CONTENIDO.

1. OBJETIVO 4
2. ALCANCE 4
3. DEFINICIONES 4
4. DESARROLLO 11
4.5. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS 15
4.6. SEGURIDAD CON DISPOSITIVOS MÓVILES 16
4.7. POLÍTICA DE USO DE DISPOSITIVOS CORPORATIVOS 16
4.8. POLÍTICA DE USO DE DISPOSITIVOS NO CORPORATIVOS 18
4.9. POLÍITICA DE CONEXIONES REMOTAS 20
4.10. SEGURIDAD DE LOS RECURSOS HUMANOS 23
4.11. GESTIÓN DE ACTIVOS 26
4.11.1. Uso aceptable de los activos 26
4.11.2. Inventario de activos información. 27
4.11.3. Devolución de los Activos 27
4.11.4. Clasificación de la Información 27
4.12. USO DE EQUIPOS DE CÓMPUTO DE PROPIEDAD DE LA ANM 28
4.13. USO DE INTERNET 29
4.14. USO DEL CORREO INSTITUCIONAL 30
4.15. GESTIÓN DE MEDIOS REMOVIBLES 31
4.16. DISPOSICIÓN DE LOS MEDIOS 32
4.16.1. Transferencia de medios físicos 33
4.17. CONTROL DE ACCESO 33
4.17.1. Lineamientos Control de Acceso 33
4.17.2. Acceso a Redes y Servicios en Red 33
4.17.3. Solicitud o inicio de acceso 34
4.17.4. Suspensión o terminación de acceso 36
4.17.5. Revisión o validación de accesos 37
4.17.6. Identificación de los usuarios 37
4.17.7. Normas para la creación de contraseñas 37
4.17.8. Segregación de funciones 38
4.18. REQUERIMIENTOS DE NEGOCIO PARA EL ACCESO LÓGICO 39

4.18.1. Control de acceso a las aplicaciones y recursos tecnológicos 39
4.18.2. Restricción del acceso a la información 41
4.18.3. Restricciones de uso sobre los sistemas operativos. 41
4.18.4. Uso de las Utilidades del Sistema 42
4.18.5. Control de acceso a la red 42
4.18.6. Acceso a datos de producción 43
4.18.7. Conexiones remotas 44
4.19. CONTROLES CRIPTOGRÁFICOS 45
4.19.1. Firma digital 47
4.19.2. Firma Electrónica 48
4.19.3. Cifrado de la información 49
4.19.4. Llaves criptográficas 49
4.19.5. Certificados digitales 50
4.20. SEGURIDAD FÍSICA Y DEL ENTORNO 51
4.20.1. Áreas seguras 51
4.20.2. Ubicación y protección de los equipos 53
4.20.3. Servicios de suministro 53
4.20.4. Seguridad del cableado 53
4.20.5. Mantenimiento de Equipos 53
4.20.6. Seguridad de equipos y activos fuera de las instalaciones 53
4.20.7. Disposición segura o reutilización de Equipos 54
4.20.8. Política de equipo desatendido, escritorio limpio y pantalla limpia 54
4.21. SEGURIDAD DE LAS OPERACIONES 55
4.21.1. Documentación de procedimientos operativos 55
4.21.2. Control de Cambios 55
4.21.3. Gestión de Capacidad 55
4.21.4. Separación de los Ambientes 55
4.22. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS 55
4.23. COPIAS DE RESPALDO 56
4.24. REGISTRO Y SUPERVISIÓN DE EVENTOS 57
4.24.1. Registro de eventos 57
4.25. CONTROL DE SOFTWARE OPERACIONAL 58
4.25.1. Instalación de software en sistemas operativos 58

4.26. GESTIÓN DE LA VULNERABILIDAD TÉCNICA 59
4.26.1. Gestión de las vulnerabilidades técnicas 59
4.27. AUDITORÍAS DE SISTEMAS DE INFORMACIÓN 60
4.28. SEGURIDAD EN LAS COMUNICACIONES 60
4.28.1. Gestión de la seguridad en las redes 60
4.28.2. Transferencia de información 61
4.29. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 62
4.29.1. Requisitos de Seguridad de los Sistemas de Información. 62
4.29.2. Seguridad en los procesos de desarrollo y soporte 63
4.29.3. Ambiente de desarrollo seguro 63
4.29.4. Desarrollo contratado externamente 64
4.29.5. Pruebas de seguridad de sistemas 64
4.29.6. Pruebas de aceptación de sistemas 65
4.29.7. Datos de prueba 65
4.30. RELACIÓN CON LOS PROVEEDORES 65
4.30.1. Seguridad de la información en las relaciones con los proveedores. 65
4.30.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. 66
4.31. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 66
4.31.1. Notificación de incidentes de seguridad de la información 68
4.33. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO 69
4.33.1. Continuidad de la seguridad de la información 69
4.33.2. Redundancias 70
4.34. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES 70
4.34.1. Identificación legislación aplicable y requisitos contractuales 70
4.34.2. Derechos de propiedad intelectual 70
4.34.3. Protección de registros 71
4.34.4. Privacidad y protección de información de datos personales 71
4.34.5. Reglamentación de controles criptográficos 71
4.35. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 71
4.35.1. Revisión de la seguridad de la información 71
4.35.2. Revisión cumplimiento técnico 71
4.36. CUMPLIMIENTO 72
4.37. BIBLIOGRAFÍA 72

1. OBJETIVO

Establecer las políticas de seguridad de la información, mediante el uso y la apropiación de los lineamientos que permitan preservar la confidencialidad, integridad y disponibilidad de los activos de información de la Agencia Nacional de Minería.

2. ALCANCE

El manual de políticas de seguridad de la información establece los lineamientos de seguridad para todos los interesados en tener acceso a la información o servicios tecnológicos que estén vinculados de manera interna o externa de a la ANM de manera que toda la información creada, procesada, almacenada y utilizada para gestión y soporte en la Agencia Nacional de Minería sea accedida con el cumplimiento de los principios básicos de confidencialidad, integridad y disponibilidad por funcionarios, contratistas, proveedores, terceros y en general cualquier ciudadano pueda hacer uso de los servicios de información .

3. DEFINICIONES

3.1. Activo de Información: Es todo lo que tenga valor para la gestión de la seguridad de la organización.[1]

3.2. Acuerdos de Niveles de servicio: Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.[2]

3.3. Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema de información o la Entidad.[3]

3.4. Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.[4]

3.5. Análisis de vulnerabilidad: Es la medida o grado de debilidad de ser afectado por amenazas o riesgo según la frecuencia y severidad de estos. La vulnerabilidad depende de varios factores, entre otros: La posibilidad de ocurrencia del evento, la frecuencia de ocurrencia de este, los planes y programas preventivos existentes, la posibilidad de programación anual entre otros.[5]

3.6. ARL: Administradora de Riesgos Laborales.[6]

3.7. 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 identidades.[7]

3.8. CCTV: Circuito Cerrado de Televisión.[8]

3.9. Ciber-amenaza o amenaza cibernética: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.[9]

[1] [FUENTE Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[2] [FUENTE: Forderer, Jo Moore, Morris, Du Toit, Blanco y Castañeda, 2020, Copyright © Axelos Ltd. All rights reserved]]
[3] [FUENTE: Organización Internacional de Normalización. (2018), Técnicas de Seguridad y gestión de la Seguridad de la Información (Norma ISO/IEC No. 27005:2018]
[4] [FUENTE Organización Internacional de Normalización. (2013); Gestión de Riesgos, Norma ISO 31000:2011]
[5] [FUENTE: Organización Internacional de Normalización. (2018), Técnica de Seguridad y Divulgación de vulnerabilidades, Norma ISO 29147:2018]
[6] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[7] [FUENTE: Organización Internacional de Normalización. (2018), Sistemas de gestión de seguridad de la información, Norma ISO/IEC 27000:2018]
[8] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[9] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]

3.10. Ciber-ataque o ataque cibernético: Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.[10]

3.11. Ciber-espacio: Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.[11]

3.12. Ciber-riesgo o riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.[12]

3.13. Ciber-seguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.[13]

3.14. Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.[14]

3.15. CNSC: Comisión Nacional del Servicio Civil.[15]

3.16. Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. El concepto de confidencialidad se refiere a la capacidad de garantizar que la información no se encuentra disponible o es revelada a individuos que no tienen autorización para consultarla. Garantizar la confidencialidad de la información es una de las funciones más relevantes de un profesional de la seguridad.[16]

3.17. Contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso. Forma parte del Plan de Continuidad del Negocio.[17]

3.18. Control de acceso: El proceso que limita y controla el acceso a los recursos de un sistema computarizado; un control físico o lógico diseñado para proteger contra usos o entradas no autorizadas. El control de acceso puede ser definido por el sistema (mandatory access control – MAC), o definido por el usuario propietario del objeto (discretionary access control – DAC).[18]

3.19. Criptografía: El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad.[19]

3.20. CSIRT (Computer Security Incident Response Team): Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.[20]

3.21. CyberArk: Es proveedor y aplicación de seguridad de cuentas privilegiadas, un componente fundamental de la seguridad de Tecnología de la Información (TI) para proteger los datos, la infraestructura y los bienes de toda la empresa, ya sea a nivel local, en la nube, en los endpoints y en todo el proceso de DevOps.[21]

3.22. DBA (Database administrator): Esta palabra define el administrador de base de datos.[22]

[10] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[11] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[12] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[13] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[14] [FUENTE: NORMAS DE SEGURIDAD DE DATOS- DSS, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago]
[15] [FUENTE: Entidad del Gobierno]
[16] [FUENTE Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[17] [FUENTE: Organización Internacional de Normalización. (2006), Tecnología de la Información. Técnicas de Seguridad. Gestión de la Seguridad de la Tecnología de la Información y las Comunicaciones. Parte 1: Conceptos y Modelos para la Gestión de la Tecnología de la Información y Las Comunicaciones, Norma NTC 5411-1:2006]
[18] [FUENTE Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[19] [FUENTE: NORMAS DE SEGURIDAD DE DATOS- DSS, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago]
[20] [FUENTE: Organización Internacional de Normalización. (2018), Técnicas de Seguridad y gestión de la Seguridad de la Información, Norma ISO/IEC No. 27005:2018]
[21] [FUENTE: Organización Internacional de Normalización. (2014), Tecnología de la información – Estándar de red de malla de eficiencia energética habilitada para balizas inalámbricas (WiBEEM) para servicios de redes domésticas inalámbricas; Norma ISO/IEC 29145-2:2014]
[22] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]

3.23. Disponibilidad: Entendida como la garantía del acceso a la información en el instante en que el usuario la necesita. El concepto de disponibilidad se refiere a la capacidad de garantizar que la información se encuentra disponible siempre que se requiere acceder a ella.[23]

3.24. DRP: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.[24]

3.25. Encriptación (Cifrado, codificación): La encriptación es el proceso para volver ilegible información considerada importante. La información una vez encriptada sólo puede leerse aplicándole una clave. Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, etc.[25]

3.26. Estimación de riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.[26]

3.27. Evaluación de Riesgos: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la Agencia Nacional de Minería.[27]

3.28. Evidencia Digital: También conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos.[28]

3.29. Firewall (Muro de Fuego - Cortafuego): Herramienta de seguridad que controla el tráfico de entrada/salida de una red.[29]

3.30. Firma Digital: Una firma digital, que no debe confundirse con un certificado digital, es una técnica matemática utilizada para validar la autenticidad e integridad de un mensaje, software o documento digital. La firma digital, a diferencia de una firma tradicional, no es un nombre, sino que consta de dos «claves» o secuencias de caracteres separadas. Consiste en aplicar mecanismos criptográficos al contenido de un mensaje o documento con el objetivo de demostrar al receptor del mensaje que:
El emisor del mensaje es real (autenticación); Éste no puede negar que envió el mensaje (no repudio);
El mensaje no ha sido alterado desde su emisión (integridad).[30]

3.31. Firma Electrónica: Es una herramienta digital que utiliza mecanismos de autenticación para sustituir a la firma autógrafa, es decir, aquella manuscrita en papel. De hecho, es la forma más simple de autenticar un documento, ya que se vale de medios informáticos para completar una solicitud de consentimiento. [31]

3.32. Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.[32]

3.33. Hacking - Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.[33]

[23] [FUENTE Organización Internacional de Normalización. (2013), Sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[24] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[25] [FUENTE: NORMAS DE SEGURIDAD DE DATOS- DSS, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago]
[26] [FUENTE Organización Internacional de Normalización. (2013); Gestión de Riesgos, Norma ISO 31000:2011]
[27] [FUENTE: Organización Internacional de Normalización. (2018), Técnicas de Seguridad y gestión de la Seguridad de la Información, Norma ISO/IEC No. 27005:2018]
[28] [FUENTE: Organización Internacional de Normalización. (2018), Técnicas de Seguridad y gestión de la Seguridad de la Información, Norma ISO/IEC No. 27005:2018]
[29] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[30] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[31] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[32] [FUENTE: Organización Internacional de Normalización. (2018), Sistemas de gestión de seguridad de la información, Norma ISO/IEC 27000:2018]
[33] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]

3.34. Hacking Ético: Es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de "pentester". A la actividad que realizan se le conoce como "hacking ético" o "pruebas de penetración".[34]

3.35. Hardware: Es un término genérico para todos los componentes de Tecnología físicos (Redes, servidores, computadores, Portátiles, etc.).[35]

3.36. HASH: Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.[36]

3.37. HIDS (Sistema de detección de intrusos en un Host): Es un sistema que busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina. Puede tomar medidas protectoras.[37]

3.38. IMAC: (Instalación, Movimiento, Actualización y cambio), formulario utilizado por la OTI para la atención y Gestión de solicitudes nuevas para la Creación de usuarios, acceso a los sistemas de información y bases de datos, instalación de Software y Hardware, desactivación de usuarios entre otras.[38]

3.39. Impacto: El impacto es la medida del alcance del daño potencial que el incidente puede causar. Los incidentes graves, por ejemplo, tienen un tiempo de resolución menor, puesto que su impacto en el servicio es mayor.[39]

3.40. Incidente de Seguridad: Es un evento adverso en el sistema o la red que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.[40]

3.41. Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014.[41]

3.42. Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.[42]

3.43. Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (Ley 1712 de 2014).[43]

3.44. Información: Es un conjunto de datos organizados y procesados que tienen un significado, relevancia, propósito y contexto. La información sirve como evidencia de las actuaciones de las entidades. Un documento se considera información y debe ser gestionado como tal.[44]

3.45. Infraestructura de TI: Todo el hardware, software, redes, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorizar, controlar o soportar aplicaciones y servicios de TI.[45]

3.46. Integridad: Entendida como la preservación de la información de forma completa y exacta. El concepto de integridad se refiere a la capacidad de garantizar la exactitud y completitud de la información a

[34] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[35] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[36] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[37] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[38] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[39] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[40] [FUENTE: Organización Internacional de Normalización. (2012), Seguridad social — Sistemas de gestión de la continuidad de las actividades — Requisitos, Norma ISO 22301:2012]
[41] [FUENTE: Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[42] [FUENTE: Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[43] [FUENTE: Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[44] [FUENTE: GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, MINTIC, 2016]
[45] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]

lo largo de todo su ciclo de vida. Preservar la integridad de la información, es una de las funciones más importantes de un profesional de la seguridad de la información.[46]

3.47. Internet: Es un sistema mundial de redes de computadores, integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computador puede, en caso de contar con los permisos apropiados, obtener información, efectuar transacciones, comunicarse y participar en toda gama de procesos públicos y privados puesto en dicha red.[47]

3.48. Intranet: Red de una Entidad que utiliza tecnologías y protocolos de Internet, pero que sólo está disponible para determinadas personas, por ejemplo, para los funcionarios o terceros autorizados de una Entidad. Una Intranet también recibe el nombre de red privada.[48]

3.49. IP: Es un número que identifica de manera lógica y jerárquica a un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP (parte de la capa de Internet).[49]

3.50. Keylogger (registrador de teclas): Es una herramienta que se encarga de registrar las pulsaciones que se hacen sobre el teclado, para guardarlas en un archivo o enviarlas a través de Internet.[50]

3.51. Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el sistema de información.[51]

3.52. Mitigación: Acciones desarrolladas antes, durante y después de un siniestro, tendientes a contrarrestar sus efectos críticos y asegurar la supervivencia del sistema, hasta tanto se efectúe la recuperación. [52]

3.53. MSPI: Modelo de seguridad y privacidad de la información. Es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades [53]

3.54. Navegador: Es un programa que, a través de la Web, permite visualizar hipertextos de datos o imágenes que estén en algún computador o en dispositivos conectados a la misma. La función primordial es la de poder acceder a páginas que se encuentran como hipervínculo en algún archivo. A esta acción de traslado de ubicación entre portales o sitios Web se le denomina Navegación. Los navegadores más utilizados son Internet Explorer y Mozilla Firefox.[54]

3.55. No repudio: Se refiere a la capacidad de garantizar que, cuando se realiza un intercambio de información, el receptor de la información no puede negar haberla recibido, y el emisor de la información no puede negar haberla enviado.[55]

3.56. Ofuscación: En computación, la ofuscación se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en el código fuente de un programa informático o código máquina cuando el programa está en forma compilada o binaria, con el fin de que no sea fácil de entender o leer.[56]

3.57. OTI: Oficina de Tecnología e Información.[57]

3.58. Password: Significa contraseña, clave, key o llave.[58]

[46] [FUENTE: Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[47] [FUENTE: Organización Internacional de Normalización. (2020), Descripción de los conceptos, terminologías, características, casos de uso y tecnologías comunes, (...) de la computación periférica para aplicaciones de sistemas de IoT. Norma ISO/IEC TR 30164:2020]
[48] [FUENTE: Organización Internacional de Normalización. (2015), Guía detallada de seguridad de la administración, operación y uso de las redes, Norma, ISO/IEC 27033-1:2015]
[49] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[50] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032:2012]
[51] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[52] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[53] [FUENTE Organización Internacional de Normalización. (2013); Gestión de Riesgos, Norma ISO 31000:2011]
[54] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[55] [FUENTE: Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[56] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[57] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[58] [FUENTE: Organización Internacional de Normalización. (2018), Aspectos relacionados con la seguridad informática (ciberseguridad) Norma ISO/TR no. 22100-4:2018]

3.59. PCN: Un plan de continuidad de negocios o BCP, por sus siglas en inglés (Business Continuity Planning), es un documento que describe los procesos y sistemas de la empresa, sus posibles fallas y cómo atenderlas. Plan de Continuidad de Negocio.[59]

3.60. PILA: Planilla Integrada de Liquidación de Aportes. es un formato inteligente que le permite a todas las personas y empresas, liquidar y pagar sus aportes de seguridad al Sistema de la Protección Social.[60]

3.61. Plan de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.[61]

3.62. PN: En informática, acrónimo del Ingles Virtual Prívate Networks, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, por ejemplo, Internet manteniendo y garantizando la protección de la información.[62]

3.63. Política de seguridad: Una política de seguridad es una regla de definición general, independiente de los ambientes tecnológicos, que representa los objetivos sobre los que se sustenta el Modelo de Seguridad de los Activos de Información. Debe cumplir con una directriz de la Entidad en general, debe revisarse y estar sujeta a modificaciones ante cambios estructurales.[63]

3.64. Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Entidad en el marco de las funciones que a ella le compete realizar.[64]

3.65. Propietario de Información: Es la persona o entidad responsable de la gestión y protección de un activo de información dentro de una organización.[65]

3.66. Redundancia: Cuando la opción de las copias de respaldo no satisfaga el RPO (Recovery Point Objective, se refiere al volumen de datos en riesgo de pérdida que una Entidad considera tolerable) y RTO (Recovery Time Objective, expresa el tiempo durante el cual una Entidad puede tolerar la falta de funcionamiento de sus aplicaciones y / o nivel de servicio, sin afectar a la continuidad del negocio) se debe contar con un esquema de redundancia para los componentes de hardware y/o software involucrados.[66]

3.67. Requerimiento: Los requerimientos son solicitudes que surgen de las necesidades y expectativas de los usuarios. Naturaleza: Los requerimientos son proactivos, impulsados por las demandas y necesidades de los usuarios.[67]

3.68. Responsable de Seguridad de la Información: Es la persona con la función de supervisar el cumplimiento de la presente Política.[68]

3.69. Riesgo de Seguridad de la Información: Es el potencial de que una amenaza pueda explotar una vulnerabilidad de un activo de información afectando la operación o imagen de la Entidad.[69]

3.70. Riesgo: Es el potencial de exposición a pérdidas. Los riesgos, ya sean naturales o provocados por el hombre, son constantes a lo largo de nuestra vida diaria. El potencial es medido normalmente por su probabilidad de ocurrencia en un periodo determinado.[70]

[59] [FUENTE: Organización Internacional de Normalización. (2012), Seguridad social — Sistemas de gestión de la continuidad de las actividades — Requisitos, Norma ISO 22301:2012]
[60] [FUENTE: Organización Internacional de Normalización. (2012), Seguridad social — Sistemas de gestión de la continuidad de las actividades — Requisitos, Norma ISO 22301:2012]
[61] [FUENTE: Organización Internacional de Normalización. (2012), Seguridad social — Sistemas de gestión de la continuidad de las actividades — Requisitos, Norma ISO 22301:2012]
[62] [FUENTE: NORMAS DE SEGURIDAD DE DATOS- DSS, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago]
[63] [FUENTE: GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, MINTIC, 2016]
[64] [FUENTE: GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, MINTIC, 2016]
[65] [FUENTE: Organización Internacional de Normalización. (2013) sistema de gestión de Seguridad de la Información Requisitos (Norma ISO nº 27001:2013]
[66] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[67] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[68] [FUENTE: GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, MINTIC, 2016]
[69] [FUENTE: Organización Internacional de Normalización. (2018), Técnicas de Seguridad y gestión de la Seguridad de la Información, Norma ISO/IEC No. 27005:2018]
[70] [FUENTE Organización Internacional de Normalización. (2013); Gestión de Riesgos, Norma ISO 31000:2011]

3.71. Rol: Es un conjunto de permisos que puede asignarse a un usuario que se registra en un administrador de sistemas. Normalmente, los roles se definen de modo que incluyan permisos para acceder a la información.[71]

3.72. RPO: determina cuánto será necesario retroceder en el historial de datos para que el almacenamiento de copias de seguridad pueda reanudar las operaciones normales después de que un equipo, sistema o red sufra una disrupción debido a un error de hardware, programas o comunicaciones. Recovery Point Objective - Punto de recuperación objetivo.[72]

3.73. Seguridad de la Información: Son todas aquellas medidas preventivas de los sistemas de información que permitan resguardar y proteger la información. [73]

3.74. Sistema de Información: El sistema de información es el sistema que se encarga de recopilar los datos necesarios para que el director del proyecto sepa si el proyecto lleva la dirección prevista.[74]

3.75. SG SST: Sistema de Gestión de Seguridad y Salud en el Trabajo.[75]

3.76. SGSI: Sistema de Gestión de Seguridad de la Información El término SGSI es utilizado principalmente por la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission y es un conjunto de políticas de administración de la información.[76]

3.77. Software de Borrado Seguro: Software que borra de forma segura, definitiva e irreversible todos los datos almacenados en los discos duros de un equipo informático, incluido el disco de sistema, permitiendo su reciclaje o reutilización con total garantía de seguridad.[77]

3.78. Tecnología de la Información y Comunicación: Se refiere al Hardware y Software que interviene en el procesamiento de la información.[78]

3.79. Teletrabajo: Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo (Artículo 2, Ley 1221 de 2008).[79]

3.80. TIER III: Los centros de datos de Tier III se caracterizan por una alta disponibilidad y redundancia. Tienen sistemas duplicados y rutas de distribución de energía y refrigeración independientes[80]

3.81. Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).[81]

3.82. Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad, funcionarios, contratistas, terceros, entre otros.[82]

3.83. Troyano: Es un programa malicioso capaz de alojarse en un computador y permitir el acceso a usuarios externos, a través de una red local o de Internet, con el fin de apoderarse de la información.[83]

3.84. UPS: Uninterruptible Power Supply - Sistema de alimentación eléctrica ininterrumpida.[84]

[71] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[72] [FUENTE: Organización Internacional de Normalización. (2012), Seguridad social — Sistemas de gestión de la continuidad de las actividades — Requisitos, Norma ISO 22301:2012]
[73] [FUENTE: Organización Internacional de Normalización. (2018), Sistemas de gestión de seguridad de la información, Norma ISO/IEC 27000:2018]
[74] [FUENTE: Organización Internacional de Normalización. (2015), Norma Técnico Colombiana, sistema Integrado de Gestión, NTC-ISO 9001:2015]
[75] [FUENTE: Organización Internacional de Normalización. (2018), Requisitos para un sistema de gestión de la seguridad y salud en el trabajo (SST), Norma ISO no. 45001:2018]
[76] [FUENTE: Organización Internacional de Normalización. (2018), Sistemas de gestión de seguridad de la información, Norma ISO/IEC 27000:2018]
[77] [FUENTE: Organización Internacional de Normalización. (2015), Norma Técnico Colombiana, sistema Integrado de Gestión, NTC-ISO 9001:2015]
[78] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[79] [FUENTE: Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones, Artículo 2, 16 de julio de 2008]
[80] [FUENTE: Forderer, et al 2020, Copyright © Axelos Ltd. All rights reserved]
[81] [FUENTE: Ley 1581 de 2012, complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación, Articulo 3]
[82] [FUENTE: GUÍA PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN, MINTIC, 2016]
[83] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[84] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]

3.85. Validación: Se realiza al comparar si el resultado de las pruebas de usuario es correcto.[85]
3.86. Verificación: Comprobación de la correcta funcionalidad de un producto o servicio o de la salida congruente e integra de la información.[86]
3.87. VLAN: (virtual local area network), acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.[87]
3.88. Vulnerabilidad: Debilidad de un activo o control que pone en riesgo la seguridad de la información y/o sus activos asociados, y que puede ser explotada por una o más amenazas.[88]
3.89. Vulnerabilidad Día Cero: Es un tipo de vulnerabilidad que acaba de ser descubierta y que aún no tiene un parche que la solucione.[89]
3.90. Wireless: Referido a las telecomunicaciones, se aplica el término inalámbrico (inglés Wireless - sin cables) al tipo de comunicación en la que no se utiliza un medio de propagación físico, sino que utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión.[90]
3.91. WPA2-PSK: WPA2 (Wi-Fi Protected Access 2), en español «Acceso Wi-Fi protegido 2», es un sistema para proteger las redes inalámbricas (Wi-Fi) WPA-PSK también se conoce como WPA-Personal. WPA2-PSK (AES) es un formato de cifrado que utiliza AES (estándar avanzado de cifrado), el formato más reciente de WPA-PSK (TKIP), y tiene un cifrado más potente. WPA2-PSK también se conoce como WPA2-Persona.[91]

4. DESARROLLO

4.1. GENERALIDADES

La posibilidad de interconectarse a través de redes, la utilización de aplicaciones, y el manejo de la información por parte de los funcionarios, contratistas, proveedores, terceros, ha abierto nuevos horizontes a las instituciones para mejorar su productividad y ofrecer sus servicios, más allá de las fronteras institucionales e incluso nacionales, lo cual, lógicamente ha traído la aparición de nuevas amenazas para los sistemas de información, como son:

- Ataques cibernéticos internos y externos.
- Pérdida de información ante la migración de datos.
- Navegación imprudente por parte de los funcionarios y contratistas.
- Correos electrónicos maliciosos.
- Explotación automática de vulnerabilidades conocidas.
- Manipulación inadecuada de la información por parte de funcionarios y contratistas.
- Fuga de información por parte de funcionarios y contratistas.
- Procesos inseguros de comunicaciones en accesos remotos
- Fraudes a través de medios informáticos

[85] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[86] [FUENTE: Definición ANM, Bogotá D.C., Oficina de Tecnología e Información, 2024]
[87] [FUENTE: Organización Internacional de Normalización. (2018), Técnica de Seguridad y Divulgación de vulnerabilidades, Norma ISO 29147:2018]
[88] [FUENTE: Organización Internacional de Normalización. (2012), Tecnologías de la información - Técnicas de seguridad - Directrices para la ciberseguridad, Norma ISO: IEC: 27032,2012]
[89] [FUENTE: Organización Internacional de Normalización. (2018), Técnica de Seguridad y Divulgación de vulnerabilidades, Norma ISO 29147:2018]
[90] [FUENTE: Organización Internacional de Normalización. (2014), Tecnología de la información – Estándar de red de malla de eficiencia energética habilitada para balizas inalámbricas (WiBEEM) para servicios de redes domésticas inalámbricas; Norma ISO/IEC 29145-2:2014]
[91] [FUENTE: Organización Internacional de Normalización. (2014), Tecnología de la información – Estándar de red de malla de eficiencia energética habilitada para balizas inalámbricas (WiBEEM) para servicios de redes domésticas inalámbricas; Norma ISO/IEC 29145-2:2014]

- Entre otros.

Es así que estas políticas, están orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, a través de los lineamientos y controles que se adoptan en cumplimiento a los requisitos exigidos por la norma técnica Internacional ISO/IEC 27001:2013 y que, con su adopción desde la Alta Dirección de la Agencia Nacional de Minería, se establece el cumplimiento a éstas para la seguridad y privacidad de sus activos de información, con el propósito de minimizar posibles impactos no deseados que puedan comprometer los principios esenciales del Sistema de Gestión de Seguridad de la Información.

4.2. POLÍITICA GENERAL

La Agencia Nacional de Minería, Entidad aliada del desarrollo sostenible del país a través de la generación de valor, con una gestión moderna, transparente y eficiente de los recursos minerales de los colombianos, está comprometida con el cuidado y gestión adecuado de la información propia, de los titulares mineros y ciudadanos mediante la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) orientado a mantener y preservar los principios fundamentales de Confidencialidad, Integridad y Disponibilidad de la información, al igual que identificar y mitigar sus riesgos asociados.

La Presidencia de la ANM mediante la aprobación de esta Política declara su posición y compromiso con el cumplimiento de los requisitos definidos en el marco del SGSI, aspectos en los cuales se involucra directamente la función de seguridad de la información, que tiene como propósito principal mantener un ambiente razonablemente seguro, alineado a la misión, objetivos estratégicos de la ANM y requerimientos regulatorios aplicables, definiendo e implementando buenas prácticas que permitan minimizar posibles impactos no deseados que puedan comprometer los principios esenciales de Seguridad de la Información.

4.3. REVISIÓN DEL MANUAL

El manual de políticas de seguridad de la información debe ser actualizado cuando surjan cambios relevantes de mejora y de cumplimiento al Sistema de Gestión de Seguridad de la Información en la ANM. No obstante, se recomienda una revisión anual con base en la alineación de los objetivos estratégicos de la entidad.

La documentación a la que hace llamado cada una de las políticas relacionadas en este manual, hacen parte de la caracterización del Proceso Administración de Tecnologías de la Información y de su operación, tales como; (procedimientos, instructivos, formatos, etc.) la cual, se ha venido fortaleciendo a través de actualizaciones o creando algunos de éstos, fundamentales para el cumplimiento de los lineamientos establecidos en este manual.

4.4. ROLES Y RESPONSABILIDADES

4.4.1. **Todo el personal que tenga acceso a la información de la ANM**: entre ellos están: servidores públicos, contratistas, proveedores, convenios entre instituciones, visitantes y en general cualquier

tercero en relación con la ANM. Toda persona natural o jurídica que tenga acceso a la información, servicios, sistemas o aplicaciones de la Agencia Nacional de Minería, debe tener claramente definidos sus deberes frente a la gestión de la Seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información, por lo tanto, debe velar por la seguridad de la información dando cumplimiento de manera obligatoria a las políticas descritas en este manual.

4.4.2. **Rol con base al acceso de la información:** Personal natural o jurídica que tenga acceso a la información, servicios, sistemas o aplicaciones debe reconocer el rol al cual pertenece dentro de la entidad y aplicar las políticas y lineamientos generales y específicos según su rol de Acceso. En caso de que no pueda encontrase en una categoría de rol específica, le serán atribuidas las obligaciones de todos los roles cuyo nivel de seguridad sea el más alto. Los roles pueden ser categorizados en:

a. **Funcionario colaborador general.** Persona natural cuya labor requiere de acceso a una información pública o pública reservada, es consumidor de aplicaciones y servicios de la entidad tales como el correo electrónico, servicios internos, servicios externos.

b. **Funcionario Colaborador de alta Confidencialidad.** Persona natural o jurídica cuya labor requiere además del acceso del colaborador General, acceso a información de carácter sensible tales como datos personales e información pública clasificada y reservada.
c. **Proveedor de Servicios con acceso a Información general.** Persona natural o jurídica cuyas actividades o acciones dentro de la entidad se realiza por contratos de prestación de servicios, obra labor y que tienen una temporalidad definida, pero que por su labor a realizar requiere de acceso a una información pública clasificada o reservada, es consumidor de aplicaciones y servicios de la entidad tales como el correo electrónico, servicios internos, servicios externos. En el ejercicio de la ejecución del contrato este rol aplicaría a contratistas y subcontratistas o empelados de personas jurídicas.

d. **Proveedor de Servicios con acceso a Información confidencial.** Persona natural o jurídica cuya labor dentro de la entidad se realiza por contratos de prestación de servicios, obra labor y que tienen una temporalidad definida, pero que por su labor a realizar requiere conocer o tener acceso a información pública reservada, sensible y/o de alta confidencialidad. En el ejercicio de la ejecución del contrato este rol aplicaría a contratistas y subcontratistas o empleados de personas jurídicas.
e. **Tercero externo con acceso a la información.** persona natural o jurídica que accede a la información o hacer uso de aplicaciones como consumidor de los datos, tales como en acuerdos de interoperabilidad o intercambio de información.
f. **Colaborador con rol que hace parte la Oficina de Tecnología e Información OTI.** persona natural o jurídica que por su rol realice, administre, aplicaciones, servicios, sistemas operativos cuya responsabilidad este a cargo de la OTI.

4.4.3. Rol con base en sus responsabilidades.

a. **La alta Dirección**, es el ente máximo en la ANM y se encuentra representado por los miembros del Comité Institucional de Gestión y Desempeño de la ANM, es responsable de revisar y aprobar la política de Seguridad de la Información y Ciberseguridad; revisar la eficacia de la implementación de la política de Seguridad; proporcionar y avalar los recursos necesarios para el desarrollo e implementación de iniciativas de Seguridad; comunicar la importancia de una gestión eficaz de la Seguridad de la Información y Ciberseguridad; promover el cumplimiento de las políticas y normas definidas en el SGSI.

b. **El Comité Institucional de gestión y desempeño**, es un grupo interdisciplinario conformado al interior de la ANM, es responsable de revisar y aprobar las políticas de Seguridad de la Información y Ciberseguridad, revisar los lineamientos definidos por Seguridad de la Información; revisar la implementación del SGSI en Entidad; realizar el seguimiento a la gestión de Seguridad de la Información y Ciberseguridad; apoyar la implementación de los lineamientos en la Entidad en temas de Seguridad de la Información y Ciberseguridad; promover la sensibilización y comunicación al interior de la Entidad del Sistema de Gestión de Seguridad de Información.

c. **La Oficina de Tecnologías de Información**, la OTI es la líder de la implementación y gestión de los controles de ciberseguridad que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad que se encuentre bajo administración de la Jefatura de la OTI, es responsable definir políticas, procedimientos de gestión de accesos lógicos y esquema, metodología de construcción de roles y perfiles para los accesos a plataformas e infraestructura de la Entidad; definir procedimientos de gestión de logs; definir líneas base, guías de aseguramiento, etc. para aseguramiento de los sistemas; definir la metodología y procedimientos del ciclo de vida de desarrollo de software incluyendo requerimientos de seguridad en cada etapa; definir la estrategia de respaldo de información; definir políticas y procedimientos de gestión de cambios; definir el diseño de red y plataformas tecnológicas teniendo en cuenta las necesidades de la Entidad Implementación de planes de remediación de vulnerabilidades; adquirir e implementar herramientas de gestión de logs y correlación; adquirir e implementar tecnologías de seguridad; adquirir, implementar y configurar la red y las plataformas tecnológicas de acuerdo con el diseño propuesto; realizar los ajustes/mejoras necesarias en el proceso de desarrollo de software; ajustes o mejoras a la estrategia de respaldo de información.

d. **El oficial de seguridad de la información**, debe asumir la responsabilidad en el desarrollo e implementación del SGSI, debe velar por el cumplimiento de las políticas, debe orientar a todo el personal que tenga acceso a la información de la Entidad, debe coordinar actividades de gestión de riesgos de seguridad y ciberseguridad, debe apoyar la identificación de controles y debe colocar en contexto al Comité Institucional de Gestión y Desempeño, de toda la Gestión del Sistema de Seguridad de la Información.

e. **El Propietario (Responsable) del activo de información,** es el líder de proceso que tiene la responsabilidad de establecer la valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta el modelo de clasificación de la información en la ANM, igualmente definir el nivel

de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad; realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida; mantener actualizada la matriz de activos de información definida en el procedimiento de Gestión de Activos; identificar riesgos asociados con la Seguridad de la Información en los procesos de los cuales son responsables o tienen participación; reportar oportunamente eventos o incidentes de Seguridad de la Información siguiendo las directrices de Etiquetado de la Información que están dentro del procedimiento de Gestión de Activos de Información código APO4-P-009.

4.4.4. Segregación de deberes y funciones.

En todos los sistemas de información de la Entidad se deben implementar controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

4.4.5. Contacto con las autoridades

Todo el personal que tenga acceso a la información de la Agencia Nacional de Minería debe tener claramente definidos sus deberes frente a la gestión de la Seguridad de la información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.

La Agencia Nacional de Minería, a través de los jefes de oficina y vicepresidentes debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control (Procuraduría General de la Nación, Contraloría General de la República, fiscalía general de la Nación), Fuerzas Militares (Policía Nacional, Comando Conjunto Cibernético).

La Oficina de Control Interno de la ANM debe definir, actualizar y publicar el listado de autoridades a contactar en caso de que se sospeche de la violación de la Ley (Normograma), para mantener contacto con organismos de control y autoridades; los funcionarios y contratistas pueden consultar el marco legal aplicable en el Normograma de la ANM.

4.4.6. Contactos con grupos de interés

La Agencia Nacional de Minería, a través de la Oficina de Tecnología e Información debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información. Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información, recibiendo comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero, avisos de ciberataques o ataques cibernéticos, reporte de vulnerabilidades y amenazas nuevas.

4.5. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La seguridad de la información se debe integrar al procedimiento de gestión de proyectos tecnológicos APO4-P-003 de la Agencia Nacional de Minería, para asegurar que los riesgos de seguridad de la información se

identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de proceso, de los funcionarios y contratistas de la OTI, asegurar que se sigan las siguientes directrices:

a. Realizar valoración de los riesgos de seguridad de la información conforme el instructivo GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EST1-P-003-I-002 en la fase de estudios previos del proyecto, para identificar los controles necesarios.

b. Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

4.6. SEGURIDAD CON DISPOSITIVOS MÓVILES

a. Los dispositivos móviles corporativos (teléfonos inteligentes, tablets, portátiles), son herramientas de trabajo que se deben utilizar **únicamente** para el desarrollo de actividades relacionadas con los procesos de la Entidad.

b. La ANM no permite la conectividad de equipos móviles personales a la red interna de la entidad, dado el riesgo que actualmente generan este tipo de dispositivos,

c. la ANM podrá suministrar servicio de conectividad hacia internet de dispositivos personales manteniendo una navegación restringida hacia internet con base a los niveles de navegación establecidos por la entidad. La OTI debe establecer las herramientas tecnológicas necesarias para que los dispositivos de esta categoría se les mantendrán los accesos restringidos y controlados a la red interna.

d. **Seguridad corporativa en equipos móviles:** El tercero que desee utilizar herramientas como el correo electrónico corporativo, One Drive, Teams o cualquier aplicación de uso corporativo debe permitir la instalación de aplicaciones de seguridad establecidas por la ANM para el control de dicha información.

4.7. POLÍTICA DE USO DE DISPOSITIVOS CORPORATIVOS

La ANM proporciona equipos de cómputo fijo y portátiles para el desarrollo de las actividades de colaboradores según su rol dentro de la entidad, por tal motivo para estos equipos proporciona las herramientas tecnológicas y mantiene restricciones encaminadas a minimizar los riesgos asociados a su uso y que son inherentes de la tecnología. Por tal motivo se establecen como mínimo los siguientes controles de seguridad:

a. **Software y protección:** Las estaciones de trabajo y equipos portátiles que son propiedad de la ANM cuentan con software licenciado y protección contra código malicioso. Solo el personal de soporte de la OTI está autorizado a instalar software específico en los dispositivos móviles propiedad de la ANM.

b. **Auditoría:** La ANM se reserva el derecho de revisar cuando se requiera el software instalado y utilizado en equipos de cómputo y servidores.

c. **Registro de equipos:** El grupo de Servicios Administrativos se encuentra encargado del sistema de inventarios de la entidad, por lo tanto, debe mantener un registro de los dispositivos asignados y actualizado de estos activos informáticos.

d. **Mantenimiento de dispositivos:** El mantenimiento de dispositivos que son propiedad de la ANM, se hace en desde el área de servicios tecnológicos de la oficina de tecnología e información de la ANM.

e. **Almacenamiento de la información:** La información de la ANM que sea clasificada como pública reservada o clasificada, solo debe almacenarse en redes o en almacenamiento establecido por la entidad. La información que no esté clasificada en las dos opciones anteriores de tipo corporativo y de uso personal y que sea necesaria para el desarrollo de las tareas del usuario se pueden almacenar en el dispositivo de cómputo en cuyo caso se mantendrá bajo su custodia y responsabilidad. No obstante, la recomendación es hacer uso de las herramientas en línea establecidas por la ANM.

La información sensible, confidencial o reservada no se debe reposar o ser almacenada en los equipos de uso personal.

f. **Cifrado:** Los equipos de cómputo de tipo portátil que para efectos de su uso requieran salir de las instalaciones de la entidad deben contar con mecanismo de cifrado en su disco duro.

g. **Conexión a redes:** Todas las conexiones de redes ajenas a la Entidad deben seguir los lineamientos establecidos por la oficina de tecnologías de información.

h. **Notificación en caso de infección:** Si un funcionario o contratista sospecha de la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible a Servicios Tecnológicos de la ANM.

i. **Transporte y custodia**: El computador de la ANM, no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo.

En ningún caso se debe descuidar el portátil, celular o Tablet si se viaja en transporte público. También debe estar protegidos físicamente contra robo, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, centros de conferencias y lugares de reuniones. En caso de robo o pérdida del equipo se debe notificar de manera inmediata al personal de servicios administrativos grupo de inventarios.

Los dispositivos de la ANM no se deben dejar sin supervisión, y donde sea posible, debe estar protegidos bajo llave o se debe usar guayas para asegurarlos, adicionalmente, los computadores portátiles que salgan de la ANM y, de surgir un robo a éste, se debe comunicar inmediatamente con la Mesa de Servicios Tecnológicos o al Oficial de Seguridad de la Información, para seguir los pasos de reporte del incidente y comunicarlo a los entes tales como Policía Nacional, el CAI, la Fiscalía, etc.

j. **Uso del puesto de trabajo:** El usuario debe aplicar las buenas prácticas de uso del puesto de trabajo que sean relativas al uso de un equipo móvil (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, entre otras).

k. **Responsabilidades:** El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones de la ANM. Por tanto, es el funcionario el que debe garantizar la seguridad tanto del equipo como de la información que contiene.

l. **Viajes de trabajo:** Los funcionarios que viajan por asuntos de la Entidad son responsables de la seguridad de la información propiedad de la Entidad.

m. Bloqueo de Puertos Externos: Todo equipo de propiedad de la ANM que se encuentre activo o en funcionamiento debe tener bloqueo de medios de almacenamiento externo tales como USB, RWDVR, bluetooth y cualquiera que corresponda a un mecanismo de salida de información. La OTI debe contar con las herramientas para la implementación de estos controles.

n. Equipos para uso General: Los equipos para uso general deben ser utilizados con un usuario asociado al Directorio activo de la entidad, adicionalmente debe tener restringido acceso a los segmentos internos con permisos exclusivos para navegación. La OTI debe contar con las herramientas para la implementación de estos controles.

4.8. POLÍTICA DE USO DE DISPOSITIVOS NO CORPORATIVOS

Todo colaborador que haga uso de un equipo no corporativo debe aplicar los siguientes lineamientos:

a. **Software con leyes de derecho de autor:** Todo tercero (contratista o proveedor) que realice actividades para la ANM y cuya herramienta corresponda a un equipo de cómputo debe garantizar dar cumplimiento con los derechos de autor y hacer uso solo software legal instalado en su equipo para las actividades relacionadas con el desarrollo de su contrato con la ANM.

b. **Acceso a red interna ANM WIFI / VPN:**

El colaborador que requiera conectarse a la red LAN de la entidad por cualquier medio tales como VPN, WIFI, o cualquier otro haciendo uso de un equipo personal, debe contar como mínimo con las siguientes herramientas de seguridad informática:

- Contar con software antivirus que cumpla como mínimo con las siguientes características:

    - Antimalware de próxima generación: El cual se encarga de verificar Malware y bloquear los componentes al momento de su ejecución.
    - Firewall de punto de conexión: Evita conexiones indebidas por terceros que quieran realizar un ataque de hombre en el medio o filtrado de redes, es especialmente en sistemas WIFI-inseguros.
    - Protección de red: Establece alertas de conexión cuando existe alguna anomalía de la Red.
    - Control web/bloqueo de URL basado en categorías: Controla que si existe una página con contenido malicioso se proceda a su bloqueo.
    - Acceso controlado a carpetas: Con base a las disposiciones del administrador restringe el uso de información confidencial.
    - Protección de identidad: Permite tener controles para validar que la identidad no sea vulnerada y que un tercero se conecte con el usuario real, a través de ataques de suplantación de identidad.
    - Debe contar con soporte de fabricante vigente, no se permite el uso de antivirus con licencia GPL, GNU, Freeware o shareware, Antivirus en periodo de evaluación, Antivirus preinstalados en libre uso con características OEM o integrados operativo como Windows Defender, para ello deberá complementarse con otras herramientas de seguridad licenciadas.

- Adjuntar a los ingenieros de soporte de la Mesa de Ayuda, el listado del software que va a utilizar para con la ANM y evidencia de las licencias correspondientes (tanto para el sistema operativo como para las aplicaciones), se debe entregar al supervisor del contrato con copia a la Oficina de tecnología e Información. La OTI podrá negar con justa causa la conectividad de un equipo que no cumpla con las condiciones anteriormente establecidas.
- Los acuerdos contractuales con terceros deben establecer el cumplimiento de estas políticas de seguridad sin que esto sea una causal de incumplimiento de los acuerdos contractuales.

c. **Uso de ONE DRIVE**: El colaborador debe guardar la información asociada a la ANM y que se denomina como “corporativa de uso personal” en el repositorio de ONE DRIVE asociado a la cuenta asignada por la ANM. El tercero no debe hacer uso del sincronismo local de esta herramienta en un equipo personal. La OTI podrá establecer los controles de sincronismo solo para equipos asociados al dominio de la ANM.

d. **Información en dispositivos propios:** Los contratistas no deben mantener en sus equipos de cómputo información corporativa de la ANM clasificada como publica reservada o publica clasificada. La información objeto del desarrollo de sus funciones se debe mantener en los repositorios oficiales establecidos por la ANM tales como ONE DRIVE y SHAREPOINT. En caso de mantener algún archivo objeto del desarrollo de su actividad para con la ANM debe proceder a la eliminación segura de la información de su dispositivo.

e. **Responsabilidad de uso de información:** La ANM delega bajo su responsabilidad y custodia el manejo de la información "corporativa de uso personal" a cada tercero, por consiguiente y solo para el desarrollo del cumplimiento de sus funciones para con la ANM, la información en ONE DRIVE puede ser compartida con terceros externos a la entidad para el desarrollo de sus funciones, para ello debe comprender y aceptar las condiciones para intercambio de información y hacer uso de los controles establecidos por esta herramienta por consiguiente es responsable de las restricciones y de mantener la seguridad de la información bajo su custodia.

4.9. POLÍITICA DE CONEXIONES REMOTAS

La implementación del teletrabajo en la ANM supone una transformación organizacional, desde sus formas de planear y hacer, hasta sus formas de realizar seguimiento y evaluación. La ANM, viene liderando las alternativas que buscan un compromiso institucional y realizando acciones para la adopción e implementación del teletrabajo buscando que genere beneficios para sus funcionarios, estos lineamientos tanto de seguridad de la Información, Seguridad en el Trabajo se establecen en el "RESOLUCIÓN NÚMERO 201 DE 14 FEB 2023" liderado por el Grupo de Talento Humano.

Adicionalmente la necesidad que terceros se conecten a las redes informáticas de la ANM de manera remota para la prestación de servicios o dar cumplimiento a los alcances de sus contratos, supone la necesidad de conectarse a las aplicaciones internas y por lo tanto requerirá establecer lineamientos de seguridad para dichas conexiones así:

4.9.1. Lineamientos para la ANM para el teletrabajo.

a. la ANM debe realizar a través del área de Talento humano la verificación de las condiciones del lugar destinado al Teletrabajo, para el cumplimiento de las condiciones de seguridad física, ambiental, tecnológicas y de seguridad de la información.
b. Garantizar que los equipos de trabajo y en la oficina mantengan las condiciones de escritorio limpio
c. Validar que el teletrabajador conozca y acepte las condiciones de seguridad tecnológicas establecidas para conexiones remotas.
d. La OTI realizará las verificaciones técnicas establecidas en los lineamientos de seguridad para permitir la conectividad remota de equipos personales y de propiedad de la ANM como requisito fundamental para autorizar las conexiones remotas al teletrabajador.

4.9.2. Lineamientos para la ANM para con terceros

a. la ANM debe realizar a través del área de contratación asegurarse de que el tercero que realizará conexiones remotas a la red de la entidad haya comprendido los lineamientos en cuanto a políticas de seguridad de la información, cláusulas de confidencialidad, responsabilidad en al tratamiento de los datos personales y en especial:

- Lineamientos para conexión remota para el Teletrabajador o Tercero.
- Política de uso de dispositivos no corporativos

4.9.3. Lineamientos para conexión remota para Teletrabajadores, Proveedores y Contratistas

a. No se debe almacenar información de la ANM en el equipo personal, para esto debe dar cumplimiento a los lineamientos establecidos en el LITERAL "POLÍTICA DE USO DE DISPOSITIVOS NO CORPORATIVOS".
b. El tercero debe asegurar que la información sea procesada y almacenada se consolide en la infraestructura tecnológica de la Entidad.
c. Debe responsabilizarse por mantener las condiciones óptimas de seguridad en los dispositivos de comunicación, donde se obliga a tener una conexión WIFI privada y no compartida con terceros, la red debe estar protegida con contraseña fuerte y protocolos actualizados de seguridad WIFI.
d. Asegurar la comunicación por diferentes medios alternos de manera que se asegure la conectividad. Debe autorizar de manera obligatoria la implementación del doble factor de autenticación para todas las aplicaciones de la ANM
e. Cumplir con las políticas definidas por la ANM respecto al uso de aplicaciones, programas informáticos, protección de datos personales, propiedad intelectual y seguridad de la información.

f. Utilizar los datos de carácter personal, privado o sensible a los que tenga acceso, única y exclusivamente, para cumplir con las funciones propias en la Agencia Nacional de Minería, así como, garantizar que ningún tercero tenga acceso por cualquier medio a los datos de carácter personal, privado o sensible de la Entidad que está tratando en la modalidad de teletrabajo.

g. Informar a la Oficina de Tecnologías de la Información, según la ruta establecida, sobre conflictos de red o problemas tecnológicos o del equipo que requieran ser solucionados para el cumplimiento de las funciones.

h. Guardar la máxima reserva y confidencialidad sobre las actividades laborales que desarrolle de otros que en modalidad de teletrabajo puedan tener acceso a la información de la ANM. Se considera información confidencial la información de propiedad de la entidad y la información que genere el trabajador remoto en virtud de su vinculación

i. Debe garantizar y mantener las condiciones de privacidad de su entorno familiar, tales como el manejo del video en reuniones. La ANM no se hace responsable por imágenes emitidas en videoconferencias asociadas en el entorno familiar o del trabajo remoto.

j. Mantener indemne a la ANM por el uso del software no licenciado en equipos personales que a responsabilidad del colaborador y bajo su voluntad utilice para el desarrollo de labores de la ANM.
k. No hacer uso del correo electrónico personal, para ningún proceso de la Entidad.

l. No realizar descargas de información a los equipos personales que se encuentren almacenados en la redes o aplicaciones de la ANM.

m. Mantener rutinas de desconexión y conexión continua mientras se realizan labores que no requieren de conectividad.

n. Para teletrabajadores cumplir con todas las obligaciones establecidas en el artículo 22 del Decreto 1295 de 1994.

4.9.4. Lineamientos para la Oficina de Tecnologías e Información

a. Fortalecer las capacidades de monitoreo para la operación remota, con el fin de detectar accesos indebidos o situaciones anormales.

b. Contar con las capacidades y disponibilidad de los servicios de VPN o tecnologías equivalentes, seguridad en artículo 22 del Decreto 1295 de 1994.los servicios de correo electrónico y el acceso a la información de la Entidad, realizando un análisis de riesgos.

c. Denegar el acceso a VPN, Redes o aplicaciones por el incumplimiento de las medidas de seguridad establecidas para el teletrabajador, contratista, proveedor o en fin cualquier colaborador si se detectan riesgos de ciberataques a través de esa conexión remota.

d. Fortalecer el monitoreo en el uso de los datos personales e información confidencial.

e. Contemplar herramientas para la gestión remota en la Entidad.

f. Preparar a los funcionarios que prestan el soporte para la instalación y la configuración de los equipos para trabajo remoto.

g. Contemplar las políticas y procedimientos para evitar disputas acerca de derechos de propiedad intelectual desarrollados en equipos de propiedad privada de los funcionarios.

h. Determinar requisitos de seguridad sobre el firewall y de protección contra software malicioso.

i. Realizar revisiones del cumplimiento por parte del colaborador (Teletrabajador, contratista proveedor) de las condiciones de Seguridad establecidas en el documento de Lineamientos técnicos de seguridad para el Teletrabajo

b. Realizar la revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos de propiedad de ANM asignados al Teletrabajador, contratista o proveedores, cuando las actividades del teletrabajo finalicen o cuando finalice las autorizaciones establecidas por la ANM.

4.9.5. Método de conexión de la modalidad de acceso remoto en la ANM

La ANM en cumplimiento de la normatividad vigente tanto de teletrabajo o conectividad remota establece los lineamientos para conceder acceso de conexión remota.

a. Cada líder del proceso debe solicitar a la Oficina de Tecnología e Información la solicitud de conexión remota del colaborador y de asignación de los recursos tecnológicos que se hayan definido para trabajo fuera de oficina a través del formulario IMAC, indicando el tiempo de acceso por el cual se requiere la conexión.

b. La OTI establece las herramientas a instalar en el computador personal para que sea posible técnicamente la conexión remota, Para esto la OTI suministra el instructivo de instalación y/o prestará el servicio de instalación con la colaboración de la mesa de servicios tecnológicos.

c. La OTI otorgará las credenciales de acceso a la herramienta de conectividad establecida

4.10. SEGURIDAD DE LOS RECURSOS HUMANOS

4.10.1. Seguridad previa a la contratación y/o vinculación de funcionarios.

Los procesos de contratación deben ser regidos por el procedimiento de contratación y vinculación laboral establecido por el área de talento humano de la ANM.

Los acuerdos contractuales con funcionarios deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

4.10.2. Seguridad de la información previa para contratistas por prestación de servicios.

La verificación está a cargo del Grupo de Contratación, la cual debe tener en cuenta toda la privacidad pertinente, la protección de la información de datos personales y legislación laboral, y cuando se permita, debe incluir lo siguiente:

- La disponibilidad de referencias satisfactorias, por ejemplo, una comercial y una personal;
- Una verificación (completa y precisa) de la hoja de vida del solicitante;
- Confirmación de las certificaciones y títulos brindados.
- Una verificación de identidad independiente (pasaporte o documento similar);
- Las verificaciones de los antecedentes del contratista los cuales se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

- Establecer acuerdos o compromisos contractuales con el personal contratista donde se indiquen las responsabilidades en cuanto a la seguridad de la información.
- Firma formato de autorización de tratamiento de datos personales por parte del contratista.
- Los acuerdos contractuales deben establecer las responsabilidades y las de la organización en cuanto a la seguridad de la información.
- Cumplir con los lineamientos de la Lista de Chequeo "contrato de prestación de servicios, profesionales y apoyo a la gestión" que se encuentra en ISOLUCION.

4.10.3. Inicio de ejecución de actividades

El cumplimiento de las Políticas de Seguridad de la Información debe ser informado en el momento que inicie sus actividades contractuales, desde Talento Humano o contratación a todos los funcionarios, contratistas, proveedores o terceros o cualquier persona que tenga una relación contractual o situacional con la Entidad, o que tengan acceso a los activos de información de la ANM, por lo tanto:

a. Todo funcionario, contratista, proveedor o tercero que desde su gestión o alcance del contrato requiera del acceso a un sistema de información ejemplo (Websafi, SGD, ANNA Minería, CMC, Trámites en Línea, etc.) o a la red corporativa de la ANM, debe hacer la solicitud a través del formato IMAC y, éste debe estar autorizado por el líder del grupo o supervisor del contrato.

b. La solicitud a través del IMAC debe especificar claramente los permisos que el funcionario, contratista, proveedor o tercero, requiere para sus actividades y acceso a los sistemas de información u otro componente tecnológico, especificando los privilegios a ser asignados en el sistema de información.

c. Desde la Oficina de Tecnología e Información se debe gestionar el requerimiento descrito desde el formato IMAC dando alcance a cada solicitud del IMAC, con el especialista del sistema de información o componente tecnológico que corresponda.

d. Desde la Oficina de Tecnología e Información se debe notificar el alcance dado desde la solicitud del formato IMAC, con el fin de que el funcionario, contratista, proveedor o tercero, sea notificado y de inicio a sus labores o actividades contractuales.

e. El colaborador, al inicio de la ejecución de su contrato debe tener firmada la aceptación a la política de seguridad de la información y la aceptación de conocimiento y tratamiento de datos personales.

4.10.4. Durante la ejecución del empleo de funcionario o contratista

Todos los funcionarios, contratistas o proveedores a los que se brinde acceso a información confidencial deben firmar un acuerdo de confidencialidad y no divulgación de información, antes de tener acceso a las instalaciones

de procesamiento de información. Para los contratistas se maneja el contrato de prestación de servicios de apoyo a la gestión, además:

a. Los líderes de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades y derechos legales con relación a leyes sobre derecho de autor o legislación sobre protección de datos personales.

b. Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades para la clasificación de la información y la gestión de activos institucionales asociados con información, instalaciones de procesamiento de información y servicios de información que deben ser manejados por el funcionario o contratista.

c. Los líderes de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades del funcionario o contratista para el manejo de la información recibida de otras Entidades o partes externas.

d. El Grupo de Gestión de Talento Humano y el Grupo de Contratación deben asegurar que los funcionarios, contratistas y proveedores respectivamente conozcan y acepten la política de seguridad de la información publicada en el sitio Web de la entidad.

e. El Grupo de Gestión de Talento Humano debe establecer los mecanismos para asegurar que los funcionarios asistan a las charlas de sensibilización en seguridad de la información brindadas por la OTI. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.

f. El Grupo de Contratación y el Grupo de Talento Humano debe establecer los mecanismos para asegurar que los colaboradores asistan a las charlas de sensibilización en seguridad de la información brindadas por la OTI. Se debe tener en cuenta el manejo de datos personales, clasificación de la información, solicitud de recursos tecnológicos, incidentes de seguridad de la información y puntos de información para asesoría sobre seguridad de la información.

g. El Grupo de Gestión de Talento Humano o el Supervisor del Contrato para los contratistas y/o terceros, deben comunicar a la Oficina de Tecnología e Información (OTI) los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados. Especialmente actualizaciones sobre los accesos a carpetas compartidas y sistemas de información.

4.10.5. Terminación o cambio de responsabilidades de empleo

Se debe informar al personal los deberes y responsabilidades después de la terminación del empleo.

Previa emisión de paz y salvo para funcionario o contratista se debe considerar:

a. Tener formato de paz y salvo firmado por la OTI, el cual asegura que se retiraron los accesos lógicos y físicos de acuerdo con el procedimiento de control de acceso.

b. Tener formato de paz y salvo igualmente firmado por jefe inmediato o coordinador de grupo donde se aseguró de la transferencia apropiada de información al sucesor del cargo e informe de gestión que indica el estado de las actividades realizadas (en desarrollo, finalizadas o pendientes) y la aceptación del jefe inmediato o coordinador del grupo.

4.10.6. Procesos Disciplinarios

En atención al incumplimiento de los lineamientos establecidos en el presente documento, la Ley 734 de 2002 (Código Único Disciplinario), y demás legislación aplicable con relación a los procesos disciplinarios, la ANM sigue los parámetros de los procedimientos establecidos en la ANM

4.10.7. Intercambio de Información

La ANM ha establecido las condiciones para el acceso, consulta o intercambio de información con otras entidades en el Procedimiento Consulta y/o Intercambio de Información APO4-P-016, adicionalmente debe poner en conocimiento de instituciones interesadas, el protocolo de Acceso y/o Intercambio de Información APO4-P-016-PT-001.

4.11. GESTIÓN DE ACTIVOS

Si bien es cierto que los sistemas de información y la misma información digital están sujetos a amenazas graves desde el ciberespacio y, que pueden tener impactos adversos a la operación, comprometiendo los activos de información, tales impactos adversos, también pueden llegar a comprometer la confidencialidad, integridad y disponibilidad de la información procesada, almacenada y transmitida.

Es así como, se deben proporcionar niveles de protección a todos los activos de información de la Entidad. Todas estas medidas o lineamientos están orientados a mitigar los posibles riesgos.

4.11.1. USO ACEPTABLE DE LOS ACTIVOS

a. La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la ANM, son activos de la Entidad y se proporcionan a los funcionarios, contratistas y proveedores o terceros autorizados, para cumplir con los propósitos del negocio.

b. Se debe mantener un inventario actualizado de los activos digitales de información donde se determinan los responsables, el nivel de riesgo y confidencialidad de estos datos físicos o digitales que soy de propiedad de la ANM.

c. Los funcionarios, contratistas, proveedores o terceros y, todo aquel que cuente con acceso a la información de la ANM debe reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Gestión de Incidentes.

4.11.2. INVENTARIO DE ACTIVOS INFORMACIÓN.

d. Todos los funcionarios y contratistas deben etiquetar la información, y darle un manejo adecuado según su clasificación, siguiendo las directrices de Etiquetado de la Información que están dentro del procedimiento de Gestión de Activos de Información código APO4-P-009.

e. Cada área debe ser responsable de mantener actualizado el inventario de "activos de información" de acuerdo con las directrices del Procedimiento de Gestión de Activos.

f. Será responsabilidad de la OTI realizar las capacitaciones en los procesos de levantamiento y mantenimiento de los activos, así como coordinar la recolección de información de las diferentes Áreas por lo menos una vez al año.

g. Solo los activos debidamente clasificados podrán ser objeto de acuerdos de acceso o intercambio de información según su clasificación.

h. Todo activo que no se encuentre clasificado, tendrá la máxima reserva de confidencialidad hasta que exista una clasificación específica del mismo, por lo tanto, todo activo de información sin clasificar tendrá el estado de "información pública clasificada"

4.11.3. DEVOLUCIÓN DE LOS ACTIVOS

Todos los colaboradores usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. incluyendo una devolución formal de los activos de información.

4.11.4. CLASIFICACIÓN DE LA INFORMACIÓN

En atención a la Ley 1712 de 2014 y sus decretos reglamentarios, la Ley 1581 de 2012 de protección de datos personales y los requisitos de la norma NTC-ISO/IEC 27001:2013, la ANM clasifica, etiqueta y maneja la información y sus activos asociados de acuerdo con el Procedimiento de Gestión de Activos, además:

a. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado en la Matriz de Activos de Información e informar al Oficial de Seguridad de la Información para su respectivo acompañamiento del registro en caso de ser necesario.

b. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que los activos están clasificados y protegidos apropiadamente.

c. El funcionario, contratista, proveedor y/o tercero responsable del activo de información, debe definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes, teniendo en cuenta las políticas de control de acceso aplicables.

d. El funcionario, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse del manejo apropiado del activo cuando es eliminado o destruido.

e. Toda información contenida en los repositorios oficiales tiene por defecto connotación de “público clasificado” salvo que el dueño identificado del activo de información establezca en la matriz de activos una clasificación diferente.
f. Todo colaborador tendrá un repositorio en línea para almacenar información “personal corporativo” de la entidad, el colaborador es el responsable de determinar el nivel de seguridad y clasificación de la información dentro de estos repositorios.

4.12. USO DE EQUIPOS DE CÓMPUTO DE PROPIEDAD DE LA ANM

a. Está prohibido que personal ajeno a la Oficina de Tecnología e Información destape o retire partes de los equipos de cómputo propiedad de la ANM.

b. La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad del proceso de Administración de Tecnología e Información y, por tanto, se debe solicitar soporte a la Oficina de Tecnología e Información para la realización de estas labores.

c. Los equipos de cómputo no deben ser trasladados del sitio asignado inicialmente, ni cambiar el funcionario al que le fue asignado, sin previo aviso a la Oficina de Tecnología e Información.

d. Debe respetarse y no modificarse la configuración de hardware y software establecido por la Oficina de Tecnología e Información.

e. No se autoriza el uso de medios extraíbles para almacenamiento de información institucional (USB, Celulares, Memory Card etc.) en las estaciones de trabajo de la Entidad, con excepción para aquellos funcionarios que, por sus funciones y actividades propias institucionales, sean autorizados por vicepresidentes/Gerentes, Jefes de Oficina o Coordinadores Regionales, mediante formato IMAC debidamente diligenciado. Las Tabletas institucionales no requieren autorización y se hará uso sin restricción alguna.

f. Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes corporativas como los sistemas de información de la ANM, están prohibidas dando lugar a los procesos disciplinarios y/o legales correspondientes.

g. Durante la permanencia en las instalaciones de la ANM, los equipos de cómputo externos al dominio de la ANM deben estar conectados únicamente a la red de datos para visitantes corporativos administrada por la Oficina de Tecnología e Información.

h. Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.

i. Los equipos de cómputo (CPU y monitor), servidores, teléfonos IP y equipos de comunicaciones, debe conectarse a los puntos de corriente eléctrica identificados como regulados, con el fin de evitar picos altos que puedan dañar el componente tecnológico. Estos puntos de corriente regulada se usan para regular la energía y están soportados igualmente por las UPS, en caso falla en el flujo eléctrico evitando su apagado abrupto.

j. La conexión eléctrica de equipos personales debe hacerse a través de los puntos eléctricos no regulados. La ANM no se responsabiliza por daños que puedan sufrir estos dispositivos.

k. La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones de la ANM y que no son propiedad de la Entidad, es responsabilidad única y exclusiva de sus propietarios. La ANM, no es la responsable por estos equipos en ningún caso.

4.13. USO DE INTERNET

a. No se autoriza conectar módems o celulares para acceder a Internet, dentro de las redes (WAN, LAN, WLAN) de la entidad salvo la red habilitada para servicios de Visitantes, personal externo a la entidad o dispositivos personales de comunicación.

b. No se autoriza a los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico en cualquiera de sus variantes, o bien páginas que promuevan cualquier tipo de ideas

que puedan ser consideradas ofensivas para las normas de la Entidad como violencia, terrorismo, grupos al margen de la Ley, discriminación, entre otras.

c. No se autoriza el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.

d. Con el propósito de minimizar la probabilidad de saturación, interrupción, alteraciones no autorizadas y errores en la red de la ANM, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.

e. Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso.

f. Todas las actividades realizadas en los sistemas de información de la ANM deben ser monitoreadas con el fin de preservar la seguridad informática de la Entidad.

g. Ningún usuario está autorizado para asignar claves de administrador sobre los computadores de la Entidad. Esto es competencia de la Oficina de Tecnología e Información.

h. Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la Entidad.

i. La OTI debe establecer políticas de navegación con base al rol del colaborador en la entidad.

4.14. USO DEL CORREO INSTITUCIONAL

a. La Entidad debe proveer a los usuarios un correo electrónico institucional con el dominio anm.gov.co.

b. El estándar para la creación de buzón del correo es “primer nombre + punto (.) + primer apellido” ejemplo: Pedro González, en caso de que exista un homónimo, se debe crear de la siguiente manera “primer nombre + punto (.) + primer apellido + primera letra del segundo apellido” ejemplo: pedro González, en dado caso continúe la igualdad, la Oficina de Tecnología e Información debe asignar un correo basado en el nombre completo del colaborador.

c. La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la Entidad.

d. El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la Entidad; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones misionales y de apoyo desempeñadas.

e. El correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes o cadenas a familiares o amigos, esquemas piramidales, terrorismo, pornografía, programas piratas, proselitismo político, religioso o racial, amenazas, estafas, virus o código malicioso.

f. No se permite el envío de correos masivos desde cuentas institucionales, El envío de información masiva solo se habilita a grupos internos como ANM Nacional y ANM Central. Esta divulgación, es limitado y es de uso exclusivo del grupo de Talento Humano, el grupo de comunicaciones y comunicaciones desde la presidencia institucional.

g. Cuando se reciban correos desde una cuenta de divulgación como ANM Nacional y ANM Central evite dar una respuesta utilizando la opción responder a todos.

h. El servidor de correo, por políticas de seguridad de la información, tiene establecido bloquear archivos adjuntos o información nociva tales como otros archivos con extensión .exe o de ejecución de comandos.

i. No está permitido abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso (virus, troyanos, keyloggers, gusanos, etc.), lo cual podría atentar contra los sistemas, programas y datos de la Entidad.

j. No está permitido abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario como si fuera propia, sin embargo, es responsabilidad de cada usuario mantener sus sesiones atendidas, entiéndase no dejar los equipos sin cerrar sesión al alcance de cualquier intruso.

k. Para el envío de información pública clasificada, publica reservada, confidencial, sensible o con datos personales, se debe hacer uso de la herramienta de cifrado establecida en el cliente de correo electrónico.

l. El usuario debe notificar cualquier recibo de correo sospechoso, a la cuenta servicios.tecnologicos@anm.gov.co, el correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

4.15. GESTIÓN DE MEDIOS REMOVIBLES

Los medios removibles en los que se almacene información clasificada como información pública clasificada e información pública reservada deben estar cifrados, de acuerdo con las directrices del procedimiento de gestión

de activos APO4-P-009 (tabla controles según clasificación de información). La Oficina de Tecnología e Información debe establecer herramientas tecnológicas para el cifrado de la información, además:

a. La OTI debe proveer el uso de carpetas compartidas en lugar de medios removibles para el intercambio de información al interior de la Entidad.

b. Las unidades de medios removibles de las estaciones de trabajo, equipos portátiles y servidores se deben bloquear mediante directorio activo y quien requiera hacer uso de estas unidades debe solicitar la activación a la Oficina de Tecnología e Información, previa autorización del Coordinador de Grupo, indicando el tiempo por el cual se requiere la activación.

c. Los funcionarios o contratistas que requieran los medios removibles habilitados de forma permanente deben tener una autorización firmada por el vicepresidente, Jefe de Oficina o Coordinador de Grupo.

d. Se debe hacer seguimiento a la transferencia de información de los medios removibles mediante herramientas tecnológicas que permita realizar la trazabilidad de la información transmitida a estos medios.

e. Los vicepresidentes, gerentes y jefes de oficina, deben controlar el ingreso y salida de los equipos de cómputo y medios extraíbles de almacenamiento de información de las instalaciones de la ANM, mediante el AP02-P-001-F-006 Formato Único de Retiro de Elementos ANM.

f. Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la Entidad se debe remover y formatear el dispositivo.

g. Los medios removibles no deben ser utilizados en sitios públicos como un café internet, así mismo, debe tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.

4.16. DISPOSICIÓN DE LOS MEDIOS

a. Los medios que contienen información confidencial se deben disponer en forma segura, mediante incineración, destrucción o el borrado seguro de datos antes de ser reutilizados o dados de baja.
b. La información en los medios externos de Backup que contienen información pública clasificada o información pública reservada se debe cifrar, además debe estar protegida en un lugar seguro y bajo llave, el lugar que disponga la OTI.
c. La información almacenada en medios removibles debe ser transferida a medios nuevos antes de que se vuelvan ilegibles, de acuerdo con el tiempo de vida útil de los mismos, esta actividad debe ser coordinada por la OTI.
d. Se debe guardar varias copias de datos valiosos para la ANM en medios separados, con el fin de evitar la pérdida de información por daño, pérdida o robo de los medios removibles.

e. Los backups se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones, para aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios etc.
f. La OTI debe realizar pruebas a las copias de datos para validar la integridad de la información.

4.16.1. TRANSFERENCIA DE MEDIOS FÍSICOS

a. Para la transferencia de medios físicos (Información en carpetas selladas, computadores, dispositivos móviles, tablets, etc.) se debe seguir las directrices del Procedimiento de Gestión de Activos APO4-P-009 y sus documentos relacionados (mensajería externa o interna - tabla controles según clasificación de información).

b. El embalaje de la información debe ser apropiada para mitigar los daños físicos que se puedan presentar en el transporte de la misma, protegiendo la exposición al calor, humedad o campos electromagnéticos.

c. Se debe llevar un registro que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

4.17. CONTROL DE ACCESO

4.17.1. LINEAMIENTOS CONTROL DE ACCESO

El Proceso de Administración de Tecnologías e Información debe controlar el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

a. **Lo que necesita conocer:** solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).

b. **Lo que necesita usar:** solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, recintos) que la persona necesita para la realización de su tarea/trabajo/rol.

4.17.2. ACCESO A REDES Y SERVICIOS EN RED

a. El acceso a redes Wi-Fi se controla con autenticación por contraseña utilizando un protocolo de seguridad que no tenga vulnerabilidades conocidas.
b. La Oficina de Tecnología e Información, provee un servicio de conectividad a todos los funcionarios y contratistas de la Entidad para la navegación en internet, dicho acceso es controlado por usuario, mediante la autorización previa de vicepresidentes, gerentes, jefes de oficina o coordinadores de grupo, mediante el formato IMAC.

c. Los usuarios que requieran contar con servicios especiales de mensajería instantánea, páginas de encuentro o descargas, deben ser autorizados por el jefe inmediato, mediante formato IMAC dirigido a la Oficina de Tecnología de la Información, justificando la necesidad del acceso.
d. La conexión remota a la red de área local de la ANM debe ser realizada a través de una conexión VPN segura o mecanismos similares de acceso seguro la cual debe ser suministrada por la Oficina de Tecnología e Información, la cual debe ser aprobada por los vicepresidentes o Jefes de Oficina mediante formato IMAC dirigido al jefe de la Oficina de Tecnología e Información.
e. La conexión a servicios en red, se controla mediante el directorio activo, a excepción del control de acceso físico mediante acceso biométrico y el servicio de impresión.
f. La conexión a redes públicas abiertas está prohibida, así como la conexión a redes Wi-Fi públicas.
g. Todo acceso o privilegio a sistemas, redes, aplicaciones o información de la ANM debe estar aprobado por los líderes de las áreas y los propietarios de información según aplique.
h. El acceso a la red Wi-Fi de la ANM para los visitantes debe realizarse por la red destinada para estos accesos a visitantes, de no conocer este acceso se debe solicitar a la Mesa de Ayuda para su debida activación.

i. Es responsabilidad del Oficial de Seguridad de la Información definir los lineamientos a seguir para garantizar accesos seguros y confiables a los sistemas y plataformas de la ANM.

4.17.3. SOLICITUD O INICIO DE ACCESO

Los procedimientos definidos por la ANM para administrar los privilegios de acceso de los usuarios a la información de la ANM deben comprender la asignación, la modificación y la revocación de los permisos. Todos los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y debe tener en cuenta por lo menos, que:

a. Los líderes de grupo son los únicos funcionarios autorizados para realizar las solicitudes de acceso a los sistemas de información o delegados formalmente por el líder para ejecutar esta actividad, que se realiza mediante el formato IMAC.

b. Ningún colaborador autorizado puede realizar solicitudes de acceso para sí mismo, excepto para el Presidente de la Entidad, Vicepresidentes y Jefes de Oficina.

c. Los jefes o quienes hagan sus veces, deben realizar las solicitudes de acceso a los sistemas de información requeridos por los funcionarios o colaboradores a su cargo en las herramientas establecidas por la ANM para tal fin, para lo que debe tener en cuenta las matrices de accesos previamente definidas y gestionadas por cada especialista funcional de la OTI.

d. La OTI, asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada grupo y/o proceso.

e. La confirmación de la gestión del requerimiento y el envío de los datos de autenticación deben ser enviados usando un canal seguro. Esta entrega debe estar controlada por un proceso de administración formal que permita, informar a los usuarios sobre el compromiso de cumplir con los lineamientos de seguridad establecidos para el buen uso de los datos de acceso (usuarios / contraseña) otorgados.

f. El re-uso de nombres de cuentas no está permitido, aun cuando la cuenta de usuario ya se encuentre eliminada/inactiva. Para lo cual la OTI debe aplicar el procedimiento definido para la creación de cuentas de usuario y correo electrónico.

g. Asignar identificaciones únicas a todos los funcionarios y colaboradores, es decir, que no debe existir cuentas genéricas para el acceso o gestión sobre los sistemas tecnológicos de la Entidad (equipos, aplicaciones, bases de datos, sistemas operativos, entre otros). Cuando por razones del negocio u operación deben ser creadas únicamente como cuentas de servicio y no deben ser utilizadas por ningún funcionario o contratista. En el Directorio Activo se debe detallar el responsable de cada cuenta. En caso de ser necesario un usuario genérico este debe quedar asignado a un responsable y debe quedar documentado en el mismo directorio activo.

h. La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, es decir el uso de las claves de usuarios administradores, tales como: “root”, “adm” y “system”, entre otros, debe ser controlado por la OTI quienes son los responsables de dichos accesos, de esta gestión existirá un registro que permita identificar la trazabilidad es decir conocer el funcionario o colaborador que está haciendo uso de estos accesos.

i. Las cuentas privilegiadas deben ser monitoreadas a través de la plataforma de seguridad de cuentas privilegiadas.

j. Todo usuario del sistema debe tener un mecanismo de autenticación privado.

k. En caso de ser necesario se debe utilizar métodos de autenticación fuerte como sensores biométricos, huellas dactilares, certificados digitales, entre otros.

l. El acceso de un usuario debe ser limitado sólo a la información requerida para el desarrollo de sus funciones.

m. Para los equipos de cómputo se debe establecer bloqueos o terminación de sesiones automáticas en caso de que queden desatendidos, con el propósito de proteger la información.

n. La utilización de información compartida por ejemplo unidades de red debe estar restringida mediante controles ejecutados por la OTI. El responsable y/o dueño de la información debe definir los accesos a la información únicamente al personal autorizado.

o. Todos los usuarios creados en ambiente de producción de los sistemas de información o servicio de la ANM, deben ser solicitados según el procedimiento establecido en el formato IMAC, con el fin de mantener

un registro formal o la trazabilidad de los privilegios otorgados a los colaboradores autorizados, para cumplir con las labores asignadas, utilizando algún servicio tecnológico.

p. Los accesos a la información o sistemas de información no deben otorgarse por los administradores de Base de Datos y de Aplicaciones del servicio hasta que se hayan completado los procedimientos de autorización.

q. Se debe considerar la inclusión en los contratos del personal y contratos de servicio con terceros, cláusulas que especifiquen las sanciones si los colaboradores o terceros intentan un acceso no autorizado.

4.17.4. SUSPENSIÓN O TERMINACIÓN DE ACCESO

El acceso a los sistemas debe ser suspendido para todo funcionario o colaborador de la ANM que se encuentre en licencia, permisos, vacaciones, entre otras novedades; si por necesidad del negocio se requiere habilitarlo temporalmente, los jefes deben realizar las solicitudes de acceso necesarias a través del formulario IMAC para sus colaboradores que requieran ejecutar las actividades justificando su solicitud y estableciendo un plazo máximo de 3 días para estas acciones.

a. La OTI debe mantener actualizado el Directorio Activo con la información de los usuarios de funcionarios y colaboradores, de acuerdo con el último formato IMAC solicitado para la gestión de los usuarios de la ANM; en la cual debe registrarse las novedades de estos para que se realice la suspensión o eliminación según corresponda.

b. Se debe definir y aplicar reglas para deshabilitar las cuentas de usuarios de red que no han cambiado la contraseña durante 180 días, igualmente se debe definir qué cuentas deben quedar bloqueadas porque no fueron reactivadas y eliminar aquellas cuentas que no presentan ninguna actividad desde su creación.

c. Los usuarios creados con acceso a las bases de datos que no hayan sido utilizados en un período mayor o igual a 3 meses, deben ser inhabilitados por los administradores de Base de Datos, así mismo, si éstas no han sido utilizadas en un periodo igual o mayor a 6 meses debe ser eliminadas.

d. La OTI debe disponer de mecanismos documentados para desactivar el acceso a los usuarios, en las siguientes, situaciones:

- Desvinculación de los funcionarios a la ANM.
- Licencias temporales de los colaboradores, o suspensión temporal de contratos para contratistas.
- Los funcionarios de la Entidad que no han accedido a los recursos tecnológicos por un período de tiempo determinado.

- Número de intentos fallidos durante el ingreso de la contraseña a un recurso tecnológico o aplicativo o cuando se presente algún tipo de incidente de seguridad de la información sobre el código de usuario.

- Cuando el responsable de la información lo solicite.

4.17.5. REVISIÓN O VALIDACIÓN DE ACCESOS

Las autorizaciones de acceso a sistemas y/o aplicaciones debe ser revisadas periódicamente por los coordinadores de grupo y/o propietarios de la información.

La oficina de tecnologías e información debe revisar o monitorear en intervalos de tiempo regulares los privilegios asignados a los usuarios tanto en redes como aplicaciones solicitando reporte a administradores de aplicaciones funcionales, para asegurar que no tengan accesos no autorizados; teniendo en cuenta los siguientes aspectos:

a. Validar solicitudes de accesos especiales como USB y VPN, administrador de máquina y acceso remoto.

e. Los derechos de acceso de un usuario se deben revisar y reasignar, ya sea por cambio de cargo o traslado de área, dentro de la misma Entidad. Teniendo en cuenta:

- El nuevo jefe debe realizar los requerimientos de acceso a los sistemas de información que el colaborador requiera según las funciones que le sean asignadas en el área.

- Se asignan los permisos autorizados por el nuevo jefe y se eliminan los demás permisos y privilegios del cargo anterior.

4.17.6. IDENTIFICACIÓN DE LOS USUARIOS

Todos los usuarios deben tener un identificador único (ID de usuario) para uso personal y se debe seleccionar una técnica de autenticación adecuada para garantizar la identidad del usuario. Este control se aplica a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, proveedores, programadores de sistemas y administradores de bases de datos etc.).

Solo En caso de ser necesario un usuario genérico este debe quedar asignado a un responsable y debe quedar documentado en el mismo directorio activo.

4.17.7. NORMAS PARA LA CREACIÓN DE CONTRASEÑAS

Los usuarios y contraseñas son de uso personal e intransferible, cualquier utilización indebida y/o irregularidad debe ser responsabilidad del colaborador. Como medida de seguridad, los usuarios deben crear y administrar sus contraseñas siguiendo las siguientes normas para la creación y el uso:

a. Las contraseñas se consideran como información confidencial y deben ser protegidas como tal.

b. La contraseña debe tener al menos ocho (8) caracteres, donde se incluyan letras en mayúscula, minúscula y números o caracteres especiales.

c. Las contraseñas deben cambiarse mínimo cada 180 días y no se pueden repetir las ultimas 10 contraseñas.

d. Si se digita más de 3 veces la contraseña de forma inválida, la cuenta del usuario debe ser bloqueada. Se deberá solicitar el desbloqueo a través de un requerimiento desde Mesa de Ayuda. Para el desbloqueo de la cuenta, a través de unas validaciones, el usuario puede rescatar su contraseña de manera autónoma en una interfaz web de la ANM.

e. La contraseña no debe incluir un nombre o palabra en algún lenguaje común (español, inglés, etc. evitando que éstas sean vulnerables a los ataques de diccionarios.) u otra información pública como números de tarjeta de crédito, nombres de calles y números telefónicos. Una contraseña debe incluir información que solo sea conocida por el usuario.

f. No utilizar contraseñas por defecto, éstas se deben cambiar una vez se adquieran componentes tecnológicos nuevos o sistemas de información que perfectamente las puedan incluir.

g. No es permitido compartir usuarios, contraseñas y cualquier mecanismo de autenticación asignado (ej. Tokens).

h. Dispositivos como los Tokens que permitan el acceso a un sistema de información en la Entidad o Entidades externas deben ser almacenados y salvaguardados en lugares seguros, donde solamente el dueño del Token tenga acceso.

i. En los casos que se sospeche del compromiso de una contraseña en un posible incidente de seguridad, ésta debe ser cambiada inmediatamente por el administrador de la aplicación y debe reportarse al Oficial de Seguridad de la Información.

j. Los usuarios deben tener presente no incluir las claves en ningún proceso de registro automatizado; por ejemplo, almacenado en una macro o sistema de información.

k. La entidad debe establecer el múltiple factor de autenticación en los sistemas de información que lo permitan.

4.17.8. SEGREGACIÓN DE FUNCIONES

La segregación de funciones en la ANM representa una actividad de control clave para separar las responsabilidades de las diversas actividades que intervienen en la ejecución de los procesos, una adecuada segregación de funciones permite mantener la confidencialidad, integridad y disponibilidad de la información.

a. La segregación de funciones permite reducir el riesgo de un mal uso accidental o deliberado del sistema, razón por la cual se debe definir lineamientos para evitar accesos no autorizados que permitan, modificar o utilizar los activos sin autorización o detección.

b. La segregación de funciones en cada uno de los procesos de la Entidad, debe garantizar como mínimo la independencia de las siguientes actividades:

- Operación de equipos de cómputo
- Administración de red
- Administración de sistemas Operativos
- Administración de bases de datos
- Administración de aplicaciones (Administradores Funcionales)
- Desarrollo de software
- Gestor de cambios
- Administración de seguridad informática

Teniendo en cuenta lo anterior los líderes de cada proceso, tienen la responsabilidad de actualizar la matriz de roles y responsabilidades periódicamente al menos una vez al año.

4.18. REQUERIMIENTOS DE NEGOCIO PARA EL ACCESO LÓGICO

Las Jefaturas, Vicepresidencias, Presidencia o líderes de proceso deben definir los privilegios de los colaboradores a su cargo siempre, bajo los conceptos de menor privilegio y necesidad de saber, igualmente es responsabilidad de la Jefatura de la OTI establecer procedimientos formales para controlar la definición de perfiles y la asignación de derechos de acceso a los usuarios, previamente definidos por los responsables del proceso. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta la eliminación o desactivación.

4.18.1. CONTROL DE ACCESO A LAS APLICACIONES Y RECURSOS TECNOLÓGICOS

a. Los accesos a las aplicaciones y recursos tecnológicos deben ser restringidos y monitoreados de acuerdo con las necesidades del negocio.

b. La OTI debe definir y mantener los lineamientos para controlar el acceso de los colaboradores a las aplicaciones o recursos tecnológicos.

c. La OTI debe implementar mecanismos de monitoreo de accesos, control de privilegios con el fin de identificar posibles incumplimientos a las políticas de Seguridad de la Información.

d. La selección de los mecanismos de control de acceso a las aplicaciones se define de acuerdo con la criticidad y/o sensibilidad de la información (procesada, almacenada, usada) utilizada por el proceso.

e. Se debe utilizar medidas de seguridad para restringir el acceso a los aplicativos, bases de datos y en general a los recursos tecnológicos.

f. Las aplicaciones de la Entidad deben contar con mecanismo para el manejo de contraseñas, que sean interactivas y cumplan con los parámetros de seguridad definidos, para ello debe tener en cuenta:

- La OTI debe mantener custodia de los usuarios administradores o usuarios con privilegios de las aplicaciones, bases de datos, servidores y equipos de infraestructura de la entidad y delegar usuarios específicos con los Roles necesarios para su gestión de administración.

- Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación.

- En los aplicativos y/o sistemas de información, tener en cuenta los lineamientos de contraseñas robustas.

- Los aplicativos deben contar con controles para cambio de contraseña obligatorio en su primer ingreso o registro.

- Mantener un registro de contraseñas de usuario previas y evitar el re-uso.

- No mostrar las contraseñas en la pantalla en el momento de ingresarlas.

- Almacenar las contraseñas cifradas con algoritmos fuertes, mediante uso de funciones hash.

- Validar el nivel de seguridad de las contraseñas de acceso creadas por los colaboradores, permitiendo solamente el uso de contraseñas fuertes.

- Los aplicativos deben controlar el cambio de contraseña en periodos definidos.

- Implementar políticas de bloqueo automático del usuario cuando la contraseña se haya ingresado de manera errónea por tres veces, igualmente definir e implementar mecanismos que permitan su desbloqueo incluyendo: un tiempo de desbloqueo automático de 15 minutos, asignación de nueva contraseña haciendo uso del sistema de control de acceso, entre otras alternativas.

4.18.2. RESTRICCIÓN DEL ACCESO A LA INFORMACIÓN

a. El acceso de los usuarios a la información y las funciones del sistema de la aplicación debe limitarse de acuerdo con la política de control de acceso definida.

b. Las restricciones para el acceso a las aplicaciones se deben basar en el rol que el usuario desempeñará, para ello se debe cumplir con los siguientes aspectos:

- Generar menús para controlar el acceso a las funciones del sistema de aplicación.
- Controlar los permisos de acceso de los usuarios: lectura, escritura, modificación y eliminación.
- Controlar y definir la interacción e intercambio de datos entre sistemas (internos y externos).
- Hay que asegurar que las salidas de información de los sistemas, aplicaciones o plataformas que manejan información confidencial sólo contengan la información requerida para el cumplimiento de las labores y solamente el personal autorizado tenga acceso a esta.

4.18.3. RESTRICCIONES DE USO SOBRE LOS SISTEMAS OPERATIVOS.

Dentro de los aspectos para tener en cuenta por parte de los usuarios, para un buen uso de los sistemas operativos están:

- El administrador de la plataforma es el responsable de otorgar los accesos a los recursos del sistema operativo.
- Las autorizaciones a las rutinas del sistema operativo no deben permitir modificaciones, en caso de requerirse, éstas deben ser autorizadas y documentadas, conforme los procedimientos establecidos por la entidad.
- El uso de herramientas o utilitarios propios de los sistemas operativos, deben ser limitado a personal autorizado y su uso está restringido a casos específicos, debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados.
- Los administradores y operadores de plataformas, no deben tener acceso a aplicaciones en producción, archivos y transacciones en línea.
- Está prohibido el uso de herramientas intrusivas o con fines de vulnerar la seguridad del sistema operativo, bases de datos, redes etc.; solamente el Oficial de Seguridad de la Información podrá utilizarlas en la realización de pruebas de hacking ético o quien éste delegue.

- Las sesiones que no han presentado actividad alguna por un período determinado, deben finalizar automáticamente de acuerdo con la configuración definida; esto mismo aplica para los accesos remotos.

- Todos los colaboradores de la ANM deben cumplir con las normas de contraseñas.

- Todas las estaciones de trabajo deben estar plenamente identificadas para garantizar la conexión de equipos confiables, esto debe venir acompañado de correctas configuraciones de red que restrinjan la conexión a los equipos de la granja de servidores permitiendo solamente las conexiones necesarias.

- Se deben registrar los accesos exitosos y los intentos fallidos de autenticación de los sistemas de información.

4.18.4. USO DE LAS UTILIDADES DEL SISTEMA

El jefe de la Oficina de Tecnología e Información debe implementar procedimientos para restringir y controlar el uso de los programas de utilidad que podrían ser capaces de vulnerar los controles del sistema y/o aplicación y mantener un inventario de éstos. Se debe tener en cuenta entre otros aspectos:

- Limitar el uso de los programas utilitarios a un número práctico mínimo de usuarios autorizados y confiables.
- Registro de todo uso de los programas de utilitarios.
- Definir y documentar los niveles de autorización de los programas de utilitarios.
- Grabar las sesiones sobre servidores críticos de las cuentas privilegiadas.

4.18.5. CONTROL DE ACCESO A LA RED

La Oficina de Tecnología e Información debe implementar procedimientos para controlar el acceso a la red de la ANM, proporcionando a los funcionarios o colaboradores el acceso a los servicios para los que específicamente se les haya autorizado su uso. Se debe considerar entre otros los siguientes lineamientos:

a. La utilización de recursos de red debe ser limitada a usuarios autorizados.

b. Para acceder a las redes de datos de la ANM, se requiere autenticación individual.

c. Las contraseñas de red de usuario y las contraseñas de usuarios privilegiados deben ser cambiadas periódicamente (mínimo una vez por mes).
d. Cuando se requiera realizar transferencia de información en especial la clasificada como publica clasificada o publica reservada, se debe utilizar mecanismos de cifrado o canales seguros.

e. La ANM permite a usuarios externos (proveedores o terceros) acceder a las redes institucionales desde redes externas, bajo ciertas condiciones de seguridad. Dicha autorización debe ser tramitada por el líder del proceso ante la OTI, en caso de ser aprobada, no se deben utilizar identificadores genéricos. No obstante, solo en el caso de ser necesario un usuario genérico este debe quedar asignado a un responsable y debe quedar documentado en el mismo directorio activo.

f. Los líderes de proceso que tienen acuerdos contractuales con proveedores o terceros y, si éstos requieren acceso a los recursos tecnológicos de la Entidad, deben contar con autorización previa de parte de la Jefatura de la OTI. De igual manera, se debe asegurar que los proveedores o terceros conozcan y acepten las políticas de Seguridad de la Información y que las normas o acuerdos específicos de seguridad que apliquen para la actividad contractual queden registrados en el documento de acuerdo contractual.

g. Los administradores de sistemas deben identificar y documentar los niveles máximos de servicio. Así mismo, hay que asegurar que el acceso y utilización de los recursos informáticos cumplen con los requerimientos de seguridad.

h. Se deben definir validaciones o revisiones teniendo en cuenta la criticidad de los proveedores o terceros ante el cumplimiento de la política de Seguridad de la Información, como los acuerdos específicos de seguridad para el desarrollo de las labores con los terceros. Este cumplimiento podrá ser validado por entes de control.

i. Cuando los usuarios acceden a datos en redes locales y remotas vía VPN, deben utilizar mecanismos de seguridad para autenticarse ante las redes. Las solicitudes deben ser realizadas ante la OTI quienes deben realizar el trámite respectivo y para lo cual es requisito contar con usuario de red asignado, posteriormente se remite al jefe de la OTI para asignar el acceso.

j. El jefe de la OTI debe mantener las redes de datos internas segmentadas por VLANS, grupos de servicios, usuarios y sistemas de información.

k. Todas las estaciones de trabajo conectadas a la red de la ANM deben contar con herramientas de seguridad, como firewalls, HIDS, Filtros de Contenido, Antivirus, Endpoint, entre otros.

l. El servicio de correo externo no debe ser habilitado para proveedores o terceros y temporales, salvo casos excepcionales por funcionalidad de un servicio.

4.18.6. ACCESO A DATOS DE PRODUCCIÓN

El líder de la OTI debe tener en cuenta las siguientes consideraciones respecto al acceso a datos de producción:

a. Se debe definir un procedimiento para el control de acceso el cual incluya la aprobación, supervisión, etc., a los datos de producción.

b. Para todo usuario autorizado, la disponibilidad de la información debe ser limitada.

c. Los procedimientos deben ser definidos para conceder el acceso de emergencia de usuarios a datos de producción.

d. El acceso a datos de producción debe ser auditable. El acceso a los datos de producción debe generar archivos de trazabilidad (logs) que pueden ser auditados, por entes de control.

e. Para acceder a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación) se debe contar con autorización de la Oficina de Tecnología e Información, lo anterior con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.

4.18.7. CONEXIONES REMOTAS

Se define como acceso remoto, cualquier conexión establecida desde fuera de la Entidad que requiere acceso a la red o aplicaciones internas de la ANM por parte de funcionarios, proveedores entre otros.

Para dichos accesos se debe tener en cuenta las siguientes consideraciones:

a. Iniciar la conexión remota de red desde computadores y sitios seguros, evitar conexiones remotas desde computadores públicos o desconocidos como, cafés internet, aeropuertos, hoteles o redes inalámbricas públicas.

b. Las conexiones remotas a los recursos de la plataforma tecnológica; deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado y por periodos establecidos, de acuerdo con las labores desempeñadas.

c. La autenticación para los accesos remotos a administración de servidores o aplicaciones debe complementarse con múltiple factor de autenticación y/o a través de la plataforma de seguridad CyberArk o la que haga sus veces.

d. Si es el caso, se debe aprobar o aceptar del lado de la Entidad para que el proveedor tome el control remoto. No debe permitirse el acceso y control total de manera automática, sino cuando la ANM lo autorice y monitorear las actividades realizadas por estos proveedores.

e. El trabajo remoto por VPN lo debe solicitar el jefe directo, conforme al procedimiento definido de solicitud de requerimientos (IMAC). la OTI valida la pertinencia de dicha solicitud y otorga el privilegio, evaluando y aplicando las medidas de protección adecuadas que garanticen una conexión segura.

f. El acceso remoto a los servidores debe estar controlado por las políticas del Directorio Activo para el ingreso por este servicio, es decir quién puede o no ingresar por este servicio, teniendo presente que este

servicio debe ser autorizado únicamente para los administradores de los servidores, los usuarios o proveedores fuera de la oficina no deben tener estos accesos o llamado a este servicio.

g. Las aplicaciones críticas de la ANM deben forzar la autenticación mediante el protocolo seguro.

4.19. CONTROLES CRIPTOGRÁFICOS

La Oficina de Tecnología e Información debe:

a. Determinar los algoritmos criptográficos y protocolos autorizados para su uso en la ANM y configurar los sistemas para permitir únicamente aquellos permitidos, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrado débil.

b. Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se valide durante el periodo que han perdido su confidencialidad.

c. La administración de llaves criptográficas y certificados digitales están a cargo de La Oficina de Tecnología e Información, sin embargo, la administración de tokens bancarios, tokens para acceso a SIIF (Sistema Integrado de Información Financiera) y firmas digitales están a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus labores.

d. Los administradores de bases de datos de la OTI, deben establecer una estrategia para cifrar las bases de datos críticas de la ANM, velando por no afectar el desempeño del sistema de información.

e. La OTI debe dar a conocer y capacitar a los funcionarios, contratistas, proveedores o terceros en el uso de las herramientas de uso criptográfico, cuando así se requiera su uso.

f. Realizar revisiones periódicas a las herramientas de uso criptográfico (Tokens, firma digital, etc.), con el fin de detectar fallas o vulnerabilidades.

g. Notificar con anticipación a los dueños de la información, aplicaciones, software que requieran certificados digitales, la fecha de caducidad de éstos para su renovación.

h. Realizar la entrega de los certificados digitales generados para su aplicación y uso.

i. Realizar las configuraciones requeridas para el uso y administración de los certificados de firma digital.

j. Prestar soporte técnico para la configuración de los usuarios y soluciones adoptadas para controles criptográficos.

k. Velar porque la información clasificada y reservada (en reposo y transmisión), se trasmita cifrada haciendo uso de las herramientas que la ANM haya adoptado.

l. Comunicar al Comité Institucional de Gestión y Desempeño, los eventos o incidentes que conlleven al no cumplimiento de los objetivos institucionales por el no uso de controles criptográficos para la información clasificada y reservada.

m. Proporcionar los recursos necesarios para la administración y monitoreo en el uso de controles criptográficos a través de herramientas o software de seguridad.

n. Identificar los puertos USB para quienes estén autorizados para la firma digital y contar con este inventario con el fin de dar seguimiento al buen uso de la información.

Los funcionarios y colaboradores de la ANM deben:

a. Conocer y cumplir la política de uso de controles criptográficos.

b. Los funcionarios o contratistas a quienes les fueron asignados tokens bancarios y tokens de acceso a SIIF, deben hacer uso de estos dispositivos, en los horarios de atención al usuario y almacenarlos bajo llave cuando no hagan uso de éstos, o cuando se van a retirar de sus puestos de trabajo.

c. Informar a los líderes del proceso, las desviaciones que se presenten por el no uso de los controles criptográficos para la información clasificada y reservada.

d. Gestionar los riesgos que se presenten por el no uso de controles criptográficos para la protección de la información clasificada y reservada.

e. Ser responsable del manejo de la información clasificada y reservada, para que ésta esté protegida con las medidas de seguridad necesarias.

f. En caso de pérdida o daño de un token, comunicar este incidente a la Oficina de Tecnología e Información a través de la Mesa de Ayuda, para su respectiva reposición, al igual, si la clave secreta o llave de cifrado ha sido vulnerada.

g. Devolver a la Oficina de Tecnología e Información, el token y las llaves de cifrado en caso de situaciones administrativas que lo desvinculen laboral o temporalmente como (vacaciones, licencias, permisos, etc.), así como la finalización de contrato de prestación de servicios. Esta verificación se debe dar a través del Paz y Salvo de entrega del cargo y que sea aceptado por la OTI.

4.19.1. FIRMA DIGITAL

a. Los certificados digitales, firmas digitales, llaves de cifrado de la información, token criptográfico (físico o lógico), son de uso personal e intransferible.

b.

c. Los funcionarios autorizados para hacer uso de la Firma Digital son: Presidente, Vicepresidentes Jefes de Oficina, Coordinadores de grupo y Gerentes de Proyecto.

d. La firma digital se utilizará para cumplir con las normativas legales, para identificar al firmante de manera inequívoca, para certificar la integridad del documento o cuando se requiera proteger un documento o la información (autenticidad e integridad) con un riesgo asociado resultado de una evaluación de riesgos.

e. Para el uso de firma digital dentro de la ANM, se ha establecido que éstas deben ser individuales, es decir cada funcionario que esté autorizado para el uso de la firma digital, es responsable único de la firma del documento.

f. La firma digital individual, se da mediante un token personalizado, con estampado cronológico e incorporando la identificación de las características del creador del documento.

g. Por ser una firma individual, la ANM debe adquirir los tokens, que se requieran para el uso de la firma digital y su asignación a cada funcionario que adopte esta responsabilidad.

h. La firma digital, debe ser verificada a través de una llave pública incluida en un certificado válido emitido por una entidad certificadora, a la cual, se le deben exigir acuerdos de niveles de servicio para el servicio de certificación o verificación.

i. Se debe realizar mantenimiento anual a todas las firmas digitales.

j. Una vez firmados los documentos con la firma digital, debe conservarse en su estado electrónico para garantizar su validez.

k. Una vez firmados digitalmente los documentos, se deben convertir en formato PDF y debe visualizarse a través del Sistema de Gestión Documental, dispuesto por la entidad

l. Si el documento que se firma es confidencial, sensible o reservado, es importante conocer que la firma digital no da privacidad a la información, por lo que su tratamiento requiere de otro control criptográfico. (Ej. Una herramienta de cifrado de información para su transporte o almacenamiento).

m. Los funcionarios autorizados para el uso de firma digital en la ANM, antes de firmar un documento que tiene otras firmas digitales, deben asegurarse de que estas firmas previas no han sido alteradas.

n. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:

- Es única a la persona que la usa.
- Es susceptible de ser verificada.
- Está bajo el control exclusivo de la persona que la usa.
- Está ligada a la información o mensaje de datos, de tal manera que, si éstos son cambiados, la firma digital es invalidada.
- Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

Los funcionarios que hagan uso o les sea asignada la firma digital deben velar por el cumplimiento de los atributos que establece la Ley 527 de 1999 como son:

a. **La autenticidad:** En la medida que se puede verificar en un mensaje de datos firmado digitalmente quién es su autor, es quién se compromete jurídicamente.

b. **La integridad:** El destinario de ese mensaje de datos podrá verificar si la información ha sido o no alterada en el proceso de comunicación electrónica, lo que es muy útil para determinar la originalidad electrónica del mensaje de datos, especialmente a la luz de los artículos 8 y 9 de la Ley 527 de 1999.

c. **El no repudio:** Quien firma digitalmente se compromete con la suscripción respectiva y posteriormente no le es dado retractarse o refutar dicho acto.

4.19.2. FIRMA ELECTRÓNICA

Todos los funcionarios y contratistas que desde el directorio activo se autentiquen a un sistema de información de la ANM, pueden hacer uso de la firma electrónica, enviando el contenido del mensaje a través de un medio electrónico válido, ejemplo: una solicitud a través del formato IMAC. Para el envío de información externa, será con base en su clasificación y será autorizada por el dueño del proceso.

En la Agencia Nacional de Minería se contempla la firma electrónica bajo las siguientes circunstancias:

- Permitir la identificación de quien firma con el fin de determinar que la persona es quién dice ser.
- La firma electrónica solo puede ser generada por el emisor del documento.
- La firma electrónica podrá ser validada pero no falsificada.
- La firma electrónica está creada de un modo que solo está bajo el control de quien firma.
- La firma electrónica está vinculada a los datos de tal forma que si los datos son alterados la firma dejará de ser válida.
- La firma electrónica debe servir para indicar que el contenido cuenta con su aprobación.
- Debe ser confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.

4.19.3. CIFRADO DE LA INFORMACIÓN

La Agencia Nacional de Minería debe contar con controles que permitan definir y administrar los mecanismos de cifrado de información, para este propósito, se ha definido un Instructivo Seguridad Cifrado, que permita el intercambio de información cifrada, para minimizar los riesgos en este proceso de intercambio o transporte de la información, que puedan brindar seguridad y confianza, además:

a. Se debe hacer uso de cifrado para la protección de claves de acceso, llaves criptográficas a datos, información clasificada y reservada, y todos aquellos servicios que estén expuestos a internet.

b. Cifrado en la transmisión de información clasificada y reservada por los diferentes canales de comunicación que utilice en el Entidad.

c. Cifrado en el resguardo de información clasificada y reservada en cualquier medio físico o componente tecnológico, o cuando así surja de la evaluación de riesgos realizada por el Dueño de la información y el Oficial de Seguridad de la Información.

d. Los equipos de funcionarios cuyo manejo de información sea confidencial y que deban salir de las instalaciones de la entidad, deben contar con cifrado de disco duro.

4.19.4. LLAVES CRIPTOGRÁFICAS

Con el fin de garantizar la confidencialidad e integridad de los datos o la información de un documento, la Agencia Nacional de Minería debe garantizar la protección de la información en reposo como en tránsito, para lo cual ha adoptado hacer uso de algoritmos de seguridad que cumplan con la reglamentación legal y la protección y privacidad de la información.

Por lo anterior, es importante además de la información, proteger las claves secretas o llaves criptográficas para que no sean vulneradas ni modificadas sin autorización. Por consiguiente, la Oficina de Tecnología e Información debe velar por la custodia de estas y todo su ciclo de vida que se relaciona a continuación.

a. **Generación:** Es la selección del valor que se va a utilizar para ser usado por un algoritmo criptográfico específico o aleatorio, La llave debe ser elegida de tal manera que no sea previsible y que en el proceso no se presente un acceso no autorizado.

b. **Distribución:** Es el proceso de traslado de una llave desde el punto de su generación hasta el punto donde va a ser usada, siendo la mayor exigencia en los algoritmos simétricos. En la ANM, se exige el uso de cifrado para las llaves.

c. **Instalación:** Es el proceso de almacenamiento de la llave en el dispositivo o proceso que se va a usar y debe mantener en todo momento la protección para evitar el acceso no autorizado. En la ANM se exige el uso de cifrado para las llaves.

d. **Almacenamiento:** Las llaves solo pueden ser almacenadas en forma cifrada, con el fin de evitar su manipulación o intento de acceso no autorizado.

e. **Cambio:** Establece la vigencia de una llave, a mayor tiempo de vigencia de una llave, mayor será la probabilidad de acceso no autorizado. El periodo se define en cada caso particular dependiendo del nivel de riesgo identificado en el activo de información.

f. **Eliminación:** Las llaves debe ser eliminadas para evitar su divulgación, esto aplica para los valores de las llaves que por algún momento puedan encontrarse en forma clara o sin cifrado en algún medio de almacenamiento.

g. **Protección:** Se debe usar mecanismos que protejan las llaves de accesos y modificaciones no autorizadas.

h. **Revocación:** hace relación a la invalidez de una llave antes de cumplir el periodo de vigencia establecido y el responsable de esta acción es el funcionario al que le fue asignada la llave correspondiente.

Las razones por las cuales un funcionario debe solicitar a la Oficina de Tecnología e Información la revocación de una llave, clave secreta o token bajo su responsabilidad son las siguientes:

- Pérdida del dispositivo en el cual se encuentra almacenada la llave.
- Se evidencia alguna circunstancia en la cual se ha dado acceso no autorizado a la llave, clave secreta o token.
- Reporte de ataques informáticos o acción de algún tipo de programa maligno.
- Cuando el funcionario responsable de la gestión de la llave termina su relación laboral o en situaciones contractuales con la Entidad.

4.19.5. CERTIFICADOS DIGITALES

Los responsables de los sistemas de información deben ser conscientes en el uso y caducidad que pueda tener un certificado digital, esto con el fin de comunicar a la Oficina de Tecnología e Información para su emisión e implementación.

El responsable de la solicitud ante la entidad certificadora para la emisión de los certificados también debe velar por la caducidad de éstos, teniendo como control un listado de todos los certificados emitidos con la fecha de

caducidad y la asignación de éstos en los sistemas de información. En la ANM, se establece el uso de certificados digitales para:

a. Garantizar la autenticidad del sitio, servicio o aplicativo Web.

b. Evitar el riesgo de ataques de suplantación de identidad o phishing de los sitios Web.

c. Proteger la confidencialidad de la información intercambiada entre la Entidad y sus ciudadanos o titulares mineros a través del sitio Web.

d. Establecer conexiones seguras cifrando la información intercambiada entre los aplicativos y los ciudadanos o titulares mineros.

e. Salvaguardar la integridad de la información intercambiada, porque el certificado presenta las características de la Entidad, algoritmo de cifrado, fecha de emisión del certificado, etc.

4.20. SEGURIDAD FÍSICA Y DEL ENTORNO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido, en consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales. Toda área donde se solicite o capture datos personales debe contar con anuncio al público de dicha actividad, a su vez esta información debe ser conservada de acuerdo con la Ley 1581 de 2012 de Protección de Datos Personales.

4.20.1. ÁREAS SEGURAS

La ANM en sus instalaciones tiene implementado un sistema de control de acceso físico mediante huella biométrica por cada piso, sin embargo (con ocasión de la pandemia COVID-19, la entidad retomó el control de tarjeta de proximidad). Adicionalmente, cada piso cuenta con una recepción donde se controla el ingreso y salida de terceros, y el ingreso y salida de elementos, tanto de funcionarios como de terceros. A sí mismo la ANM debe exigir a los proveedores, que gestionen o procesen información por fuera de las instalaciones de la ANM, cumplir con las políticas de seguridad de ANM y las que disponga el proveedor en sus instalaciones.

El Datacenter o centros de cableado, deben contar con mecanismos que cumplan los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que allí se alojan, igualmente debe contar con sistemas mecánicos para control de incendios, controlar el acceso a personal no autorizado, así como restricciones de consumo de alimentos, bebidas o cigarrillo.

La ANM cuenta con un Sistema de Seguridad con Circuito Cerrado de Televisión - CCTV, para otorgar la mayor seguridad posible tanto a los ciudadanos como a los funcionarios que ingresan a sus instalaciones. El Sistema de Seguridad CCTV opera bajo las siguientes directrices:

a. La Oficina de Tecnologías e Información es la responsable del mantenimiento y soporte de la plataforma tecnológica que soporta el sistema CCTV.

b. La Oficina de Tecnologías de Información, debe garantizar el funcionamiento del sistema CCTV las 24 horas del día de los 365 días del año. El Grupo de Servicios Administrativos garantizará la operación y monitoreo.

c. El acceso al centro de monitoreo es de carácter restringido. Las únicas personas que tienen permiso de acceder son los operadores, o aquellos funcionarios que autorice el Grupo de Servicios Administrativos.

d. Cuando el operador de medios tecnológicos del CCTV deba ausentarse de su puesto de trabajo, éste procederá a notificar o registrar en la bitácora diaria.

e. El operador de medios tecnológicos del CCTV debe registrar en la bitácora diaria cualquier evento ocurrido durante su turno.

f. El operador de medios tecnológicos del CCTV debe notificar vía telefónica o electrónica a la Oficina de Tecnología e Información, acerca de las fallas o ausencias de video que se presenten en las cámaras del sistema CCTV de la Agencia. Lo anterior con el fin de restablecer dicho servicio y mantener su correcto funcionamiento.

g. Cuando el operador detecte que alguna cámara ha sido girada sin autorización, debe informar al Grupo de Servicios Administrativos, para que se genere la evidencia y se autorice devolverla a su posición original.

h. Cuando el operador de medios tecnológicos del CCTV detecte anomalías o incidentes en las zonas de monitoreo, éstas deben ser reportadas inmediatamente al Supervisor de contrato de Vigilancia y Seguridad Privada.

i. Las imágenes en video están protegidas por la ley 1581 de 2012 (Protección datos personales) y se restringe el acceso a dicha información, en consecuencia, toda solicitud de copias de video debe hacerse por escrito al Grupo de Servicios Administrativos. Procedimiento APO2-P-008

j. La descarga de videos es posible realizarla únicamente en el centro de monitoreo de la sede principal de la ANM. En las diferentes sedes de la entidad no existe la posibilidad de descarga de videos, solo se permite la visualización.

k. Todas las grabaciones tienen una duración mínima de 30 días y después se reescribe.

l. Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.

m. Toda copia de video generada debe ser entregada mediante oficio o mediante cadena de custodia.

n. La oficina de Tecnologías e información debe brindar las condiciones de almacenamiento para dar cumplimiento a los tiempos de retención establecidas para tal fin. A su vez debe la confidencialidad y disponibilidad de esta información.

o. La ANM debe contar con un plan de emergencias definido por el Grupo de Servicios Administrativos, que debe ser probado anualmente, con el fin de brindar protección contra amenazas externas.

4.20.2. UBICACIÓN Y PROTECCIÓN DE LOS EQUIPOS

El datacenter se encuentra ubicado en un sitio seguro, con controles de acceso de personal no autorizado, y es administrado por personal de la OTI-. El datacenter externo cumple con las características de seguridad TIER III que garantizan la eficiencia de los procesos y dan fe de que el servicio cumple con las normas y estándares internacionales de Calidad, Gerenciamiento de Servicios de TI, Seguridad de la Información y de la Infraestructura

4.20.3. SERVICIOS DE SUMINISTRO

La ANM debe contar con servicios redundantes en **todos** los niveles así:

Debe contar a nivel físico con aire acondicionado de contingencia, UPS (sistema de alimentación ininterrumpida, en inglés (Uninterruptible Power Supply) que asegure al menos 15 planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica.

4.20.4. SEGURIDAD DEL CABLEADO

El Datacenter de la ANM debe cumplir parcialmente con el estándar ISO/IEC 11801 de seguridad óptima para cableado estructurado.

4.20.5. MANTENIMIENTO DE EQUIPOS

La Oficina de Tecnología e Información debe establecer y ejecutar planes anuales de mantenimiento de la infraestructura tecnológica de la ANM, el cual se estable en el Formato informe de servicio / APO4-P-002-F-003.

.

4.20.6. SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES

La salida de elementos de la ANM es controlada mediante el formato APO2-P-001-F-006 Formato Único de Retiro de Elementos ANM.

a. Los equipos y medios removibles que son retirados de las instalaciones de la ANM deben estar debidamente cifrados.

b. Los funcionarios y contratistas que retiren equipos o medios removibles de las instalaciones de la ANM deben seguir las siguientes directrices:

- En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de la ANM, se debe colocar la denuncia ante la autoridad competente e informar inmediatamente al Jefe de Grupo y al Grupo de Servicios Administrativos para que se inicie el trámite interno correspondiente.
- Los equipos de funcionarios cuyo manejo de información sea confidencial y que deban salir de las instalaciones de la entidad, deben contar con cifrado de disco duro.

4.20.7. DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS

Cuando una estación de trabajo o equipo portátil se reasigne o sea dado de baja, se debe realizar una copia de respaldo de la información de la ANM que allí se encuentre almacenada (en caso de ser necesario), conforme los lineamientos establecidos por la entidad, posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada (destrucción física, eliminación o sobre escritura de los medios que contienen información) con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma. Ver indicaciones adicionales en el procedimiento de borrado seguro.

4.20.8. POLÍTICA DE EQUIPO DESATENDIDO, ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Todos los colaboradores de la ANM deben conservar su escritorio libre de información propiedad de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

a. Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), estos deben ser enviados con pin de seguridad y retirados de la impresora inmediatamente.

b. Los computadores deben cargar por defecto el fondo de pantalla de la ANM, éste no debe ser modificado y debe permanecer activo.

c. Los funcionarios y contratistas de la ANM deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplique el comando de bloqueo oprimiendo

simultáneamente las teclas Windows + L), a su vez, la Oficina de Tecnología e Información debe implementar mecanismos para cierres de sesión automáticos no superior a cinco minutos.

d. Los usuarios son responsables y asumen las consecuencias por la pérdida de información que esté bajo su custodia. Se prohíbe el almacenamiento de información personal en los computadores de la ANM. El escritorio lógico (del computador) debe estar libre de información pública clasificada e información pública reservada.

e. La información de gestión del área deber ser almacenada por los usuarios en carpetas compartidas del área y la información de gestión del usuario en el almacenamiento virtual de OneDrive corporativo de Office 365.

4.21. SEGURIDAD DE LAS OPERACIONES

4.21.1. DOCUMENTACIÓN DE PROCEDIMIENTOS OPERATIVOS

Se debe contar con procedimientos documentados de trabajo debidamente para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

4.21.2. CONTROL DE CAMBIOS

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se debe realizar de acuerdo con los lineamientos del Procedimiento de Gestión de Cambios Tecnológicos APO4-P-010.

4.21.3. GESTIÓN DE CAPACIDAD

La ANM debe gestionar la capacidad de su plataforma tecnológica (hardware y software) de acuerdo con las indicaciones del Procedimiento de Gestión de Capacidad APO4-P-008.

4.21.4. SEPARACIÓN DE LOS AMBIENTES

La ANM debe contar con ambientes de desarrollo, pruebas y producción separados por máquinas físicas y máquinas virtuales.

La ANM debe controlar el acceso al ambiente de pruebas de la misma forma que controla el acceso al ambiente de producción.

4.22. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

a. Se deben proteger las estaciones de trabajo, equipos portátiles, dispositivos móviles y servidores propiedad o de uso de la ANM contra códigos maliciosos.

b. Los contratistas que hagan uso de sus equipos personales deben contar con un software antivirus según especificaciones previas en el literal POLÍTICA DE USO DE DISPOSITIVOS NO CORPORATIVOS.

c. El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

d. El único servicio de antivirus autorizado en la ANM es el asignado directamente por la Oficina de Tecnología e Información (OTI), el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

e. El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

f. El usuario no debe instalar o emplear programas que no se encuentren autorizados para manejo de antivirus.

g. Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus y que han sido establecidos por la Oficina de Tecnología e Información.

h. El programa de antivirus debe ser instalado única y exclusivamente por la Oficina de Tecnología e Información en los servidores y estaciones de trabajo de la ANM.

4.23. COPIAS DE RESPALDO

La ANM debe realizar copias de respaldo de la información y pruebas periódicas a las mismas. Para ello la Oficina de Tecnología e Información define el procedimiento de copias de respaldo APO4-P-012, que definen las actividades para la estrategia de backup requeridas; además:

a. La Oficina de Tecnología e Información debe establecer los lineamientos para la realización y validación de copias de seguridad .

b. Todos los administradores de base de datos, aplicaciones y servicios deben cumplir con las políticas de backup establecidas por la Oficina de Tecnología e Información.

c. La Oficina de Tecnología e información debe realizar copias de respaldo a las carpetas compartidas definidas en el servidor de archivos de la ANM.

d. Todas las copias de respaldo deben ser almacenadas en un área adecuada y con control de acceso, y aplicar los controles para la protección de los medios de respaldo.

e. Todas las copias de respaldo deben contemplar un plan de continuidad del negocio, orientado a evitar la pérdida de la información al contemplar un sitio secundario para su preservación.

f. Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.

g. Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la Entidad, motivo por el cual se deben establecer todas las condiciones de seguridad por parte del responsable de su salvaguarda. La ANM proporciona herramientas en línea para salvaguardar la información corporativa y de uso personal pero corporativa, por lo cual es de responsabilidad del usuario almacenar en este repositorio la información y habilitar esta herramienta como aplicación de escritorio en caso de que lo considere necesario. En caso de ser necesario el usuario puede solicitar la colaboración a la OTI por medio de la mesa de servicios tecnológicos.

h.

4.24. REGISTRO Y SUPERVISIÓN DE EVENTOS

4.24.1. REGISTRO DE EVENTOS

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones de la ANM, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

4.24.2. Protección de la información de registro

La Oficina de Tecnología e Información con el fin de proteger la información de registro de modificación no autorizada por parte de usuarios no autorizados, administradores u operadores de los sistemas de información debe implementar mecanismos de copiado de logs en “tiempo real” a un sistema por fuera del control de administradores y operadores de los sistemas.

4.24.3. Sincronización de relojes

Con el fin de obtener un control apropiado para la relación adecuada de eventos no deseados en la infraestructura o para la investigación efectiva de incidentes, los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por la ANM debe estar sincronizados utilizando como referencia la hora oficial de Colombia de INM (Instituto Nacional de Metrología) horalegal.inm.gov.co

4.25. CONTROL DE SOFTWARE OPERACIONAL

4.25.1. INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

El proceso de instalación y desinstalación de software, está autorizado exclusivamente al personal de la Mesa de Ayuda del Proceso de Administración de Tecnologías e Información, Por lo tanto, a los funcionarios o contratistas no le es permitido realizar esta labor.

Para la instalación de software se debe seguir las siguientes directrices:

- El software licenciado debe contar con su respectiva documentación (Licencia) y en el caso del software libre debe estar permitido el uso comercial.
- El instalador debe ser descargado de la página oficial del fabricante.
- Debe dejarse evidencia documentada en lo repositorios destinados por la OTI para tal fin de que las directrices fueron correctamente realizadas.

Se debe proporcionar capacitación adecuada a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de las nuevas adquisiciones de software o mejoras al software existente, antes de su puesta en producción.

Todo el software nuevo y mejorado debe estar completamente soportado por una documentación suficientemente amplia y actualizada, y no debe ser puesto en el ambiente de producción sin contar con la debida documentación.

- **Documento de licencia del software** (representa el permiso que da el fabricante para la instalación y uso de su producto)

- **Manual de instalación del software** (Para determinar que el software ha sido instalado apropiadamente)

- **Manual del usuario para uso del software** (Para guiar al usuario en su uso y apropiación)

La OTI debe realizar revisiones periódicas anuales del uso del software instalado en las estaciones de trabajo y servidores de la Entidad, con el fin de validar el cumplimiento de la Ley 603 de 2000 de Derechos de Autor, conjuntamente debe identificar los activos de información que se encuentran afectados por derechos de propiedad intelectual.

Todo software que viole los acuerdos de licenciamiento debe ser desinstalado inmediatamente y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la política y de los términos y condiciones de uso, poniendo en riesgo la seguridad de la información y quizás sanciones económicas por incumplimiento a la Ley 603 de 2000 de derechos de autor

Para contar con una trazabilidad del software instalado en los componentes tecnológicos de la ANM, (sistemas operativos, programas ofimáticos, sistemas de información), entre otros, se debe contar con un sistema de control de la configuración, en donde se observen los cambios ejecutados en dicho software, como (instalación de parches, cambios de versiones, actualizaciones, etc.), con el fin de mantener el historial y el control del software operacional en la ANM.

Toda reproducción del software, transporte, almacenamiento, adquisición para la venta o distribución sin la debida autorización del titular, se constituye como un delito a los Derechos Patrimoniales del Autor.

Todo software que la ANM adquiera debe ser del conocimiento de Arquitectura Empresarial quien a su vez debe emitir criterios adicionales con el fin de que el software a adquirir cuente con la interoperabilidad en su instalación y uso con los demás sistemas de información de la Entidad.

La OTI debe comunicar a los funcionarios y contratistas sobre las consecuencias por utilizar software ilegal; conjuntamente con la Oficina Asesora Jurídica debe definir y establecer las cláusulas de los contratos para cumplir con la legislación vigente relacionada con los derechos de autor y datos personales.

El software que desde fábrica de software se contemple y, los desarrollos Inhouse, debe anexar un certificado de uso y cesión de derechos según sea el caso, cuando de adquisición se trate.

Es importante que la Oficina Asesora Jurídica, haga parte de esta adquisición en cuanto a la lectura que se haga a la licencia, derechos de autor y propiedad intelectual del software adquirido y que será propiedad de la ANM cuando de desarrollos de Fábrica de Software y Desarrollos Inhouse se trate.

Para llevar el Control del Software Operacional instalado en la ANM, se han establecido los siguientes procedimientos:

- Procedimiento Administración de la infraestructura tecnológica APO4-P-002
- Formato dar de Baja un Software

4.26. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

La Oficina de Tecnología e Información, es responsable de verificar de manera periódica anual la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la Entidad, adicionalmente, debe contar con un procedimiento y análisis de vulnerabilidades que permitan la identificación y mitigación de las vulnerabilidades identificadas en toda la plataforma tecnológica de la ANM.

4.26.1. GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS

a. Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o Hacking Ético para las plataformas críticas de la Entidad, cuya viabilidad técnica y de administración lo permita.

b. Una vez se lleve a cabo la ejecución de escaneos de vulnerabilidad en la plataforma tecnológica de la Entidad, la identificación de estas vulnerabilidades o hallazgos se deben remediar de acuerdo con los lineamientos establecidos desde el Procedimiento de Gestión de Vulnerabilidades.

c. Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de La Oficina de Tecnología e Información, para estas remediaciones se debe tener en cuenta las directrices establecidas en el Procedimiento de Gestión de Cambios cuando su aplicación se lleve al ambiente de producción.

4.27. AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

4.27.1. Controles sobre auditorías de sistemas de información

Para la ejecución de auditorías a los sistemas de información se debe tener en cuenta las siguientes consideraciones:

a. Los requisitos de auditoría para acceso a sistemas y a los datos se deberán acordar con los líderes de los procesos involucrados.

b. El alcance de las pruebas técnicas de auditoría se debería acordar y controlar entre auditores y auditados.

c. Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se debe realizar en horario laboral en un ambiente controlado.

d. Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.

e. Las pruebas de auditoría se deben limitar a acceso a software y datos únicamente para lectura.

4.28. SEGURIDAD EN LAS COMUNICACIONES

La Oficina de Tecnología e Información, debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de la información en las redes definidas en la Entidad, la disponibilidad de los servicios en red y la seguridad en sí de la información que viajan a través de estos canales de redes de comunicaciones.

4.28.1. GESTIÓN DE LA SEGURIDAD EN LAS REDES

La Oficina de Tecnología e Información debe definir e implementar mecanismos de separación de las redes de la ANM con base en los niveles de confianza (por ejemplo, dominio de acceso público, dominio de computador de escritorio, dominio de servidor), por dependencias (por ejemplo, oficina de talento humano, oficina de

servicios administrativos, oficina de gestión financiera, oficina de tecnología e información) o alguna combinación (por ejemplo, un dominio de servidor que se conecta a múltiples dependencias), además:

a. La Oficina de Tecnología e Información debe mantener separadas la red de datos y la red de voz, con el fin de minimizar el impacto de interceptación de alguna de las dos redes.

b. El acceso remoto a las redes de la ANM se controla mediante conexiones VPN, las cuales deben estar monitoreadas para que se evidencie la desactivación de ésta en el tiempo que se ha definido.

4.28.2. TRANSFERENCIA DE INFORMACIÓN

La ANM debe firmar acuerdos o compromisos de confidencialidad con los servidores públicos y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que, por alguna razón, requieran conocer o intercambiar información restringida o confidencial. En este acuerdo deben quedar especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se debe firmar antes de permitir el acceso o uso de dicha información.

Todos los lineamientos para la transferencia de información deben aplicarse en toda la Entidad, proveedores y terceros que dentro de sus funciones se establezca la necesidad de intercambio de información física como digital.

Actualmente se cuenta con el procedimiento de Consulta y/o Intercambio de Información APO4-P-016, el cual incorpora, el formato de intercambio de información entre Entidades, el cual deber ser firmado por los representantes de las partes cuando se lleve a cabo esta transferencia de información, además tener en cuenta:

a. Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar la clasificación de la información y las consideraciones de seguridad sobre la misma, así como, los lineamientos que se establecen en el Procedimiento de Intercambio Seguro de Información APO4-P-016.

b. Todos los responsables de la información deben asegurar que el intercambio de información con el tercero (Contratos, convenios, pólizas, etc.), esté debidamente autorizada y protegida conforme a los lineamientos del procedimiento Intercambio Seguro de Información.

c. Todos los responsables de la información deben ser quienes autoricen la transferencia de la información que esté bajo su responsabilidad, teniendo en cuenta la legislación (Ley 1581 de 2014 y Ley de Habeas Data de 2008).

d. Todos los responsables de la información deben seguir las indicaciones del Procedimiento de Gestión de Activos de Información, para la transferencia y transporte de la información, teniendo presente que esté totalmente etiquetada como se indica en este procedimiento.

e. La transferencia de información digital debe contemplar una trazabilidad de toda la actividad de envío de los datos, a través de logs, en donde se registre la siguiente información:

- Fecha y hora de envío.
- Dirección IP de origen y destino.
- Usuario que envía la información.
- Algoritmo de cifrado o firma digital usada.

f. El proveedor de servicios en la Nube para los servicios con los que cuenta la ANM, debe certificar que se dispone de una transferencia de información segura hacia la Nube.

g. Independientemente del modo en el que se produzca el intercambio de información, es necesario contar con los controles de seguridad, que generen confianza y protección de la información

4.29. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La Oficina de Tecnología e Información debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la ANM. Las dependencias que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en la Oficina de Tecnología e Información para definir los requisitos de seguridad de la información. Para ello, debe tener en cuenta los lineamientos establecidos en el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de información, además los siguientes:

4.29.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

a. El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario. Por ejemplo, la implementación de segundos factores de autenticación y un sistema de gestión de contraseñas que exija el uso de contraseñas fuertes, el cambio periódico de contraseñas y que guarde un historial de contraseñas para evitar su reutilización.

b. Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.

c. Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad. Por ejemplo, cifrado de información almacenada, el envío de información por canales cifrados.

d. Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación mediante HTTPS, cifrado de contraseñas almacenadas y uso de firmas digitales.

e. Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.

f. La necesidad de exigir la implementación de metodologías de desarrollo seguro.

g. Los desarrolladores propios de la ANM liberan de derechos de autor cualquier desarrollo hecho para el cumplimiento de sus funciones u obligaciones contractuales, siendo estos derechos de autor únicamente de la Agencia.

4.29.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

La Oficina de Tecnología e Información debe definir e implementar principios de desarrollo seguro en actividades de construcción de sistemas de información internos.

Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso de construcción. También se debe revisar regularmente para que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

Los lineamientos para el desarrollo seguro deben aplicarse también para los sistemas de información existentes en la ANM y, a los de uso externo con los proveedores (Fábrica de desarrollo), teniendo en cuenta el Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información, además:

a. La ANM (OTI y supervisor del contrato); deben velar porque el desarrollo tanto interno como externo de los sistemas de información, cumpla con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, la ANM debe asegurar que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Entidad.

b. Los cambios en sistemas deben realizarse de acuerdo con el Procedimiento de Gestión de Cambios APO4-P-010.

c. En todo desarrollo interno, externo y/o a través de la fábrica de desarrollo, se debe hacer uso de metodologías de desarrollo seguro, que contemplen lineamientos de seguridad en todas las etapas del desarrollo.

4.29.3. AMBIENTE DE DESARROLLO SEGURO

a. La Oficina de tecnología e Información debe aplicar los mismos controles en al ambiente de producción y ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

b. La Oficina de Tecnología e Información debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el Procedimiento de gestión Cambios Tecnológicos APO4-P-010.

c. La Oficina de Tecnología e Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la ANM.

4.29.4. DESARROLLO CONTRATADO EXTERNAMENTE

Cuando se contrata desarrollo externo, se debe acordar el cumplimiento de los niveles de soporte requeridos por la ANM. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación, además:

a. Las dependencias deben asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

b. Las dependencias deben exigir el suministro de evidencia de la realización de pruebas de seguridad al software desarrollado por terceros.

c. Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

d. Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

e. Las dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.

f. Las dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la ANM a realizar auditorías durante el desarrollo del contrato.

4.29.5. PRUEBAS DE SEGURIDAD DE SISTEMAS

Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

4.29.6. PRUEBAS DE ACEPTACIÓN DE SISTEMAS

Independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable); en estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido las brechas de seguridad, además:

a. Se debe realizar pruebas de aceptación del software por una persona diferente a quien han desarrollado el software, además estas pruebas evidenciadas a través de un documento, deben estar firmadas por quienes realizaron las pruebas, en donde se acepte que el software desarrollado cumple con los lineamientos y funcionalidades para su uso. Para mayor detalle se debe dirigir al "Manual de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información".

b. De ser posible, las pruebas se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo de la ANM, y que las pruebas son confiables.

c. En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados conforme el instructivo de GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD. EST1-P-003-I-002

4.29.7. DATOS DE PRUEBA

La Oficina de Tecnología e Información debe certificar que la información entregada a los desarrolladores (tanto internos como externos) para sus pruebas, debe ser enmascarada y los datos sensibles deben ser eliminados con el fin de no revelar información confidencial de los ambientes de producción, dando cumplimiento a la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información pública).

4.30. RELACIÓN CON LOS PROVEEDORES

4.30.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES.

La ANM debe establecer mecanismos de verificación de lineamientos de seguridad en sus relaciones con todos los proveedores, especialmente aquellos proveedores críticos para la ANM por el manejo de información crítica o confidencial, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que cumplan con las políticas de seguridad de la información, es fundamental que se llevan a cabo visitas a los proveedores con el fin de identificar situaciones que puedan comprometer la información de la ANM en el no cumplimiento de los lineamientos establecidos en este manual. Para estas visitas se ha

establecido el Procedimiento GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADA A PROVEEDORES APO4-P-014.

4.30.2. TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES.

a. Los supervisores de contratos deben asegurar que se comuniquen las políticas y procedimientos de seguridad de la información a los proveedores y/o contratistas.

b. El Grupo de contratación debe incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información**:**

- Cláusula de confidencialidad.
- Cláusula que defina las responsabilidades que continúan después de terminado el contrato (por ejemplo, confidencialidad durante 5 años después de terminado el contrato).
- Cumplimiento de las políticas de seguridad de la información de la ANM.
- Reporte de eventos de seguridad de la información a través de los canales definidos en el procedimiento de gestión de incidentes de seguridad de la información APO4-P-007.
- Etiquetado y manejo de la información de acuerdo con las directrices del procedimiento de GESTIÓN DE ACTIVOS DE INFORMACIÓN APO4-P-009.
- Cláusula de seguimiento y revisión de los servicios de los proveedores o terceros para asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, en los acuerdos contractuales correspondientes.

c. Los supervisores de contratos deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad de la información establecidos con ellos y monitoreando la aparición de nuevos riesgos.

d. Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la Oficina de Tecnología e Información, utilizando el formato IMAC.

4.31. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La gestión de incidentes de seguridad debe ejecutarse de acuerdo con los lineamientos del Procedimiento de Gestión de Incidentes, donde se debe establecer como mínimo: quiénes deben reportar, los canales de comunicación, tipo de situaciones que se deben reportar, decisiones sobre las situaciones reportadas, respuesta a incidentes, aprendizaje de estos y recolección de evidencias digitales.

Es deber de todo funcionario, contratista o colaborador informar el incumplimiento de los lineamientos descritos en este manual.

Cualquier incumplimiento identificado debe remitirse al Oficial de Seguridad de la información, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación.

Categorías de incidentes de seguridad de la información: Si el incumplimiento es sujeto de clasificación teniendo en cuenta las siguientes categorías, se debe considerar como incidente de seguridad de la información:

a. **Fuga de información:** Se evidencia divulgación no autorizada de información de la ANM.

b. **Acceso no autorizado:**

- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso.
- Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario.
- Personal no autorizado ingresa a las instalaciones de la ANM.

c. **Ataque:**

- Se evidencia intención de afectar un recurso específico.
- Se modifica la imagen institucional en aplicaciones de la ANM.
- No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio.
- Se evidencia caso de suplantación ya sea en correo electrónico o en páginas web.

d. **Código dañino:**

- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información.

- El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso.

e. **Denegación de servicio:**

- El sistema de información no responde por alta cantidad de peticiones.
- El sistema de información se encuentra con latencia o degradación del servicio.

f. **Robo o pérdida:**

- Se presenta robo o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida.
- Se presenta robo o pérdida de elementos personales en las instalaciones de la ANM.

g. **Alarmas de sistemas de monitoreo:**

Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas.

h. **Usos inadecuados:**

- Si se ingresa texto copiado de internet en documentación oficial de la ANM, sin registrar la fuente.
- Si se publican comunicados en nombre de la Entidad sin revisión y aprobación del proceso de comunicación estratégica.

4.31.1. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Al incurrir en el incumplimiento de estas políticas se debe notificar inmediatamente a la Oficina de Tecnología e Información a través de los siguientes canales.

- E-mail: servicios.tecnologicos@anm.gov.co
- Mesa de Ayuda; extensión: 5000
- A través de la herramienta de gestión de Mesa de Ayuda reportando el incidente de seguridad, con copia al jefe de la OTI, a través de su correo electrónico.

Se deben notificar situaciones tales como: personas ajenas a la ANM en oficinas y centros de cómputo, correos maliciosos o sospechosos, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso de software ilegal, divulgación, alteración y robo de información.

4.32. GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN

La gestión del riesgo de seguridad de la información y ciberseguridad se encuentra a lineada a la metodología del Sistema Integral para la Administración y Gestión de Riesgos de la ANM y, a los lineamientos que desde la Norma ISO 31000:2018 - Sistema de Gestión de Riesgos se describen.

La matriz de riesgos definida en la metodología de riesgos de seguridad incluye el análisis de los atributos generales de Seguridad de la Información y Ciberseguridad; (confidencialidad, integridad y disponibilidad), es decir, se identifican y analizan para cada uno de los riesgos, estos pilares.

4.32.1. Gestión de riesgos para la confidencialidad

Se define como riesgos que afectan este pilar, aquellos que describen que la Información puede ser conocida o utilizada sin autorización por cualquier colaborador, persona o ente dentro o fuera de la ANM. Así mismo, la información que pueda estar expuesta para ser utilizada por personas no autorizadas.

4.32.2. Gestión de riesgos para la integridad

Se define como riesgos que afectan este pilar, los que hagan referencia a aquella información que puede ser manipulada o alterada, es decir se tendrán en cuenta aquellas situaciones o escenarios en que la información no pueda mantener la exactitud, modificaciones indebidas que afecten el orden lógico de los datos cambiando su estructura o significado.

4.32.3. Gestión de riesgos para la disponibilidad

Se define como riesgos que afectan este pilar, los que describan aquella información que no pueda ser accesible y utilizable en el momento que sea necesario o se requiera por las personas, sistemas o procesos operacionales.

4.33. SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

4.33.1. CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

La ANM, debe contemplar una estrategia de Continuidad de Negocio basada en los resultados del BIA (Bussines Impact Analisis por sus siglas en inglés) y demás documentación que se ha desarrollado, que permita contar con lineamientos para la continuidad de las operaciones de negocio, entre ésta se encuentra; (Política de Continuidad de Negocio, Manual Continuidad de Negocio, Análisis GAP y Plan de Gestión de Crisis).

Planificar e implementar la Continuidad de Negocio en la ANM, debe ser un aspecto fundamental teniendo en cuenta no sólo los recursos tecnológicos, sino también activos de información críticos de los procesos, los cuales han sido definidos y estructurados en el BIA, además:

a. Se deben realizar pruebas periódicas a los controles de continuidad de negocio y de continuidad de la seguridad de la información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

b. Los responsables de los procesos e información deben asegurar que se actualicen los planes de continuidad de negocio posterior a los cambios en la infraestructura tecnológica con respaldo de la Oficina de Tecnología e Información.

c. Contemplar un sitio alterno, donde los controles implementados en el ambiente de producción deben ser consistentes con éste.

d. Los cambios de seguridad en el ambiente de producción deben ser aplicados de la misma forma para el ambiente de contingencia.

e. El Plan de Continuidad de Negocio debe ser protegido contra accesos no autorizados, contemplando a su vez copias de respaldo y que éstas sean resguardas en un sitio externo con la protección adecuada tanto física como medioambiental.

4.33.2. REDUNDANCIAS

a. La ANM debe establecer e implementar un Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

b. La ANM debe realizar pruebas periódicas al DRP en cabeza de la oficina de tecnología e información OTI, con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

4.34. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

4.34.1. IDENTIFICACIÓN LEGISLACIÓN APLICABLE Y REQUISITOS CONTRACTUALES

La Oficina Asesora Jurídica y el Oficial de Seguridad de la Información deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la ANM y relacionados con seguridad de la información. Para ello, se pueden apoyar en los Jefes de Oficina, tales como el Grupo de Gestión de Talento Humano, Gestión Documental.

4.34.2. DERECHOS DE PROPIEDAD INTELECTUAL

a. La Oficina de Tecnología e Información debe asegurarse de que todo el software que se ejecute en la ANM esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

b. Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos portátiles suministrados para el desarrollo de sus actividades.

c. Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, basado en el Procedimiento Derechos de Propiedad Intelectual.

d. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de Ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

e. El Grupo de Contratación debe incluir cláusulas de propiedad intelectual y derechos de autor en contratos con terceros.

4.34.3. PROTECCIÓN DE REGISTROS

La ANM se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de Confidencialidad, Integridad y Disponibilidad, siguiendo las directrices del Procedimiento de Gestión de Activos.

4.34.4. PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES

La ANM, quien será responsable del tratamiento de los datos personales, tal y como éste término se define en la Ley 1581 de 2012, respeta la privacidad de cada uno de los terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de dicha información. Por lo tanto, la ANM debe implementar los controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la Ley lo permita.

4.34.5. REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS

La ANM, se regirá por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según aplique.

4.35. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

4.35.1. REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

El proceso de Evaluación, Control y Mejora debe realizar auditorías internas de revisión independiente al menos anualmente, ésta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la Entidad para gestionar la seguridad de la información, esta revisión que es responsabilidad de Control Interno de la ANM debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control.

4.35.2. REVISIÓN CUMPLIMIENTO TÉCNICO

El Jefe de la Oficina de Tecnología e Información, debe coordinar la revisión periódica (al menos anualmente) de los Sistemas de Información para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se le hará revisión.

4.36. CUMPLIMIENTO

El incumplimiento de esta política está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión.

4.37. BIBLIOGRAFÍA

La debida documentación de las Políticas de Seguridad de la Información establecidas en este manual, han sido estructuradas teniendo en cuenta las buenas prácticas de los marcos de referencia que se citan a continuación.

a. NTC ISO/IEC 27001:2013 - Norma Técnica Colombiana Sistemas de Gestión de Seguridad de la Información.
b. NTC ISO/IEC 27002:2013 - Norma Técnica Colombiana Sistemas de Gestión de Controles de Seguridad de la Información.
c. Norma ISO 22301:2019 - Sistema de Gestión de Continuidad de Negocio.
d. Norma ISO 31000:2018 - Sistema de Gestión de Riesgos

Versión	Fecha	Descripción del Cambio
1	02/dic/2020	Versión Inicial
2	26/Nov/2024	Actualización del documento Manual de Políticas de Seguridad de la Información 1. Se establecieron los roles en materia de seguridad de la información, para los interesados que deben dar cumplimiento con la presente política. 2. Se incluyeron los requisitos y lineamientos para el intercambio de información. 3. Se reforzó el cumplimiento en materia de protección de los datos personales complementándola con la política de tratamiento de datos personales de la ANM.

Elaboró	Revisó	Aprobó
Nombre: Luis Alonso Lugo Charry **Cargo**: Contratista **Fecha**: 26/Nov/2024	**Nombre:** María Catalina Pérez López **Cargo:** Jefe de Oficina **Fecha:** 03/Dic/2024 **Nombre:** Luis Alberto Colorado Aldana **Cargo:** Contratista **Fecha:** 10/Dic/2024	**Nombre**: Luis Álvaro Pardo Becerra **Cargo:** Presidente de Agencia_07 **Fecha:** 10/Dic/2024