1. OBJETIVO:

Definir las actividades para la gestión de los riesgos de seguridad digital dentro del marco de la Política de Administración de Riesgos – UPME y su alineación con la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" del DAFP.

2. ALCANCE:

Este procedimiento aplica para la gestión de riesgos de Seguridad Digital en todos los procesos, dependencias y niveles de la UPME, iniciando con la identificación de los activos de información de mayor criticidad y continuando con las diferentes etapas de gestión de riesgos (identificar, evaluar, controlar y monitorear).

3. RESPONSABLES:

Líderes y dueños de los procesos, serán los responsables de los Riesgos de Seguridad Digital, son los encargados de revisar y aprobar los resultados finales, en relación con las etapas de identificación, medición y tratamiento de los riesgos de Seguridad Digital y tendrán a cargo la identificación, medición y definición de planes de tratamiento.

Profesional Responsable de Seguridad de la Información de la Oficina de Gestión de Información - OGI, será el encargado de liderar y acompañar un adecuado y efectivo ejercicio en la gestión de Riesgos de Seguridad Digital que afecten el cumplimiento de los objetivos de cada uno de los procesos de la UPME.

4. GLOSARIO:

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. (Guía DAFP)

ACTIVO DE INFORMACIÓN: En relación con la seguridad y la privacidad de la información, se refiere al componente que contiene información pública o privada que la entidad genere, obtenga, adquiera, transforme o controle.

ADMINISTRACIÓN DE RIESGOS: Proceso adelantado por la Alta Dirección y todo el personal de la entidad, para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.

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

AUTENTICIDAD: Característica que busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidad.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

CAUSA: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo

CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

CAUSA RAÍZ: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

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.

CONTROL: Medida que permite reducir o mitigar un riesgo.

DISPONIBILIDAD: Característica de la información, que indica que esta debe estar disponible en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso, solo para las personas autorizadas.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Cualquier ocurrencia relacionada con los activos o el entorno que indique un posible compromiso de las políticas o la falla de los controles, o incluso una situación no asignada que pueda afectar la seguridad.

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

GESTIÓN DE RIESGOS EN LA UPME: Proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información.

IMPACTO: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos o procesos de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento, entre otros.

INTEGRIDAD: Propiedad de exactitud y completitud de la información que indica que ésta debe ser precisa, coherente y completa desde su creación hasta su destrucción. Solo se podrá modificar la información mediante autorización.

PROBABILIDAD: Posibilidad de ocurrencia del riesgo

PROPIETARIO DE LA INFORMACIÓN: Área de la organización que tiene la responsabilidad de definir quién tiene acceso o no, a determinada información, qué controles requiere la información y en qué condiciones se concede el acceso.

RIESGO: El riesgo se define como la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

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 del ambiente físico, digital y las personas.

RIESGOS DE INFORMACIÓN: Está asociado con la probabilidad de que las amenazas exploten vulnerabilidades de un activo de información o grupo de activos de información y por lo tanto causar un daño a la organización

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

RIESGO INHERENTE: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente.

SEGURIDAD DE LA INFORMACIÓN: Conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

TRATAMIENTO DEL RIESGO: Proceso de selección e implementación de acciones de mejora que permita gestionar el riesgo. Busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad, Integridad y Disponibilidad de los activos), evitando aquellas situaciones que impidan el logro de los objetivos Institucionales.

VULNERABILIDAD: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

VALORACIÓN DEL RIESGO: Proceso de análisis y evaluación del riesgo, que permite la identificación y el análisis de los riesgos que enfrenta la Entidad para la consecución de sus objetivos institucionales, tanto de fuentes internas como externas relevantes.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

5. LINEAMIENTOS O POLÍTICAS DE OPERACIÓN Y CONTROL

A continuación, se describen los lineamientos y normas aplicables adoptados por la UPME para la Gestión de Riesgos de Seguridad Digital:

5.1. Activos de Información. (Guía para la administración del riesgo y el diseño de controles en entidades públicas).

Como primer paso para la gestión de los riesgos de seguridad digital, se debe realizar el inventario de activos de información (Matriz de activos de la información), el cual es el principal insumo para la gestión de riesgos de seguridad de la información. Por lo cual, cada uno de los procesos de la UPME debe identificar, establecer y actualizar los activos de información de cada proceso y valorarlos de acuerdo con su nivel de criticidad.

5.2. Guía para la administración del riesgo y el diseño de controles en entidades públicas.

La UPME ha documentado la Política para la Gestión Integral de Riesgos de acuerdo con las declaraciones de la alta dirección y las intenciones generales de la entidad con respecto a la gestión del riesgo (NTC ISO 31000:2018 Numeral 5.2 Liderazgo y Compromiso), herramienta guía para la identificación y tratamiento de los riesgos, priorizando los de mayor criticidad.

5.3. Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas - Anexo 4.

La UPME utiliza como herramienta el Anexo 4 LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS 2018 de MinTIC como complemento a lo definido en la Guía para la Administración del Riesgo de Gestión, Corrupción y Seguridad Digital.

Este anexo presenta el diseño de Controles en Entidades Públicas (con un enfoque hacia el entorno digital), exponiendo los siguientes ítems:

- Identificación de activos
- Catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad digital.
- Controles para la mitigación de los riesgos de seguridad digital.
- Reporte de riesgos de seguridad digital y otros aspectos adicionales para llevar a cabo una gestión adecuada del riesgo de seguridad digital.

5.4. Política para la Gestión Integral del Riesgos UPME

La Política para la Gestión Integral del Riesgo en la Unidad de Planeación Minero-Energética – UPME contempla el presente procedimiento (Procedimiento de Gestión de Riesgos de Seguridad Digital), así como los lineamientos para la identificación, y valoración de los riesgos que puedan afectar el cumplimiento de la misión de la entidad.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

5.5. Metodología y acompañamiento para la gestión de riesgos de seguridad digital

La OGI participa y/o acompaña a los delegados y líderes de los procesos en las etapas para la gestión de riesgos de seguridad digital (identificar, evaluar, controlar y monitorear), iniciando con:

- La identificación de los activos críticos de cada proceso.
- La identificación de los riesgos, su valoración y evaluación del tratamiento a aquellos activos que resulten con criticidad alta.

Teniendo en cuenta lo anterior, la tipología de riesgos inherentes de seguridad digital que se podrán identificar es la siguiente:

- Pérdida de integridad.
- Pérdida de confidencialidad.
- Pérdida de disponibilidad.

En la identificación y descripción del riesgo de seguridad digital, se deben considerar y analizar las amenazas y vulnerabilidades que posibilitan la materialización de los riesgos inherentes y que se han identificado en cada uno de los procesos de la UPME.

Es de aclarar que los dueños de los procesos deberán participar activamente en cada una de las etapas de la gestión de riesgos de Seguridad Digital, deberán acompañar, revisar, aceptar o emitir comentarios a los informes de los análisis de riesgo realizados.

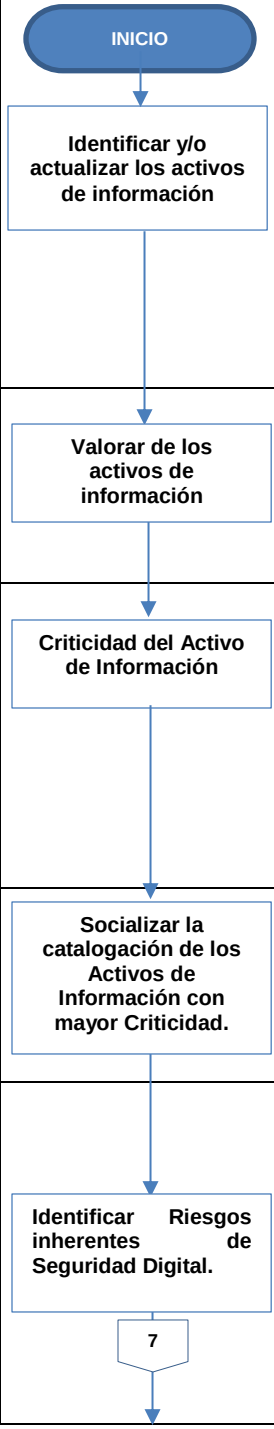
5.6. Niveles de aceptación al riesgo

Los niveles de aceptación del riesgo se determinan como resultado de la valoración de la probabilidad de ocurrencia del riesgo y de la magnitud del impacto al momento de evaluar su materialización. Los riesgos de seguridad digital inherentes, ubicados en la zona de riesgos “Baja y Moderada” pueden ser aceptados por la UPME y por lo tanto no es necesario establecer controles; no obstante, se realizará seguimiento y monitoreo periódico para asegurar que el riesgo aún se mantiene en estos niveles.

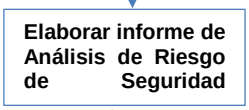
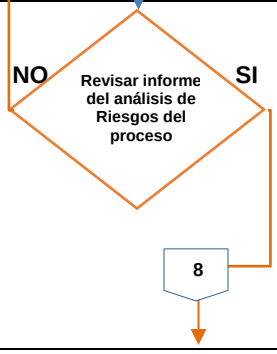
Los riesgos de seguridad digital que se encuentren fuera del nivel aceptable de la UPME; es decir, en las zonas “Alta y Extrema”, será necesario emprender por parte de los Líderes y dueños de los procesos un plan de tratamiento con los mecanismos que permitan modificar la probabilidad de ocurrencia y/o impacto de los riesgos de seguridad digital.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

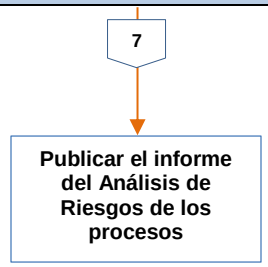
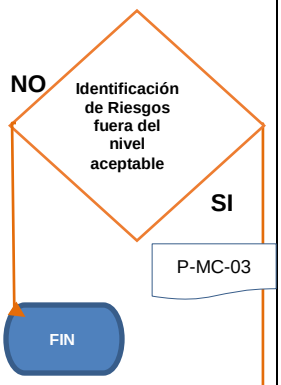
6. DESARROLLO Y FLUJOGRAMA DEL PROCEDIMIENTO

No. /PC	Flujograma	Actividades	Responsable	Registro o documento
1		El profesional de la OGI se reunirá con cada uno de los dueños de los procesos, a fin de identificar, establecer y actualizar los activos de información. *Nota: La identificación o actualización del inventario de activos de información se realiza anualmente o cuando se requiera por cambios en la normatividad vigente, modificaciones en la estructura organizacional de la UPME o en su mapa de procesos.*	Responsables de cada proceso Profesional OGI Responsable de Seguridad de la Información	Inventario de activos de la información
2	**Valorar de los activos de información**	Los dueños de los procesos a partir del inventario de activos de información identificados realizan la valoración de acuerdo con los principios de seguridad de la información: integridad, confidencialidad y disponibilidad.	Responsables de cada proceso	Inventario de activos de la información.
3	**Criticidad del Activo de Información**	El profesional de la OGI a partir de la valoración de los activos de información realizada por los dueños de los procesos ejecuta una catalogación, a fin extraer los activos de mayor criticidad sobre los cuales se realiza el análisis de riesgos. El resultado de esta catalogación será remitido a cada dueño de proceso a fin de solicitar su respectiva verificación y aprobación	Profesional OGI Responsable de Seguridad de la Información	Inventario de activos de la información.
4	**Socializar la catalogación de los Activos de Información con mayor Criticidad.**	El profesional de la OGI socializa el resultado de la catalogación de los Activos de Información con mayor Criticidad y la Metodología con la cual se desarrollarán los análisis de riesgos de Seguridad Digital a los procesos de la UPME	Profesional OGI Responsable de Seguridad de la Información	Registro de asistencia de la socialización.
5	**Identificar Riesgos inherentes de Seguridad Digital.** 7	Una vez identificados los activos de información críticos de cada uno de los procesos, estos serán actualizados dentro de la matriz de análisis de riesgos de seguridad digital y se procede a realizar la identificación de riesgos de Seguridad Digital bajo los criterios de integridad, confidencialidad y disponibilidad.	Responsables de cada proceso Profesional OGI Responsable de Seguridad de la Información	Matriz de Riesgos de Seguridad Digital.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

No. /PC	Flujograma	Actividades	Responsable	Registro o documento
6		Esta etapa consiste en evaluar dentro de la matriz de análisis de riesgos de seguridad digital, los riesgos identificados con el fin de determinar la probabilidad y el impacto de estos. se debe tener en cuenta: - El impacto se valora de acuerdo con las consecuencias que puede ocasionar la materialización del riesgo; se refiere a la magnitud de sus efectos. - La probabilidad se valora desde la posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse. *Nota: El resultado de combinar la probabilidad con el impacto, genera el riesgo inherente que se visualiza en el mapa de calor de la matriz de riesgos.*	Responsables de cada proceso Profesional OGI Responsable de Seguridad de la Información	Matriz de Riesgos de Seguridad Digital.
7		Consiste en determinar los controles que actualmente se tienen para mitigar los riesgos y causas identificadas con el fin de evaluar la efectividad en la implementación de los controles y reducir la severidad de los riesgos. *Nota: El resultado de aplicar la efectividad de los controles al riesgo inherente, genera el riesgo residual que se visualiza en el mapa de calor de la matriz de Riesgos de Seguridad Digital.* Actividad para desarrollar con el acompañamiento del Profesional de la OGI Responsable de Seguridad de la Información.	Responsables de cada proceso	Matriz de Riesgos de Seguridad Digital.
8		Una vez generada la matriz de riesgos (inherente/residual) se procede a elaborar el informe del análisis de riesgos de cada proceso evaluado, el cual deberá ser enviado por correo electrónico a cada dueño de proceso para su revisión y aprobación.	Profesional OGI Responsable de Seguridad de la Información	Informe de análisis de riesgos para cada proceso/ Correo electrónico/ Matriz de Riesgos de Seguridad Digital
9 PC		**Punto de Control** Una vez recibido el correo remitido por el Profesional de la OGI, se procede a la revisión del informe para emitir aprobación o comentarios. **Si** están de acuerdo remiten aprobación mediante correo electrónico dirigido al profesional de la OGI y se continúa con la actividad **No.10** Publicar el informe del Análisis de Riesgos de los Procesos. Si **no** están de acuerdo y se requieren modificaciones o eliminaciones se debe informar por correo electrónico al profesional de la OGI y se devuelve a la actividad **No. 7** Control de los Riesgos.	Profesional Especializado 2028-13 del GIT de Planeación	Aprobación o devolución del documento en el gestor documental

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

No. /PC	Flujograma	Actividades	Responsable	Registro o documento
10		Envía solicitud por correo electrónico al GIT Planeación para la Publicación en Sígueme, del informe del análisis de riesgos de seguridad digital de cada uno de los procesos.	Jefatura de la OGI Profesional OGI Responsable de Seguridad de la Información	Correo electrónico Matriz de Riesgos de Seguridad Digital.
11 PC		**Punto de Control** Se identifica si existen riesgos fuera del nivel tolerable. **Si** se detectan riesgos fuera del nivel aceptable, el responsable de cada proceso deberá generar un plan de tratamiento (aplicar P-MC-03 *ACCIONES PREVENTIVAS, CORRECTIVAS Y DE MEJORA.)* y se continúa con la actividad **No.12** monitorear riesgos. Si **no** existen riesgos fuera del nivel aceptable finaliza el procedimiento y se vuelve a analizar en la próxima vigencia.	Jefatura de la OGI Profesional OGI Responsable de Seguridad de la Información Responsables de cada proceso	Plantilla de seguimiento de los riesgos fuera del nivel tolerable de UPME Matriz de Riesgos de Seguridad Digital.
12		Se realiza monitoreo de acuerdo con la periodicidad definida en el plan de tratamiento a los riesgos fuera del nivel aceptable de la UPME, con el fin de validar el estado de implementación del plan de tratamiento con los mecanismos que permitan minimizar la probabilidad de ocurrencia y/o impacto.	Responsables de cada proceso Profesional OGI Responsable de Seguridad de la Información	Plantilla de seguimiento de los riesgos fuera del nivel no aceptable de la UPME
13		Socializar en el Comité de Gestión y Desempeño los riesgos con severidad fuera del nivel tolerable de la UPME, y su respectivo plan de mitigación; con el fin de dar un estatus de la implementación de las mejoras por parte de los responsables de cada uno de los procesos.	Jefatura de la OGI Profesional OGI Responsable de Seguridad de la Información.	Jefatura de la OGI Profesional OGI Responsable de Seguridad de la Información.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción de los cambios**
19/09/2022	1	Creación procedimiento de Riesgos de Seguridad Digital de la UPME.

UPME - Av. Calle 26 # 69 D-91 Torre 1, Piso 9°
Bogotá D.C. Colombia
PBX: +57 601 222 06 01
Línea Gratuita Nacional: 01 8000 91 17 29
Sede electrónica http://www.upme.gov.co