prácticas de tratamientos de riesgos de seguridad y privacidad de la información en la UESVALLE.

Optimizar la gestión del tratamiento de los riesgos de seguridad y privacidad de la información.

Desarrollar una matriz, donde se establezca el inventario de los riesgos de seguridad y privacidad de la información que afecten a los activos de información de la UESVALLE con base a los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad), y se contemplen la identificación del riesgo, la valoración del riesgo inherente, evaluación de los controles existentes, nivel de riesgo residual, el tratamiento del riesgo y sus indicadores.

2. ALCANCE

El alcance del documento es proteger todos los activos de información de los procesos de la UESVALLE, a través de un adecuado tratamiento de los riesgos de seguridad y privacidad de la información para el año 2020, teniendo en cuenta la normativa vigente.

3. MARCO NORMATIVO.

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

Decreto 1078 de 2015-Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

NTC / ISO 27001:2013 - Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

NTC/ISO 31000:2009 - Gestión del Riesgo. Principios y directrices

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.

Guía No. 7 -Guía de gestión del riesgo, versión 3.0 – del Ministerio de Tecnologías de la Información y las Comunicaciones.

Guía para la administración del riesgo y el diseño de controles en UESVALLE es públicas - riesgos de Gestión, corrupción y Seguridad Digita. Versión 4.0- Departamento Administrativo de la Función Pública -DAFP

4. ETAPAS SUGERIDAS PARA LA GESTIÓN DEL RIESGO

De acuerdo con lo señalado en la Guía de Gestión del Riesgo del DAFP, se tienen tres etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a la UESVALLE tener una administración de riesgos acorde con las necesidades de la misma.

1ra. Etapa: la primera y más importante para lograr un adecuado avance en todo el proceso de administración del riesgo es el “Compromiso de las alta y media dirección” puesto que al igual que como se menciona en la guía, tener el verdadero compromiso de los directivos garantizan en gran medida el éxito de cualquier proceso emprendido, puesto que se necesita su aprobación y concurso en el momento de cualquier toma de decisiones, así mismo como se menciona en el MSPI la necesidad de tener aprobación de la dirección en cada etapa es necesaria.

Así mismo en concordancia con lo estipulado en la guía “debe designar a un directivo de primer nivel (debe ser el mismo que tiene a cargo el desarrollo o sostenimiento del MECI y el Sistema de Gestión de la Calidad) que asesore y apoye todo el proceso de diseño e implementación del Componente”, el MSPI se acoge puesto que lo que se busca es lograr una gestión integral del riesgo.

2da. Etapa: En segundo lugar se encuentra la “Conformación de un Equipo MECI o de un grupo interdisciplinario”, la idea de una integralidad en el tratamiento de los riesgos para poder tener una visión completa de la UESVALLE y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso, es esencial y ayuda a encaminar correctamente el MSPI, es por esta razón que se deben incluir los riesgos de seguridad en el momento que se hace el análisis para el MECI, o para el modelo de Gestión de Calidad.

3ra. Etapa: Finalmente se encuentra la “Capacitación en la metodología”, este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar ahora los riesgos de seguridad, sin embargo, dicho equipo debe estar integrado por alguno de los integrantes del proyecto MSPI, para tener un contexto Organizacional en todos los aspectos del desarrollo del MSPI.

5. VISION GENERAL PARA ADMINISTRACIÓN DEL SEGURIDAD DE LA INFORMACÓN

El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento *(ver imagen 1 proceso para la administración del riesgo y imagen 2 proceso para la administración del riesgo de seguridad de la información*).

- Proceso para la administración del riesgo:

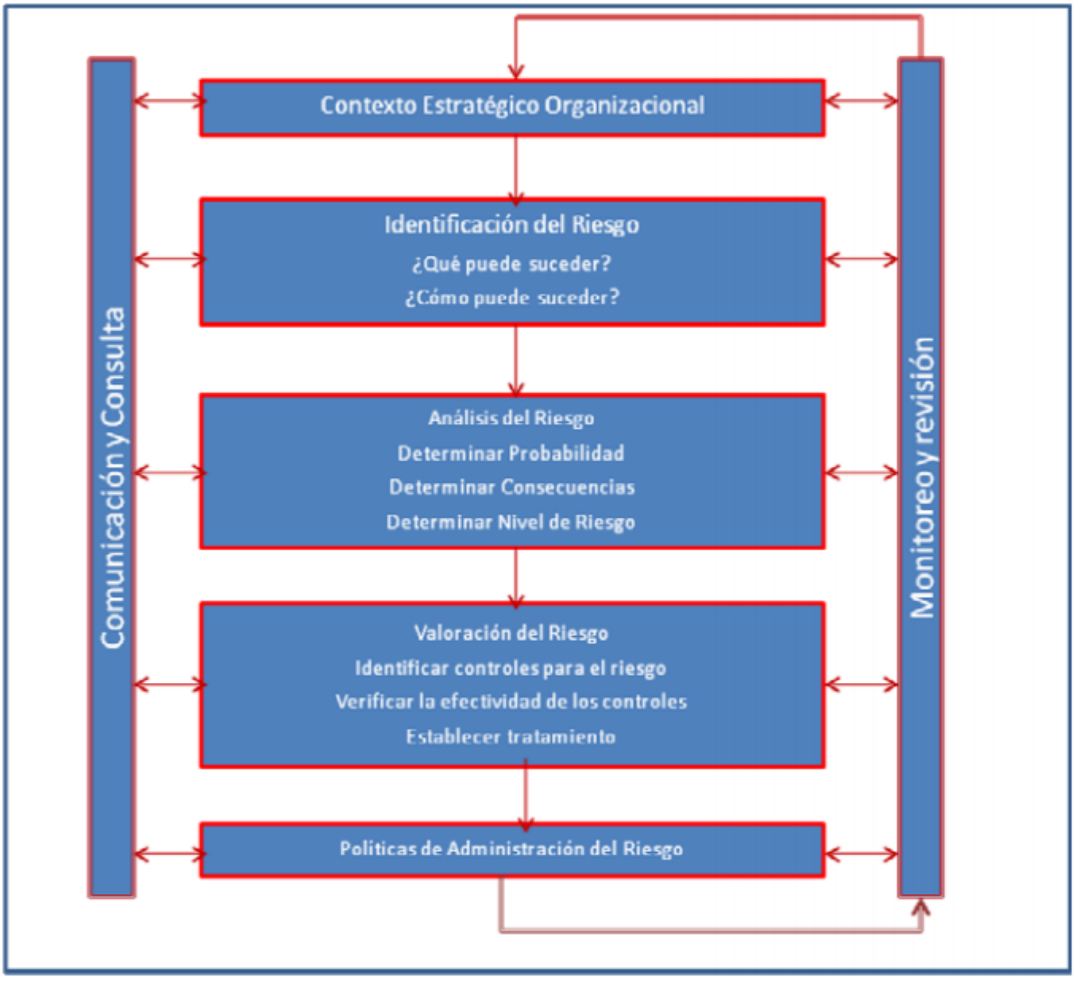


Imagen Proceso para la administración del riesgo - Tomado de la Cartilla de Administración de Riesgos del DAFP

- Proceso para la administración del riesgo de seguridad de la información

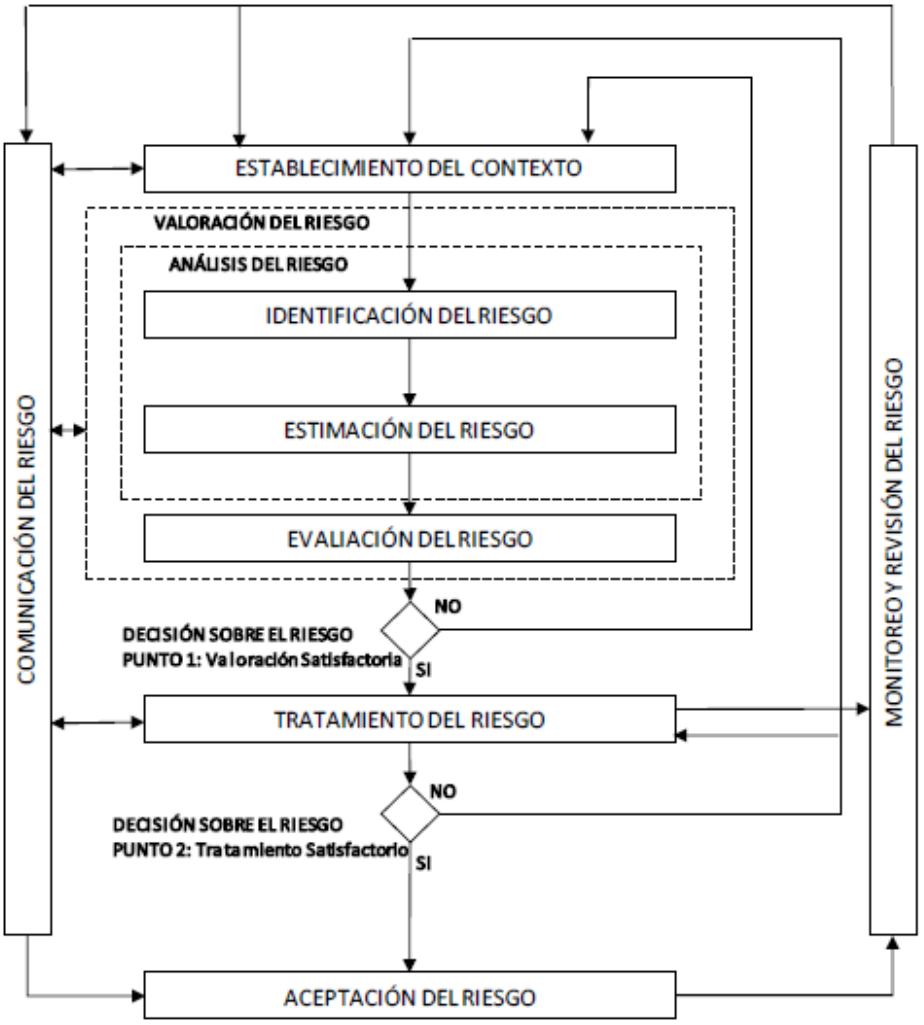


Imagen proceso para la administración del riesgo de seguridad de la información- Tomado de la NTC-ISO/IEC 27005

Así como lo ilustra la imagen 2 el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración.
El contexto se establece como primera medida, luego se realiza la valoración del riesgo y si esta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos a un nivel aceptable entonces la labor está terminada y sigue el tratamiento del riesgo.

Si la información no es suficiente, se llevará a cabo otra iteración de la valoración del riego con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo los criterios para aceptar el riesgo o los criterios de impacto).

La eficacia de tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es

posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual en esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo, criterios para la valoración del riesgo, de aceptación o de impacto del riesgo).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la UESVALLE. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo, por costos.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información –(Ver Tabla 3. Etapas del Modelo de seguridad y privacidad de la información).

ETAPAS DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDADDE LA INFORMACIÓN
Planear	✓ Establecer Contexto ✓ Valoración del Riesgo ✓ Planificación del Tratamiento del Riesgo ✓ Aceptación del Riesgo
Implementar	✓ Implementación del Plan de Tratamiento de Riesgo
Gestionar	✓ Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	✓ Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información

Tabla 3. Etapas del Modelo de seguridad y privacidad de la información - Etapas de la Gestión del Riesgo a lo Largo del MSPI del MINTIC.

6. CONTEXTO ESTRATÉGICO.

El contexto estratégico se tiene en cuenta en el proyecto del MSPI desde el inicio, sobre todo en el momento de definir el objetivo y el alcance del proyecto, así como la política de Seguridad de la UESVALLE, esto debido a que es necesario tener claro el entorno en el cual se desarrollará el proyecto, precisando cuál será el contexto en el que se desenvolverá, qué procesos involucrará, cual es el flujo de dicho o dichos procesos, y de ésta forma identificar sus objetivos y finalmente, de allí obtener los riesgos de Seguridad asociados.

De igual forma el personal asignado para el desarrollo del MSPI tiene como ventaja, el contexto estratégico avanzado para los modelos de Gestión establecidos en la UESVALLE, analizando los flujos de procesos ya identificados, para aportar su visión desde el MSPI.

Sin embargo, cabe mencionar que la Guía de Gestión del Riesgo del DAFP, señala las siguientes estrategias a través de las cuales se puede hacer ese levantamiento del contexto Estratégico:

1. Inventario de Eventos
2. Talleres de Trabajo
3. Análisis de Flujo de Procesos

Es esencial determinar el propósito de la gestión del riego en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. Este propósito puede ser:

- Dar soporte al modelo de seguridad de la información al interior de la UESVALLE.
- Conformidad legal y evidencias de la debida diligencia.
- Preparación de un BCP.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- El resultado de la especificación del contexto estratégico es la especificación de los criterios básicos alcance, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

7. CRITERIOS BÁSICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques, pero debe ser adecuado y que contenga criterios como: criterios de evaluación del riesgo, criterios de impacto, y criterios de aceptación del riesgo:

7.1 CRITERIOS DE EVALUACIÓN DEL RIESGO:

Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos:

- ✓ El valor estratégico del proceso de información para la UESVALLE
- ✓ La criticidad de los activos de información involucrados en el proceso
- ✓ Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- ✓ La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- ✓ Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la UESVALLE.

De igual modo, los criterios de evaluación de impacto del riesgo y se pueden utilizar para especificar las prioridades del tratamiento del riesgo.

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- *ver. (Tabla No. 4 criterios de Valoración de los activos de información).*:

Criterio de Valor	
Critico	=5
Alto	= 3 y < 5
Medio	= 1 y <3
Bajo	= 0 y <1

Tabla No. 4 criterios de Valoración de los activos de información.

7.2 CRITERIOS DE IMPACTO:

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la UESVALLE, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- ✓ Nivel de clasificación de los activos de información del proceso
- ✓ Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- ✓ Operaciones deterioradas
- ✓ Perdida del negocio y del valor financiero

- ✓ Alteración de planes y fechas limites
- ✓ Daños para la reputación
- ✓ Incumplimiento de los requisitos legales

7.3 CRITERIOS DE ACEPTACIÓN DEL RIESGO

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas La organización debería definir sus propias escalas para los niveles de aceptación del riesgo.

Durante el desarrollo, se deberían considerar los siguientes aspectos:

- ✓ Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- ✓ Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado
- ✓ Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual
- ✓ Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas
- Factores sociales y humanitarios

8. ALCANCE Y LÍMITES PARA LA GESTION DE RIESGOS EN SEGURIDAD DE LA INFORMACION

Es importante que la UESVALLE defina los límites y el alcance para de esta manera garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo.

Al definir el alcance y los límites la UESVALLE debería considerar la siguiente información:

- ✓ Objetivos estratégicos de negocio, políticas y estrategias de la organización
- ✓ Procesos del negocio
- ✓ Funciones y estructura de la organización

- ✓ Los requisitos legales, reglamentarios y contractuales aplicables a la organización
- ✓ La política de seguridad de la información de la organización
- ✓ El enfoque global de la organización hacia la gestión del riesgo
- ✓ Activos de información
- ✓ Ubicación de la organización y sus características geográficas
- ✓ Restricciones que afectan a la organización
- ✓ Expectativas de las partes interesadas
- ✓ Entorno sociocultural
- ✓ Interfaces (Ej. Intercambio de información con otras entidades)

9. IDENTIFICACIÓN DE RIESGOS

De acuerdo a lo planteado en la Guía de Gestión del Riesgo del DAFP, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la entidad a través del Contexto estratégico.

En este momento es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con éste punto se revisa la pertinencia del alcance planteado para el MSPI.
En esta etapa es especialmente importante la participación del personal designado para la implementación del MSPI, dentro de la mesa interdisciplinaria en la cual se revisan los procesos, tomando parte en la identificación de los riesgos de seguridad, para los procesos identificados como críticos dentro del planteamiento del MSPI.

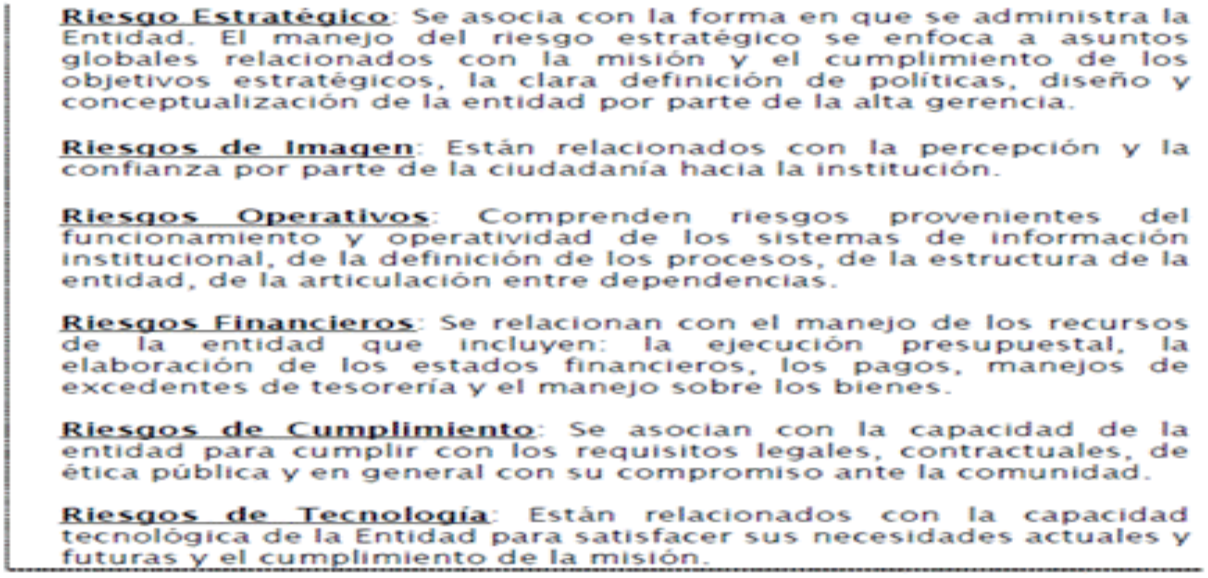
Para este capítulo, la Guía de Gestión del Riesgo del DAFP, inicia con la definición de algunos términos que son necesarios dentro del empleo de esta metodología, estos términos son comúnmente empleados en las entidades para efectos de la aplicación del sistema de Calidad o el MECI, y se listarán a continuación:

- ✓ Proceso.
- ✓ Objetivo del Proceso.
- ✓ Identificación de Activos.
- ✓ Riesgo.
- ✓ Causas (Amenazas y Vulnerabilidades).
- ✓ Descripción del Riesgo.
- ✓ Efectos de la materialización del Riesgo.

10. CLASIFICACIÓN DE LOS RIESGO:

Como acto seguido se debe realizar la clasificación de los riesgos, para esto la guía presenta las siguientes opciones- *ver (imagen No 3 lista de clasificación de Riesgo*):

Ilustración lista de Clasificación de Riesgos



Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Imagen. Lista de clasificación de Riesgo- Fuente: Guía de Riesgos DAFP

La entidad tiene la posibilidad de agregar a este listado los riesgos de seguridad que considere pertinentes dentro del desarrollo del MSPI en el proceso de identificación del riesgo, teniendo en cuenta cómo se podría vulnerar alguno de los pilares de la seguridad de la información:

- ✓ Disponibilidad
- ✓ Confidencialidad
- ✓ Integridad

10.1 RIESGO POR PERDIDA DE 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.

valor	Nivel	Descripción
5	Critico	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 UESVALLE.
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 UESVALLE.
0	Nulo	La falta o no disponibilidad de algún dato que posea el activo de

		información no afecta los procesos

10.2 RIESGO POR PERDIDA DE CONFIDENCIALIDAD.

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

valor	Nivel	Descripción
5	Critico	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 UESVALLE
3	Medio	Es la información que es utilizada por los funcionarios de la UESVALLE 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 UESVALLE. 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.

Tabla No.5

10.3 RIESGO POR PÉRDIDA DE LA 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.

valor	Nivel	Descripción
5	Critico	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 UESVALLE.
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 UESVALLE

Tabla No.6

11. ANÁLISIS DE RIESGOS

Para la UESVALLE es muy importante documentar y especificar cada una de las etapas surtidas para el proceso de Gestión de Riesgos, de allí la entidad tendrá su propia guía para poder replicar este mismo procedimiento para cualquier etapa que sea necesaria, ya sea para el momento en la que la UESVALLE decida extender el alcance de la aplicación del MSPI, o para la etapa de revisión de los controles, en la cual la entidad sólo debería poder aplicar la misma metodología simplemente teniendo como base el trabajo ya adelantado en las primeras etapas del MSPI.

11.1 ETAPAS DEL ANALISIS DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

A continuación, se presentan una serie de etapas propuestas para la Generación del análisis de riesgos de la UESVALLE, basadas la norma ISO27005.

11.1.1 IDENTIFICACIÓN DEL RIESGO

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

11.1.2 IDENTIFICACIÓN DE LOS ACTIVOS

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la UESVALLE y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Por lo cual se soportarán, en el Manual M-GI-04 gestión y clasificación de activos de información de la entidad para esta actividad.

11.1.3 IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la UESVALLE. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas.

Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas)

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación, se describen una serie de amenazas comunes – *(ver tabla No. 7 amenazas comunes)*:

D= Deliberadas, A= Accidentales, E= Ambientales

TIPO	AMENAZA	ORIGEN
Daño Físico	Fuego	A,D,E
	Agua	A,D,E
	Contaminación	A,D,E
	Accidente importante	A,D,E
	Destrucción del Equipo o medio	A,D,E
	Polvo, corrosión Congelamiento.	A,D,E
Eventos Naturales	Fenómeno Climáticos	E
	Fenómeno Sísmico	E
	Fenómeno Volcánico	E
	Fenómeno Meteorológico	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministros de agua o aire acondicionado.	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	E
Perturbación debida a la radicación.	Radiación electromagnética	E
	Radiación Térmica	E
	Impulsos electromagnéticos	E
Compromiso de la Información	Interceptación de señales de interferencia comprometida	
	Espionaje Remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Recuperación de medios reciclados o desechados.	
	Divulgación	
	Datos provenientes de fuentes no confiables.	
	Manipulación con Hardware	

	Manipulación con software	
	Detección de la posición	
Fallas técnicas	Fallas del equipo	
	Mal Funcionamiento del equipo	
	Saturación del sistema de información.	
	Mal funcionamiento del software	
	Incumplimiento en el manteamiento del sistema de información.	
Acciones no autorizadas	Uso no autorizado del equipo	
	Copia fraudulenta del software	
	Uso de software falso o copiado	
	Corrupción de los datos	
	Procesamiento ilegal de datos.	
Compromiso de las funciones	Error en el uso	
	Abuso de derechos	
	Falsificación de derechos	
	Negación de acciones	
	Incumplimiento en la disponibilidad del personal.	

Tabla No. 7- Amenazas Comunes

Es recomendable tener particular atención a las fuentes de amenazas humanas. Estas se desglosan específicamente en la siguiente tabla:

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	✓ Reto ✓ Ego ✓ Rebelión ✓ Estatus ✓ Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema. • Acceso no autorizado.
Criminal de la computación	✓ Destrucción de la información. ✓ Divulgación ilegal de la información. ✓ Ganancia Monetaria. ✓ Alteración no autorizada de los datos.	• Crimen por computador • Acto fraudulento. • Soborno de la información. • Suplantación. De idUESVALLE. • Intrusión en el sistema.
Terrorismo	✓ Chantaje ✓ Destrucción. ✓ Explotación. ✓ Venganza. ✓ Ganancia Política. ✓ Cubrimiento de los Medios de comunicación.	• Bomba/Terrorismo. • Guerra de la información. • Atauques contra el sistema DDoS. • Penetración en el sistema. • Manipulación en el sistema.
Espionaje Industrial (Inteligencia, empresas, gobiernos extranjeros	✓ Ventajas competitivas ✓ Espionaje	• Ventaja de defensa. • Ventaja Política.

otros intereses)	✓ Económico.	• Explotación Económica. • Hurto de información. • Intrusión de privacidad personal. • Ingeniería social. • Penetración en el sistema. • Acceso no autorizado en el sistema.
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	✓ Curiosidad ✓ Ego ✓ Inteligencia ✓ Ganancia monetaria ✓ Venganza ✓ Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

Tabla No.8

11.1.4 IDENTIFICACIÓN DE CONTROLES EXISTENTES

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.
Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo, se deberían considerar en la misma forma que aquellos que ya están implementados.

Un control existente planificado se podría calificar como ineficaz, insuficiente o injustificado, si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar o reemplazar por otro más adecuado.

Actividades para revisar controles existentes o planificados:

- Revisando los documentos que contengan información sobre los controles.
- Verificación con las personas responsables de la seguridad de la información y los usuarios.
- Efectuar revisiones en sitio comparando los controles implementados contra la lista de

controles que deberían estar.
- Cuáles están implementados correctamente y si son o no eficaces.
- Revisión de los resultados de las auditorías internas.

11.1.5 IDENTIFICACIÓN DE LAS VULNERABILIDADES

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes.
Se pueden identificar vulnerabilidades en las siguientes áreas:

- ✓ Organización.
- ✓ Procesos y procedimientos.
- ✓ Rutinas de gestión.
- ✓ Personal
- ✓ Ambiente físico
- ✓ Configuración del sistema de información.
- ✓ Hardware, software y equipos de comunicaciones.
- ✓ Dependencia de partes externas.

NOTA: La sola presencia de una vulnerabilidad no causa daños por si misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se enunciarán vulnerabilidades conocidas y métodos para la valoración de la misma.

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/ instalación fallida de los medios de almacenamiento.	Incumplimiento en el manteamiento del sistema de información.
	Ausencia de esquemas de reemplazo periódico.	Destrucción de equipos o medios.
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento.
	Sensibilidad a la radiación electromagnética	Radiación electromagnética.
	Ausencia de un eficiente control de cambios en la configuración	Error en el Uso.
	Susceptibilidad a las variaciones de voltaje	Perdida del suministro de energía.
	Susceptibilidad a las variaciones de temperatura.	Fenómenos meteorológicos.
	Almacenamiento sin protección	Hurtos medios o documentos.
	Falta de cuidado en la disposición final.	Hurto medios o documentos.
	Copia no controlada	Hurtos medios o documentos.
SOFTWARE	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos

	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de “terminación de sesión “Cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencias de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de Datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error de uso
	Ausencia de documentación	Erro de uso
	Configuración incorrecta de parámetros .	Error en el uso
	Fechas incorrectas	Error en el Uso
	Ausencia de mecanismos de identificación y autentificación de usuario	Falsificación de derechos.
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos.
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación con software
	Ausencia de copias de respaldo	Manipulación con software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos.
	Fallas en la producción de informes de gestión.	Uso no autorizado del equipo
RED	Ausencia de pruebas de envió o recepción de mensaje	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Trafico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Fallas del equipo de telecomunicaciones
	Punto Único de fallas	Fallas del equipo de telecomunicaciones
	Ausencia de identificación y autentificación de emisor y receptor	Falsificación de derechos.
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)	Saturación del sistema de información

	Conexión de red Pública sin protección	Uso no autorizado del equipo
PERSONAL	Ausencia Del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos y medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad.	Error en el uso.
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de los datos.
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos.
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería.	Uso no autorizado del equipo.
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos.	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación (puertas y ventanas)	
ORGANIZACIÓN	Ausencia de procedimientos formal para el registro y retiro de usuario	Abuso de los derechos
	Ausencia de proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respeto a la seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información.	Abuso de los derechos.
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos.
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Respuesta inadecuada de manteamiento del servicio.	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información.
	Ausencia de procedimiento de control de cambios	Incumplimiento en el manteamiento del sistema de información.
	Ausencia de procedimiento formal para la	Corrupción de datos.

	documentación del MSPI	
	Ausencia de procedimiento formal para la supervisión del registro del MSPI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público.	Datos provenientes de fuentes no confiables.
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información.	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso de correo electrónico	Error de Uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error de uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimiento para el manejo de información clasificada.	Error en el uso.
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles.	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información.	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado de equipo
	Ausencia de procedimientos para la prestación de informes sobre las debilidades en la seguridad	Uso no autorizado de equipo
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.	Uso de software falsificado o copiado.

Tabla No.9

11.1.6 MÉTODOS PARA LA VALORACIÓN DE LAS VULNERABILIDADES TÉCNICAS:

11.1.6.1 LEVANTAMIENTO DE INFORMACIÓN

En esta fase la UESVALLE debe recopilar la información necesaria para iniciar la actividad, dicha información puede ser organizada por parte del equipo de seguridad de la información de la UESVALLE.

La información recogida no solo debe permitir identificar los activos más importantes de la UESVALLE, relacionados con los procesos de la misma, ya sea misionales o de apoyo. También me debe permitir el conocer el contexto de la entidad, es decir, el entorno donde se proyectan los objetivos de la UESVALLE.

El grupo de personas que hace la recolección de información, debe reconocer el organigrama de la UESVALLE, mapa de procesos, política de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros, esta información es la base para la identificación de la brecha de seguridad que tiene la entidad.

En esta fase también se debe identificar los grupos de interés, al interior de la UESVALLE, como lo es control interno, tecnología, recursos humanos, calidad, comunicaciones, GEL, líderes de procesos. - ver imagen No. levantamiento de la información.

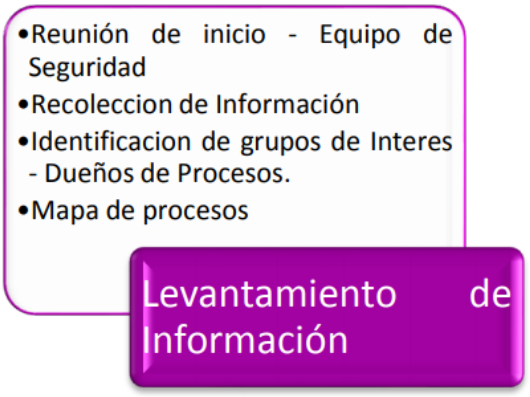


Imagen. Levantamiento de la Información

Para entender mejor esta fase, tenga presente las actividades de revisiones manuales e identificación de amenazas.

11.1.6.2 REVISIONES MANUALES

Las revisiones son inspecciones a los manuales que la UESVALLE debe realizar con el objetivo de identificar lo comprendido en seguridad por los servidores públicos, realizado en seguridad en los procesos y el estado de las políticas de la UESVALLE; dichas revisiones se hacen analizando la documentación, a través de reuniones con las personas a cargo de estos temas, dueños de los procesos.

Esta es una manera efectiva ya que a través de estas inspecciones se consigue identificar el porqué de las implementaciones de seguridad y sus controles en la UESVALLE. Permite comprobar si las personas comprenden los procesos de seguridad, si se ha tomado conciencia de las políticas de seguridad y privacidad que tiene la UESVALLE.

11.1.6.3 IDENTIFICACIÓN DE AMENAZAS

La identificación de amenazas no es otra cosa que la evaluación del riesgo que se realiza en la UESVALLE, es decir, es la evaluación de las actividades donde se ven involucradas las personas, la infraestructura y los procesos; con el objetivo de identificar las amenazas que se ciernen sobre la entidad. El resultado de estas actividades permite desarrollar planes de mitigación para las vulnerabilidades encontradas, orientar mejor los recursos y la ayuda a las áreas de la entidad que más lo requieren; la búsqueda de estas amenazas debe ser desde que se crean los procesos y durante su ciclo de vida.

Estas actividades deben tener un enfoque simple, es decir, descomponer los procesos a través de la evaluación manual, de manera que se sepa cómo funciona y su interrelación con las otras actividades.

- ✓ Definir y clasificar los activos de la entidad, evaluando su criticidad, sus posibles vulnerabilidades técnicas, operacionales y de gestión.
- ✓ Desarrollar una matriz con las amenazas potenciales, con sus vectores de ataque.
- ✓ Elaborar planes de mitigación para cada amenaza real.

El resultado de todo esto puede ser una serie de documentos, listas o diagramas, en los cuales se plasma los análisis de riesgo de la entidad y sus planes de mitigación a través de los controles sugeridos.

11.1.6.4 PRUEBAS Y ANÁLISIS

En esta fase la UESVALLE, podrá identificar los riesgos que se manifiestan a través de las debilidades en la implementación del modelo de seguridad y privacidad de la información y las vulnerabilidades que se presentan por la falta de controles de seguridad, que mitiguen los riesgos.

Estas pruebas están orientadas a evaluar la estructura de seguridad en la UESVALLE. Para esto se podrá revisar varios frentes de trabajo, como son el anexo A de la ISO 27001:2013, el ciclo de vida de la seguridad (PHVA), el nivel de madurez de la entidad de acuerdo a los niveles expuestos en el modelo de seguridad y privacidad y recomendaciones para que la entidad llegue a plasmar el concepto de Ciberseguridad.

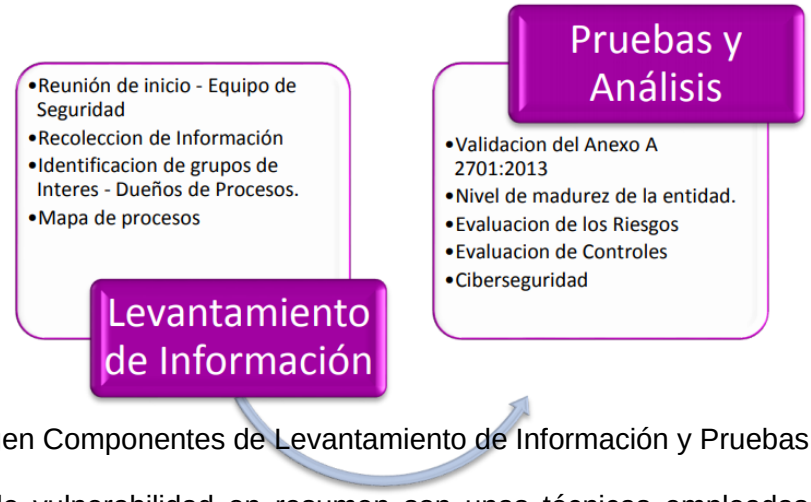


Imagen Componentes de Levantamiento de Información y Pruebas y Análisis

Las pruebas de vulnerabilidad en resumen son unas técnicas empleadas para comprobar la seguridad de una entidad. Las pruebas son esencialmente las pruebas sobre aplicaciones,

procesos y usuarios para encontrar vulnerabilidades.

Actualmente se encuentran diferentes técnicas y de cuándo usarlas, las cuales son necesarias para tener un marco de referencia del nivel de seguridad en la que estoy evaluando; así como tampoco hay una sola técnica que cubra todas las comprobaciones necesarias para evaluar todo lo requerido por la entidad.

Una orientación objetiva al realizar la evaluación, le permite a la entidad de manera equitativa realizar actividades manuales como pruebas técnicas; esto dará como resultado la posibilidad de una comprobación completa de lo avanzado en la implementación del modelo de seguridad y privacidad.

TIPOS DE PRUEBAS DE EFECTIVIDAD

Pueden realizarse 3 tipos de pruebas de efectividad, basados en el nivel de conocimiento del entorno o infraestructura de la UESVALLE:

- Pruebas Con Conocimiento Nulo Del Entorno: Es un tipo de prueba que simularía a un atacante real, ya que se basa en que tiene muy poco o nulo conocimiento del objetivo o su infraestructura.

- Pruebas Con Conocimiento Medio Del Entorno: Es cuando para la prueba de pentesting, se tiene más información sobre el ambiente que será atacado, es decir, direcciones IP, sistemas operativos, arquitectura de red etc… pero es información de igual manera limitada o media. Esto emula a alguna persona dentro de la red con conocimiento básico de la misma.

- Pruebas Con Conocimiento Completo Del Entorno: Es cuando el hacker tiene toda la información relacionada al sistema objetivo del ataque. Es generalmente para temas de auditoría.

ALCANCE DE LAS PRUEBAS

Deben existir reglas específicas para la ejecución de las pruebas de efectividad técnicas, para asegurar que dichas actividades no incurran en fallas mayores y se pueda afectar la infraestructura o las operaciones de la entidad.

Dentro del alcance se pueden definir los siguientes aspectos:

1- Plan De Trabajo: Debe definirse durante cuánto tiempo se realizarán las pruebas, los sistemas que harán parte de las pruebas, las actividades específicas, los procedimientos de contingencia en caso de alguna afectación etc….

2. Insumos: Que recursos son necesarios para realizar las actividades: Personal adicional, ventanas de tiempo, equipos etc…

3. Responsables: Quienes serán los encargados de efectuar las pruebas (sean proveedores o funcionarios de la entidad).

4. Afectaciones Posibles: El tipo de afectación que puede llegar a darse sobre cada sistema, también debe definirse si el objetivo es realizarlo en horario de producción o en horario de baja actividad laboral.

5. Multas o Sanciones: En caso de incumplir los parámetros anteriormente mencionados, deberán fijarse las sanciones disciplinarias o multas.

Estos alcances permitirán bien sea controlar internamente el desarrollo de las pruebas, como manejar los acuerdos de servicio con terceros que pueden llegar a realizar estos procedimientos.

11.1.6.5 PROCEDIMIENTO DE EJECUCIÓN DE PRUEBAS DE EFECTIVIDAD

Las pruebas de efectividad pueden realizarse por medio de las siguientes acciones de manera secuencial:

Imagen. Ciclo para la Ejecución de Pruebas de Efectividad Técnicas

Contextualización:

Esta fase se basa en identificar los alcances reales de las pruebas y de los procedimientos a ejecutar con base a las necesidades identificadas:

Dicha identificación de necesidades, puede darse por medio de las siguientes preguntas.

a. ¿Cuáles serán los objetivos a evaluar?
b. ¿Qué quiere alcanzar la entidad específicamente con estas pruebas?
c. ¿Si desea realizarlo en horas hábiles, no hábiles o fines de semana?
d. ¿Qué direcciones IP internas o externas serán objetivo de las pruebas (Si aplica)?
e. En caso de poderse vulnerar el sistema, que tipo de acciones posteriores solicita realizar (Pueden ser pruebas de vulnerabilidades en la máquina comprometida, escalamiento de privilegios etc)

f. Fechas de inicio y finalización de las actividades
g. ¿Se incluirán temas de ingeniería social?
h. ¿Qué temas de ingeniería social pueden ser válidos para ejecutar estos procedimientos?

Además de lo anterior, es importante tener en cuenta que estas pruebas no tienen como objetivo identificar solamente una vulnerabilidad sobre un sistema específico o algún sistema desactualizado, sino que la meta principal es identificar los riesgos de seguridad de la información a través de los controles que serán evaluados a través de las pruebas, para así tomar las medidas proactivas/preventivas para mitigar los riesgos encontrados.

Otros aspectos importantes para la contextualización del procedimiento son las siguientes:

- Establecer líneas de comunicación con los administradores de cada sistema a evaluar.
- Reportes parciales de avance de las pruebas con una frecuencia definida.
- Manejo de evidencias o soportes de las actividades.

Un punto final a tener en cuenta, es que estas pruebas también deben medir la efectividad de un sistema de monitoreo o detección, es decir, si se están realizando actividades de escaneo, ataques, infiltración, alteración de la información, exista una respuesta eficaz.

Reconocimiento del Objetivo:

Una vez se definen los alcances y necesidades, se procede con la fase de reconocimiento. Esta fase tiene por objetivo obtener tanta información del objetivo como sea posible para poder ser empleada en las fases de evaluación de vulnerabilidades y la fase de explotación.

Entre más información pueda obtenerse, más puntos de explotación podría encontrarse y aprovecharse en las siguientes fases.

Para realizar este levantamiento de información pueden utilizarse 3 métodos (enfocado a los sistemas de información):

- *PASIVO:* Este método aplica si la recolección de la información no implica acceder a ningún sistema de la entidad o generar tráfico que pueda ser detectado por alguno de sus sistemas. Generalmente es información que está disponible en otros sitios y puede estar desactualizada, sin embargo, puede llegar a ser útil.
- *SEMI-PASIVO:* En este punto, se apunta hacia los sistemas de la entidad, simulando ser tráfico normal proveniente de internet, sin emplear ningún método que pueda considerarse sospechoso por parte de los sistemas, es “camuflar el tráfico”. Como por ejemplo consultas DNS simples para verificar los servidores públicos.
- *ACTIVO*: Este método de obtención de información es el más propenso a ser detectado por los sistemas de detección y monitoreo, comprenden actividades como:

✓ Escaneo de puertos.
✓ Análisis de vulnerabilidad a puertos abiertos
✓ Búsqueda de directorios, archivos o servidores adicionales que no estén públicamente disponibles.

Otra información que puede obtenerse como punto de referencia contempla los siguientes temas:

- ✓ Relaciones con proveedores
- ✓ Acceso a información del personal, como extensiones telefónicas y direcciones de las sedes.
- ✓ Organigrama de la entidad.
- ✓ Direcciones de correo electrónico de funcionarios publicados en las páginas de la entidad.
- ✓ Bloques de direccionamiento IP adquirido.
- ✓ Tecnologías utilizadas por la compañía (información que puede obtenerse a través de ingeniería social hacia los proveedores).
- ✓ Identificar la presencia de equipos de respuesta a incidentes (CERT/CSIRT)
- ✓ Identificación de las instalaciones físicas.
- ✓ WHOIS lookups a través de LACNIC, RIPE, ARIN, IANA entre otros.

Modelado de Amenazas:

Esta fase maneja la relación atacante vs activo, es decir, el atacante que beneficio puede obtener si logra su objetivo de penetrar el sistema y modificar, borrar, copiar o destruir algún activo de información.
En resumen, esta fase se centra en realizar un análisis desde 2 frentes:

ENFOCADO EN LA ENTIDAD: Gestión del riesgo para determinar el apetito de riesgo de la entidad y para identificar los activos más críticos (o los que mayor impacto negativo pueden causar en caso de verse afectados). Este análisis busca resolver la incógnita “Que pasa si”, por ejemplo, que pasa si se divulga la información de mis sistemas de información, ¿Se vulnera la confidencialidad?, ¿Qué probabilidad existe de que este evento se materialice?, ¿Qué impacto tendría dicha divulgación?

Dentro de la gestión de riesgos se incluyen o se deben considerar los siguientes activos:

- ✓ Datos De Empleados
- Datos De Clientes
- Sistemas De Información
- Información Financiera
- Información De Mercadeo
- Políticas, Planes y Procedimientos
- Información Técnica (Diseños de infraestructura, información de configuración del sistema, cuentas de usuarios, cuentas de usuarios privilegiados)
- Personas
- Información generada a través de los diferentes procesos de negocio.
- Información de producto (Investigación y desarrollo, patentes etc.)

Si la entidad cuenta con este análisis, es importante revisarlo, ya que puede permitir identificar y perfilar ataques posibles y si los controles implementados si son suficientes.

ENFOCADO EN EL ATACANTE: Identificando los posibles agentes o grupos que podrían llegar a perpetrar algún tipo de ataque hacia la entidad. Dicha identificación está centrada en los siguientes grupos:

Internos	Externos
Empleados	Sociedades
Administrativos, Ejecutivos	Competidores
Administradores De Infraestructura	Contratistas
Desarrolladores	Proveedores
Ingenieros	Crimen Organizado
Técnicos	Hacktivistas
Contratistas	Hackers Tipo Script Kiddies
Soporte Remoto	

Tabla No. Posibles Agentes de Ataque a una Organización.

Dentro de las poblaciones que más ataques pueden llegar a generar se encuentran los empleados inconformes y los empleados a nivel ejecutivo, que pueden llegar a aprovechar sus usuarios con privilegios adicionales para vulnerar el sistema para sus propios fines.

Análisis de Vulnerabilidades: Es el proceso de descubrir falencias en los sistemas y aplicaciones que pueden llegar a ser aprovechados por un atacante. Dichas falencias pueden ser descubiertas a nivel del host o en la administración o configuración o diseño del mismo. Dependiendo de la amplitud de los alcances propuestos, el análisis de vulnerabilidad puede variar desde analizar un servicio o host específico o a un inventario completo de máquinas.

Estos procesos de análisis pueden ejecutarse también de dos maneras:

1ra. ANÁLISIS ACTIVO

El análisis activo involucra tener un contacto directo con el objetivo a probar. Puede hacerse de manera automática o de manera manual bajo diversas actividades conjuntas.

a. MÉTODO AUTOMATIZADO:
Se denomina método automatizado dado que se utiliza un software para que este haga la interacción con el objetivo, generalmente realiza varios procedimientos de análisis de manera simultánea, dando ventajas significativas de tiempo y esfuerzos respecto a los métodos manuales.

Un ejemplo de las ventajas, es por ejemplo ejecutar un telnet hacia un puerto para verificar si este responde o está abierto, repetir este proceso para los más de 60 mil puertos es una labor tediosa y un software puede ejecutarla.

Dentro de los métodos automáticos para análisis se encuentran:

- Escáneres de puertos.
- Escáneres basados en servicios.
- Lectura de Banners.

- Escáneres específicos para servicios web.
- Software para ataques o escaneo de fuerza bruta.
- Escáneres de red.
- Escáneres para tráfico de voz.
- Múltiples nodos de ataque.

2da. ANÁLISIS PASIVO

Esto implica métodos como análisis de metadatos en archivos publicados en internet, que pueden contener información sobre el tipo de servidor, nombres de dominio, direccionamiento IP, etc... También incluye el monitoreo de tráfico o copiado de tráfico (espejo de puertos) para captura y posterior análisis.

INVESTIGACIÓN: Una vez se realiza la verificación de las vulnerabilidades con base a los métodos anteriores, es necesario investigar en las diferentes bases de datos para comprobar la veracidad de lo que se ha encontrado y las posibles maneras de apalancar o aprovechar las fallas identificadas. Para ello se dispone de las siguientes fuentes de información:

- Bases de datos de vulnerabilidades (CVE)
- Alertas o publicaciones de proveedores de plataformas.
- Bases de datos de exploits.
- Passwords por defecto de plataformas específicas.
- Guías de hardening (endurecimiento) para plataformas.
- Investigación propia (empleando virtualización o duplicación de máquinas por
- ejemplo).

Una vez se realiza la investigación, se deben confirmar las vulnerabilidades encontradas en un archivo consolidado, con su respectiva justificación y los tipos de ataque que podrían ejecutarse con base a los mismos.

Explotación

Esta fase se centra puramente en obtener acceso al sistema, apalancando las debilidades identificadas en la etapa anterior o sobrepasando los controles de seguridad existentes. Dentro de las técnicas de explotación más utilizadas se encuentran las siguientes:

1. Evasión: implica realizar las pruebas de penetración escapando de los sistemas de detección, pueden implicar desde seguridad física (evadir una cámara) hasta evadir un sistema tipo IDS/IPS.

2. Ataques de precisión: Uso de ataques bien focalizados, es decir, no empezar a atacar objetivos de manera indiscriminada sino bien estructurada y puntual.

3. Ataques personalizados con base a tecnologías/medios de transmisión: Dependiendo del medio de transmisión (cableado, vía WiFi,

4. Exploits adaptados o complementados: Tomar exploits ya existentes y adaptarlos para las plataformas o sistemas objetivos.

5. Enfoque de día zero: Si se encuentra alguna vulnerabilidad nueva, idear la manera de aprovecharla para ejecutar algún ataque.

6. Exploits comunes: Buffer overflow, SEH (Structured Exception Handler), ROP (Return Oriented Programming).

7. Crackeo De SSID (WIFI): Movimientos enfocados a apalancar vulnerabilidades sobre este medio y sus protocolos de encripción como (WEB, WPA, EAP-FAST etc…)

8. Ataques al usuario (Ingeniería social): Con base a los temas encontrados en la fase de modelado de amenazas, emplear los ataques de ingeniería social al personal de la organización para obtener passwords, documentación adicional etc…

9. Hombre en el medio (Man In-The-Middle): Ataques de interceptación de tráfico, donde se suplanta el direccionamiento bien sea físico o IP.

10.VLAN Hopping: Este método de ataque consiste en engañar a dispositivos conmutadores (switches) con el fin de ganar acceso a la red como un dispositivo confiable, los métodos más comunes son VLAN HOPPING y Switch Spoofing.

11.Análisis de código fuente: (Puede ser tanto de aplicaciones como de sistemas operativos que dispongan de código abierto).

Existen aún más métodos de ataque, con los cuales se puede intentar lograr el objetivo de vulnerar o acceder a los sistemas. Una vez se logre el objetivo de ingreso, deberán documentarse los hallazgos de una manera evidente y concreta para utilizar la información como herramienta de mejora.

Post-explotación

Una vez se encuentra comprometido el sistema o host (fase anterior), se procederá a identificar qué tipo de información puede obtenerse, a que otros sistemas de información se puede ingresar desde el sistema capturado, identificar opciones de configuración, información de red (direccionamiento IP de VLAN, servidores vecinos, direcciones físicas, etc.), todo esto con el objetivo principal de determinar el valor de la máquina para la organización.

Es importante tener en cuenta que a este punto ya se vulneró el sistema y no es necesario dañarlo o desestabilizarlo gravemente (a menos que el plan desde el principio así lo indique).

Por lo tanto, se debe definir un alcance máximo a ejecutar para las siguientes acciones:

- Escalamiento de privilegios
- Acceso a datos específicos (bases de datos, repositorios, fileservers, ftp)
- Denegación de servicios (CRÍTICO)
- Obtención de passwords para otros sistemas**.**
- Acceso a logs de dispositivos.
- Ingreso a servidores Web, DNS, proxy, servidores de impresión
- Acceso a directorios activos o LDAP, para obtener información de usuarios (cuentas de correo electrónico, extensiones o dependencias donde trabajan), información que puede

emplearse para posteriores ataques de ingeniería social.

- Ingreso a las entidades certificadoras, que podría afectar la creación de certificados, revocación e incluso la encripción de dichos certificados si se llega a comprometer la llave.
- Acceso a los sistemas de almacenamiento, para verificar información sobre tipos de backup, medios empleados etc.
- Ping Sweeps (Barridos A VLANS para identificar hosts).
- Instalación de exploits remotos.
- Instalación de backdoors para posterior ingreso y que no se afecten por los
- reinicios de los hosts.
- Modificación de los servicios.

Reporte

Es necesario documentar todos los resultados obtenidos en cada fase, para tener soportes de las labores realizadas y a su vez la respectiva justificación de los resultados finales. Es importante tener en cuenta las audiencias a las cuales se les presentará el reporte, dado que no es conveniente entrar en demasiados detalles cuando la audiencia será de tipo administrativo y así mismo cuando la audiencia es de tipo técnico, no se disponga de un reporte más preciso y específico.

REPORTE GERENCIAL:

Puede contener la siguiente información:

- Introducción, justificación y objetivos alcanzados durante las pruebas.
- Calificación De Riesgo, ubicando los activos que mayor riesgo pueden traer a la organización con base al criterio del ejecutor de la prueba de efectividad de los controles.
- Motivos o causa raíz de las vulnerabilidades encontradas, entre las cuales se pueden encontrar razones como:
    - ✓ Máquinas sin parches.
    - ✓ Sistemas operativos sin el hardening adecuado.
    - ✓ Máquinas con servicios activos no utilizados.
    - ✓ Contraseñas débiles o faciles de adivinar.
    - ✓ Diseños o arquitecturas de sistemas inseguros, servicios de red sin hardening.
    - ✓ Firmware de dispositivos obsoleto.
- Plan de trabajo para solucionar todas las falencias encontradas, pueden manejarse plazos trimestrales, semestrales y anuales para determinadas labores que requieran ejecutarse

REPORTE TÉCNICO:
Este reporte puede contener la información anterior, pero incluyendo los aspectos más importantes a nivel técnico, dado que quienes reciban esta información serían quienes ejecuten las acciones de mejora para cada vulnerabilidad encontrada:

- ✓ Recolección de información basada en recursos publicados por la propia entidad.
- ✓ Información recolectada en plataformas como google, bing, páginas de referencia etc…
- ✓ Información que pudo ser recolectada en las plataformas publicadas como, estructura de

la organización, unidades de negocio, mercados, proveedores etc…
- ✓ Inteligencia con el personal interno, donde se evidencia la información que pudo obtenerse por medio de ingeniería social (solo en primera instancia, no para solicitar claves o accesos).
- ✓ Vulnerabilidades encontradas (clasificadas bien sea por los servicios, plataformas o hosts).
- ✓ Explotación de las vulnerabilidades (cuales fueron apalancadas o pudieron ser aprovechadas en cada host y cuales no).
- ✓ Actividades de POST-Explotación efectuadas en cada host comprometido con la prueba.

Una vez se finaliza el reporte, se espera que la entidad inicie con las actividades propuestas para cerrar las brechas y aumentar la efectividad de los controles implementados o se implementen otros que cumplan con las expectativas de seguridad de la información.

11.1.6.6 IDENTIFICACIÓN DE LAS CONSECUENCIAS

Para la identificación de las consecuencias es necesario tener:
- ✓ Lista de activos de información y su relación con cada proceso de la UESVALLE.
- ✓ Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros.

En esta actividad se deben identificar los daños o las consecuencias para la UESVALLE que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas a un activo.

La UESVALLE, podrá identificar las consecuencias operativas de los escenarios de incidentes en términos de:
- ✓ Tiempo de investigación y reparación
- ✓ Pérdida de tiempo operacional
- ✓ Pérdida de oportunidad
- ✓ Salud y seguridad
- ✓ Costo financiero
- ✓ Imagen, reputación y buen nombre.

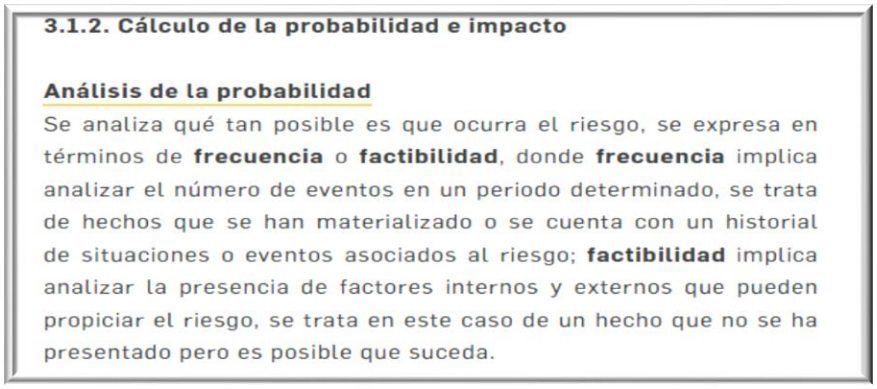
12. EVALUACIÓN DE RIESGO

Para continuar con el análisis y la evaluación del riesgo depende de la información obtenida en las fases de identificación anteriormente descritas de Identificación de los riesgos, es por ello que la UESVALLE debe crear los criterios de riesgo definiendo los niveles de riesgo aceptado por la Organización.

De esta forma la Guía de Gestión del Riesgo del DAFP, menciona cuales son los pasos claves en el análisis de riesgos, probabilidad e impacto, definiendo como sigue cada uno de ellos:

“Por Probabilidad”, se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo

determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado – en las siguiente imágenes No. 4 se presenta el análisis de la probabilidad y la tabla No.10 de los criterios para calificar la probabilidad por parte del DAFP.



3.1.2. Cálculo de la probabilidad e impacto

Análisis de la probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de **frecuencia** o **factibilidad**, donde **frecuencia** implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; **factibilidad** implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Imagen Análisis de la Probabilidad Fuente: DAFP

Tabla 2. Criterios parar calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Tabla No 10 Criterios para Calificar la Probabilidad.

Fuente. DAFP

“Por Impacto “, se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo”, en la siguiente tabla No 11 se presenta los criterios para calificar el impacto- riesgo de gestión por parte del DAFP.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Tabla No 11 - Criterios para calificar el impacto- Riesgo de gestión por parte del DAFP.
Por otro lado, se presenta la tabla en la cual se señalan “los impactos de mayor ocurrencia en las Entidades del Estado”, en éste punto se toca el impacto sobre la Confidencialidad de la Información, el cual es uno de los pilares de la Seguridad de la Información.

Tabla No. 7 Nivel de Impacto Sobre la Confidencialidad de la Información

NIVEL	CONCEPTO
1	Personal
2	Grupo de Trabajo
3	Relativa al Proceso
4	Institucional
5	Estratégica

Fuente: Guía de Riesgos DAFP

Este puede ser el punto de partida para la inclusión de los temas de seguridad de la Información dentro del análisis hecho para los procesos que se cubrirán según el alcance del MSPI, así pues, podría extenderse el análisis hacia la Integridad y la Disponibilidad de la Información

De esta forma se procede a hacer la “calificación del riesgo”, en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

De igual forma la guía presenta una “tabla de probabilidad” y una “Tabla de Impacto”, en las cuales presenta 5 niveles para medir la probabilidad de ocurrencia y 5 niveles para lograr medir el impacto, dando las herramientas con las cuales se definen los criterios de riesgo.

Por otro lado presenta la tabla en la cual se señalan “los impactos de mayor ocurrencia en las UESVALLEes del Estado, en éste punto se toca el impacto sobre la Confidencialidad de la Información, el cual es uno de los pilares de la Seguridad de la Información.

13. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ENTIDAD

Riesgo se puede definir como la probabilidad de que una amenaza pueda afectar una vulnerabilidad o debilidad de una UESVALLE 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.

La UESVALLE definió el documento F-DE-13 MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DIGITAL, donde se consagra todo lo relacionado a la implementación del plan de tratamiento de riesgos y privacidad de la información de la ENTIDAD.

13.1. 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.

13.2. 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.

13.3. 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.

La UESVALLE definió el procedimiento P-GI-06 Gestión y Clasificación de Incidente de Seguridad de la Información. Con el objetivo de reducir los riesgos de seguridad y privacidad de la información con relación a los diferentes eventos no deseados o inesperados que se puedan presentan durante las ejecuciones de las actividades de la UESVALLE.

13.4. 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 UESVALLE 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 UESVALLE y que afectan de manera directa o indirecta algún proceso.

13.5. Tipos de activos

Activos Esenciales:

Datos importantes o vitales para la Administración de la UESVALLE: Aquellos que son esenciales, imprescindibles para la continuidad de la UESVALLE; es decir que su carencia o daño afectaría directamente a la UESVALLE, 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 UESVALLE, 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.

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.

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

14.1. 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 o encuestas 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.

14.2. 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.

15. CRONOGRAMA DE ACTIVIDADES DEL PLAN DE TRATAMIENTO - 2020

Actividad	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Realizar diagnostico										
Realizar inventario de activos										
Identificar y clasificación riesgos con responsables de procesos										
Elaborar matriz de valoración de activos y análisis de riesgos										
Valoración del riesgo residual										
Plan de Tratamiento de Riesgos.										
Seguimiento y Control										

Tabla No.12

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.

16. PROYECCION DE PRESUPUESTO CUMPLIMIENTO PLAN DE TRATAMIENTO DE RIESGOS

A continuación se presentan las actividades y la proyección presupuestal para cumplir con dicha actividad:

No.	ACTIVIDADES	Descripción	EJECUCION 2020
1.	Cumplir con el plan de acción de la estrategia de gobierno digital y MIPG.	Implementar y actualizar el plan de tratamiento de riesgos de seguridad y privacidad de la información.	$40.000.000

17. NOTAS DE CAMBIO

FECHA	VERSIÓN INICIAL	MOTIVO DEL CAMBIO Y NUMERALES MODIFICADOS	VERSIÓN FINAL
01 Enero de 2019	0.0	Versión inicial del documento	1.0
Ene. 30 de 2020	1.0	Se adiciona, términos de conceptualización, objetivos específicos, marco normativo, se adiciona nuevos puntos que ayudan a comprender la forma de darle los tratamientos a los riesgos de seguridad y privacidad de la información.	2.0

18. APROBACIÓN

	Elaboró	Revisó	Aprobó
Nombre:	Robert Andrey Fernández de Córdoba Flórez	Constanza Ivette Hernández Fernando Girón Vanderhuk Álvaro José Cruz Montoya	Diego Victoria Mejía
Cargo:	Profesional Universitario Gestión Informática	Asesora de Planeación Subdirector Administrativo Profesional Universitario SGC	Director General
Fecha:	Ene. 30 de 2020	Ene. 30 de 2020	Ene. 30 de 2020
Firma:			