ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

FORMATO DE APROBACIÓN DOCUMENTAL

CÓDIGO: DESI-FM-008 | **VERSIÓN: 11**

FECHA DE APLICACIÓN: MAYO 2019

INFORMACIÓN DOCUMENTADA:		CÓDIGO:		VERSIÓN:		JUSTIFICACIÓN:		
TIPO	NOMBRE	ANTERIOR	VIGENTE	ANTERIOR	VIGENTE	ELABORA	ACTUALIZA	ANULA
Documento Interno	Políticas de Seguridad para la Gestión de Riesgos	-	EGTI-DI-013	-	1	X		

DESCRIPCIÓN DE LA JUSTIFICACIÓN:

Se elabora el Documento Interno EGTI-DI-013 Políticas de Seguridad para la Gestión de Riesgos con el fin de alinear la política de Gestión del Riesgo con el Modelo de Seguridad y Privacidad de la información (MSPI) y la Gestión del Riesgo que define MINTIC, con la implementación de las políticas de seguridad de la información de la Entidad, la administración de la seguridad de los activos de información y los lineamientos para la Administración de los Riesgos que ha definido la UAERMV para sus procesos, a través de la aplicación del Documento Externo DESI-DE-002 Guía para la Administración de los Riesgos, Corrupción y Seguridad Digital y el Diseño de Controles en la Entidades Públicas.

AVALA: **LÍDER DE PROCESO** *(Puede ser el Líder Estratégico o Líder Operativo dependiendo del proceso)*	**ELABORA/ACTUALIZA/ANULA:** *(Colaborador del proceso en compañía del enlace)*	**ACOMPAÑAMIENTO:** **ASESOR OAP** *(Colaborador de la Oficina Asesora de Planeación a cargo de procesos)*
(Firma)	*(Firma)*	*(Firma)* Andrea del P. Zambrano
Nombre: Marcela Rocío Márquez Arenas	*Nombre: Gloria Méndez/ Omar Garzón/ Yuly González*	*Nombre: Andrea del Pilar Zambrano Barrios.*
Cargo: Secretaría General	*Cargo: Contratistas Secretaría General -Proceso EGTI*	*Cargo: Contratista Proceso DESI*

TRÁMITE DE APROBACIÓN DOCUMENTAL (DILIGENCIADO POR LA OFICINA ASESORA DE PLANEACIÓN)	**¿ES APROBADO?**		**FECHA DE APROBACIÓN:**	**RESPONSABLE DEL SISTEMA DE GESTIÓN DE CALIDAD**
	SI [X]	**NO** [ ]	30-05-2019	
	OBSERVACIONES:			*(Firma)*
				Martha Patricia Aguiar Copete
				REPRESENTANTE DE LA ALTA DIRECCIÓN

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

POLÍTICA DE SEGURIDAD PARA LA GESTION DE RIESGOS.

Bogotá, D.C.,
(MAYO DE 2019)

CONTENIDO

1. INTRODUCCIÓN

El siguiente documento hace parte de la POLÍTICA GENERAL DE TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÖN Y COMUNICACIONES de la entidad.

La Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial - UAERMV, basará la Administración de la Seguridad de los Activos de Información, en las políticas contenidas en este documento; así mismo, como las buenas prácticas y herramientas informáticas que favorezcan las actividades del proceso de apoyo: "Gestión de Servicios de Infraestructura Tecnológica" (GSIT).

La gestión integral de riesgos es un principio prioritario en la actuación de los colaboradores de la entidad.

La gestión de riesgos es la combinación de administrar el recurso humano, los procesos, los proyectos, las instalaciones y la implementación de mecanismos de prevención y mitigación de los riesgos identificados. Así mismo, la construcción de una cultura proactiva de conciencia y autocontrol frente al manejo del riesgo. Finalmente, la gestión integral de riesgos tiene como propósito reducir la probabilidad de ocurrencia y afectación en la continuidad de la operación de los procesos que utilicen los sistemas de información y la infraestructura tecnológica de la Entidad.

El riesgo es un aspecto inseparable de los procesos y debe ser adecuadamente administrado y gestionado, siendo por ello necesario analizar y considerar la existencia de condiciones, situaciones o eventos que pueden desencadenarse y resultar en consecuencias negativas para la entidad, sus empleados, el medio ambiente, la comunidad o sus partes interesadas.

2. GLOSARIO DE TERMINOS

- **Apetito de Riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que se toma para modificar la exposición al riesgo, bien sea para disminuir la probabilidad de ocurrencia del evento o para disminuir su impacto.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Disponibilidad:** Capacidad de un componente o servicio para realizar su función requerida durante un periodo de tiempo.
- **Gestión Integral de Riesgos:** Es el proceso de identificación, valoración y control de los riesgos que amenazan el logro de los objetivos de la entidad.
- **Identificación de riesgos:** Es el proceso de encontrar, reconocer y definir los escenarios de riesgo, sus causas y sus potenciales consecuencias.
- **Integridad:** propiedad de exactitud y completitud.
- **Proceso:** Grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de la entidad para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
- **Responsable del Riesgo:** Persona o entidad que tiene la responsabilidad y autoridad para gestionar el riesgo a través de la implementación de los planes de mitigación.
- **Riesgo:** El riesgo es la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. Es esa vulnerabilidad y amenaza a que ocurra un evento y sus efectos sean negativos y que los activos puedan verse afectados por él.
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **Riesgo inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior, es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **Seguridad de la Información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.
- **Tolerancia al Riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Tratamiento del riesgo (Plan de Mitigación):** Selección y aplicación de medidas, con el fin de poder modificar la magnitud del riesgo, para evitar de este modo los daños intrínsecos de materializarse.
- **GSIT:** Gestión de Servicios de Infraestructura Tecnológica.
- **EGTI:** Estrategia y Gobierno de TI.
- **Impacto:** Es el resultado de la materialización de un evento, se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Probabilidad:** Se refiere a la posibilidad de ocurrencia de un riesgo potencial.
- **Usuario:** Persona que utiliza los servicios diarios.
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

3. OBJETIVO GENERAL

Suministrar los lineamientos sobre las acciones que se deben adelantar al interior la entidad, encaminadas a disminuir la probabilidad de ocurrencia y el impacto de todas aquellas situaciones que puedan interferir con la continuidad de la operación de la infraestructura tecnológica y los sistemas de información que afecten el funcionamiento de los procesos de la entidad.

4. OBJETIVOS ESPECIFICOS

- Minimizar la materialización de los riesgos asociados a la infraestructura tecnológica y sistemas de información.
- Identificar las principales amenazas y vulnerabilidades a los que están expuestos los activos de información.
- Garantizar la disponibilidad, confidencialidad e integridad de los activos de información de la entidad, minimizando el riesgo que se pueda generar por la fuga o perdida de alguna credencial de acceso.
- Gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad).

5. ALCANCE

El alcance de los lineamientos que se definen en esta política da cubrimiento a:

a) Identificación de amenazas asociadas a los activos de información.
b) Identificación de vulnerabilidades asociadas a los activos de información.
c) Identificación del riesgo inherente.
d) Tratamiento del riesgo.
e) Aplicación de controles.

Todos los colaboradores de la Unidad: Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas y demás personal que tengan asignados activos de información y que luego de realizar su valoración de riesgos, se categoricen en extremo, deberán realizar la identificación de los riesgos inherentes de mencionados activos, así como aplicar los controles necesarios para minimizar dicho riesgo.

6. DECLARACIÓN

En este documento se encuentran los lineamientos que aseguran una actuación adecuada para alcanzar un alto nivel en cuanto a seguridad de la información en la UAERMV. La información es un activo importante para la entidad, tiene un alto valor para la misma, por esto mismo la unidad ha definido las directrices de seguridad para los Activos de Información, por medio de las cuales se deben orientar todas las acciones a seguir.

Estas directrices hacen parte del marco de POLÍTICAS GENERALES DE TECNOLOGÍA Y SEGURIDAD DE INFORMACIÓN Y COMUNICACIONES y están basadas en:

- La NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información publicado por la *International Organization for Standardization* y la Comisión Electrotécnica Internacional. La versión más reciente es la ISO/IEC 27002:2013)
- La norma ISO 27005 que contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información.
- Anexo 4, lineamientos para la gestión de riesgos de seguridad digital en entidades públicas modelo de gestión de riesgos de seguridad digital (MGRSD).
- Guia 7, guia de gestion de riesgos (MSPI).

Por lo anterior, se busca minimizar los riesgos asociados a los activos de información, asegurar la continuidad de la UAERMV y ayudar en el cumplimiento de los objetivos misionales.

6.1. Acuerdo de confidencialidad:

Todos los Usuarios que administran, leen, modifican o crean información en la UAERMV deben firmar un acuerdo de confidencialidad o de no divulgación como parte de sus términos y condiciones iníciales de empleo. Esta directriz también incluye a personal ocasional y los Usuarios externos no contemplados en un contrato formalizado.

7. ROLES Y RESPONSABILIDADES

7.1. Encargado de seguridad de la información: Se designará al responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información, el cual debe pertenecer a la Secretaría General, a través del proceso Estrategia y Gobierno de TI (Proceso Estratégico) y tendrá responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital, que se describen a continuación:

- Definir el procedimiento para la Identificación y Valoración de Activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

8. POLÍTICA DE SEGURIDAD PARA LA GESTION DE RIESGOS

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso: "Integridad, confidencialidad y disponibilidad".

La entidad, se compromete a gestionar los riesgos, identificando y administrando los eventos potenciales que pueden afectar la plataforma estratégica, los objetivos institucionales y los procesos de la entidad. Para la adecuada gestión integral del riesgo en la UAERMV, se presenta los siguientes lineamientos:

1. Se adoptarán las metodologías para gestionar los riesgos de la entidad a través del análisis del contexto (DOFA de la UAERMV), entendido como el entorno externo e interno, y la valoración de los mismos, es decir, su identificación, análisis y evaluación, y su posterior tratamiento, todo esto manteniendo comunicación y consulta constante y permanente monitoreo y revisión, para evitar así su materialización.

Tabla 1 Contexto Estratégico

CONTEXTO	CATEGORIA	DESCRIPCIÓN
Contexto Externo	ECONÓMICOS:	• **Disponibilidad de capital**: Es la apropiación presupuestal aprobada para una vigencia fiscal de la entidad. • **Liquidez**: Capacidad con la que cuenta una entidad para hacer frente a sus obligaciones financieras. • **Mercados financieros**: Se refieren tanto al mecanismo a través del cual se intercambian activos financieros (como acciones, bonos y futuros) entre agentes económicos, como al lugar donde se determinan sus precios. • **Desempleo**: Situación de la persona que está en condiciones de trabajar, pero no tiene empleo o lo ha perdido. • **Competencia**: Conjunto de entidades que compiten por algo, especialmente por un producto dispuesto en el mercado.
	POLÍTICOS:	• **Cambios de gobierno**: Cambios en políticas, planes, programas, prioridades y proyectos relacionados al gobierno. • **Legislación**: Cambios en la normatividad en vigencia. • **Políticas públicas**: Son un conjunto de acciones y decisiones encaminadas a solucionar problemas propios de las comunidades.
	SOCIALES:	• **Demografía:** poblaciones humanas según su estado y distribución en un momento determinado o según su evolución histórica. • **Responsabilidad social**: compromiso u obligación que los miembros de una sociedad, ya sea como individuos o como miembros de algún grupo, tienen tanto entre sí, como para la sociedad en su conjunto. • **Orden público**. Situación o estado de paz y de respeto a la ley de una comunidad. "El Estado es garante del orden público; solo podrán prohibirse las manifestaciones cuando existan razones fundadas de alteración del orden público"
	TECNOLÓGICOS:	Avances en tecnología o acceso a sistemas de información externos. Ej. Gobierno en línea.
	AMBIENTALES:	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	COMUNICACIÓN EXTERNA:	Mecanismos utilizados para entrar en contacto con los usuarios o la ciudadanía. Canales establecidos para que la ciudadanía se comunique con la entidad.

CONTEXTO	CATEGORIA	DESCRIPCIÓN
Contexto interno	FINANCIEROS:	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL:	Competencia y disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS:	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA:	Integridad de los datos, disponibilidad de datos y sistemas, desarrollo, producción y mantenimiento de sistemas de información.
	ESTRATÉGICOS:	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA:	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
Contexto del proceso	DISEÑO DEL PROCESO:	Claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS:	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD:	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	PROCEDIMIENTOS ASOCIADOS:	Pertinencia en los procedimientos que desarrollan los procesos.
	RESPONSABLES DEL PROCESO:	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	COMUNICACIÓN ENTRE LOS PROCESOS:	Efectividad en los flujos de información determinados en la interacción de los procesos.
	ACTIVOS DE SEGURIDAD DIGITAL DEL PROCESO:	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso de cara al ciudadano.

Fuente: Guía DAFP

2. Asegurar los recursos necesarios para ayudar a los responsables a gestionar y tratar los riesgos.
3. Los riesgos que se gestionan en la UAERMV, se encuentran relacionados en las matrices dispuestas para ello, y que están publicadas en www.umv.gov.co/transparencia asi como la identificación, valoración y tratamiento.
4. Identificación de los Activos de Información:

Los pasos para identificar los activos son:

4.1. Listar los activos por cada proceso: En cada proceso deberán listarse los activos indicando algún consecutivo, nombre y descripción breve de cada uno. Se deberá revisar

desde el proceso de Gestión Documental las matrices identificadas, y articularlas para este ejercicio.

4.2. Identificar el dueño de los activos: Cada uno de los activos identificados deberá tener un dueño designado (Dependencia/ dependencia o proceso), si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

4.3. Clasificar los activos: Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros (ver tabla 2).

4.4. Clasificar la información: Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, y demás normatividad aplicable. Esto adicionalmente ayudará a dilucidar la importancia de los activos de información en el siguiente Paso 4.5.

4.5. Determinar la criticidad del activo: Se debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

4.6. Se deben identificar las vulnerabilidades de los activos: La entidad debe identificar vulnerabilidades y amenazas.

Tabla 2. Clasificación de Activos

CLASIFICACION DE ACTIVOS	DESCRIPCION
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.

CLASIFICACION DE ACTIVOS	DESCRIPCION
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros
Hardware	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
Know How - Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software)
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Intangibles	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros
Personas	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
Informacion	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
Instalaciones	Espacio o Dependencia asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: MINTIC

Tabla 3 Vulnerabilidades y amenazas

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
HARDWARE	Mantenimiento insuficiente/Instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento 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

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Susceptibilidad a las variaciones de voltaje	Pérdida 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	Hurtos 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 en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación, como la 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

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	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
	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico 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
	Conexiones de red pública sin protección	Uso no autorizado del equipo
	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 Dependencia susceptible de inundación	

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Red energética inestable	
	Ausencia de protección física de la edificación (Puertas y ventanas)	
ORGANIZACION	Ausencia de procedimiento formal para el registro y retiro de usuarios	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 respecto 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	Abuso de los derechos
	administradores y operadores	
	Respuesta inadecuada de mantenimiento 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 procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para la documentación del MSPI	Corrupción de datos
	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

TIPO DE ACTIVO	EJEMPLOS DE VULNERABILIDADES	EJEMPLOS DE AMENAZAS
	Ausencia de políticas sobre el uso de correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de procedimientos 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 presentación 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

Fuente: ISO 27005

5. Se deben identificar las amenazas de los activos: Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

5.1. Deliberadas (D)
5.2. Accidentales (A).
5.3. Ambientales (E).

Tabla 4 Amenazas más comunes

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 medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	E
	Perdida de suministro de energía	E
	Falla en equipo de telecomunicaciones	
Perturbación debida a la radiación	Radiación electromagnética	
	Radiación térmica	
	Impulsos electromagnéticos	
Compromiso de la información	Interceptación de señales de interferencia comprometida	
	Espionaje remoto	
	Escucha encubierta	
	Hurto de medios o documentos	
	Hurto de equipo	
	Recuperación de medios reciclados o desechados	
	Divulgación	
	Datos provenientes de fuentes no confiables	
	Manipulación con hardware	
	Manipulación con software	

TIPO	AMENAZA	ORIGEN
	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 mantenimiento 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	

Fuente: ISO 27005

6. Se deben identificar los riesgos de los activos.
7. Se debe realizar una descripcion de los riesgos.
8. Se debe revisar la probabilidad y el impacto de ocurrencia de los riesgos.

Para lo anterior, es necesario tener en cuenta las siguientes tablas que dan cuenta de como se debe revisar el impacto y la probabilidad según lo sugerido por la Guía de Administración de Riesgo de Gestión, Corrupción y Seguridad Digital del DAFP.

Tabla 5 Probabilidad

PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi Cierta	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de una 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 podría 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 4 años.

1	Raro	El evento puede ocurrir solo en circunstancias excepcionales. (poco comunes o anormales)	No se ha presentado en los últimos 4 años.

Fuente: DAFP

Tabla 6 Impacto

IMPACTO DE SEGURIDAD DIGITAL		
Niveles para calificar el impacto		**Impacto (consecuencias) Cualitativo**
1	**Insignificante**	Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad
2	**Menor**	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad
3	**Moderado**	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros
4	**Mayor**	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
5	**Catastrófico**	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros

Fuente: DAFP

9. Se debe calcular el riesgo inherente.
10. Se deben aplicar los controles a los riesgos identificados: Esa identificación se debe realizar basado en la Guía de DAFP, que se describe en Manual Política Administración del Riesgo.
11. Los controles deben tener una frecuencia de aplicación.
12. La tolerancia es el nivel del riesgo que la entidad puede o está dispuesta a soportar, que corresponden a los riesgos que se encuentren en zona residual Baja y los que se encuentran en otra zona se trataran de acuerdo a los lineamientos establecidos por la entidad.
13. La entidad revisará y actualizará la política de Gestión de Riesgos de acuerdo con los cambios del entorno, las nuevas metodologías y los resultados de los indicadores de gestión asociados a la materialización de riesgos definidos.
14. Los riesgos identificados en la entidad, deberán ser monitoreados permanentemente, para asegurar que los controles sean eficaces y eficientes, y obtener información para mejorar la evaluación y gestión de los riesgos e identificar la materialización oportuna de los riesgos.
15. Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo procedimientos de Gestión de Riesgos con los que cuenta la entidad.
16. Comunicar interna y externamente, los resultados de la gestión del riesgo desarrollada institucionalmente, reportando en el Mapa Institucional de Riesgos, los riesgos priorizados de acuerdo con los procedimientos de Gestión de Riesgos.
17. Las opciones del tratamiento a los riesgos que se evalúan en la entidad son:
    - 17.1. **Evitar el riesgo:** Se logra cuando al interior de los procesos se genera cambios sustanciales por rediseño, eliminación o cancelación de una actividad o conjunto de actividades que causan el riesgo, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
    - 17.2. **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.
    - 17.3. **Compartir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o dependencias, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.
    - 17.4. **Asumir el riesgo:** Despues de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo. No aplica para los riesgos de corrupción, estos siempre deben conducir a un plan de acción o de tratamiento para mitigarlo.

REVISIÓN Y APROBACIÓN:

Elaborado y/o Actualizado por EQUIPO OPERATIVO SIG del Proceso:	Validado por RESPONSABLE DIRECTIVO SIG del Proceso:	Aprobado por:
OMAR FERNANDO GARZÓN / GLORIA MÉNDEZ Contratistas / Proceso EGTI		
Acompañamiento EQUIPO TÉCNICO SIG:		
ANDREA DEL PILAR ZAMBRANO Contratista/ Proceso DESI	Firma: MARCELA ROCÍO MÁRQUEZ ARENAS Secretaria General	Firma: MARTHA PATRICIA AGUILAR COPETE Representante de la Alta Dirección

CONTROL DE CAMBIOS:

VERSIÓN	DESCRIPCIÓN	FECHA	APROBADO Representante de la Alta Dirección SIG
1	Actualizado por el Ing. Omar Fdo. Garzón Giraldo (Especialista en Seguridad de la Información), ajustes realizados para alinear la política a la Guía 7 del Modelo de Seguridad y Privacidad de la Información (MSPI) y Guía 4 de MINTIC sobre Gestión de Riesgos.	Mayo 2019	Jefe Oficina Asesora de Planeación