TABLA DE CONTENIDO

1. ANTECEDENTES

Migración Colombia, determina la información como un activo de alta importancia para la Entidad que permite el desarrollo continuo de la misión y el cumplimiento de los objetivos de la misma, lo cual genera la necesidad de implementar medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En este sentido, se establecen las políticas y lineamientos que integran el Sistema de Gestión de Seguridad de la Información - SGSI, los cuales deben ser cumplidos por los grupos de valor y partes interesadas de la Entidad que presten sus servicios o tengan algún tipo de relación con la Unidad Administrativa Especial Migración Colombia en adelante Migración Colombia.

Al respecto, las normas y lineamientos adoptados por la Entidad, se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO/IEC 27001:2013 y al Modelo de Seguridad y Privacidad de la Información de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, con en el Decreto 1078 de 2015, que hace referencia a la obligación de los sujetos obligados a desarrollar capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos, generando un marco de confianza en el ejercicio de sus deberes con el estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes en concordancia con la misión y visión de la Entidad.

Así mismo la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital y como tal deben definir lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - en adelante MSPI, la guía de gestión de riesgos de seguridad de la Información, el procedimiento para la gestión de los incidentes de seguridad digital que establecer los lineamientos y estándares para la estrategia de seguridad digital. Bajo este contexto y en el entendido que la seguridad de la información para Migración Colombia es una labor prioritaria que invita a todos a velar por el cumplimiento de las políticas.

Para ello, Migración Colombia involucra la implementación de esta política en su planeación estratégica institucional.

2. OBJETIVO DE LA POLÍTICA

Establecer los lineamientos relacionados con la Seguridad y Privacidad de la Información y Seguridad Digital de la Entidad, con el fin de preservar la confidencialidad, integridad y

disponibilidad de los activos de información de Migración Colombia, en cumplimiento a las directrices, lineamientos y las medidas organizacionales, técnicas y físicas necesarias para la adecuada gestión de la seguridad y privacidad de la información; enmarcadas en la implementación del MSPI.

3. ALCANCE DE LA POLÍTICA

Aplica a todos los funcionarios, grupos de valor y partes interesadas de Migración Colombia, que por alguna razón tengan cualquier tipo de interacción con los activos de información.

4. MARCO NORMATIVO Y LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 57 de 1985. “Por la cual se ordena la publicidad de los actos y documentos oficiales”.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las Entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000, por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones**.**
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de Entidades públicas;”
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”.
- Ley 1266 de 2008, por la cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1221 DE 2008, Normas para promover y regular el Teletrabajo Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1581 de 2012, "Protección de Datos personales".
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
- Ley 1952 de 2019, Principios y normas rectoras de la ley disciplinaria.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 2573 de 2014. “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea".

- Decreto 1074 de 2015 - Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 338 de 2022. Establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 767 de 2022, Por el cual se actualiza la Política Colombiana de Gobierno Digital.
- Resolución 1053 de 2012 se creó el grupo interno de trabajo denominado Políticas y Lineamientos para el manejo de la información, dependiente de la Subdirección de Extranjería y se dictaron otras disposiciones.
- Resolución 1351 de 2018, Actualización de la Política General de la Seguridad y Privacidad de la Información de la Unidad Administrativa Especial Migración Colombia.
- Resolución 500 de 2021 Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Resolución 3671 de 2021. “Por la cual se adopta el Manual Especifico de funciones y Competencias Laborales de la planta de empleos de la Unidad Administrativa de Migración Colombia”.
- Resolución 746 de 2022 Ministerio de Tecnologías de la Información y las Comunicaciones.
- Resolución 4357 del 2023. “Por la cual se actualiza la Política de Administración de Riesgos de la Unidad Administrativa de Migración Colombia”.
- Resolución 3403 de 2024. “Por la cual se modifica parcialmente la Resolución 0415 de 2018. “Por la cual se crea el Comité Institucional de Gestión y Desempeño de la Unidad Administrativa Especial Migración Colombia y se adopta el nuevo modelo Integrado de Planeación y Gestión”.
- Resolución 2661 de 2024, “Por la cual se actualiza el manual y los elementos esenciales del Sistema Integrado de Gestión Migración Colombia y se dictan otras disposiciones”.
- Directiva 17 del 2012, de la Unidad Administrativa Especial de Migración Colombia, se establecieron las políticas de seguridad de la información.
- Directiva 54 de 2013 donde se adoptó la política del Sistema de Gestión de la Seguridad de la Información — SGSI.
- Directiva 17 de 2014 se establecieron los parámetros y definieron lineamientos de política para la seguridad de la información.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.
- CONPES 3995 de 2020. Política Nacional Confianza y Seguridad Digital.
- Norma Técnica ISO/IEC 27001 – Estándar Internacional aplicable a sistemas de gestión de la seguridad de la información.
- Norma Técnica ISO/IEC 27002 – Estándar Internacional que condensa buenas prácticas en gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la información (MSPI), adoptado por el Ministerio de Tecnologías de la información y las Comunicaciones, fundamentado en los lineamientos de

las Normas Continuidad del negocio SGCN (Norma ISO/IEC 22301:2012), y seguridad de la información SGSI (Normas ISO/IEC 27001:2013 e ISO/IEC 27002:2013).

5. DEFINICIONES Y/O SIGLAS

Activo de información: Cualquier elemento que tenga valor para la organización, tales como: información digital, impresa, Tablas de retención documental TRD, personas, hardware, software, aplicaciones o sistemas de información de la Entidad, servicios Web, intranet, redes (infraestructura), que utiliza la organización para su funcionamiento.

Acuerdos de niveles de servicio (ANS): Acuerdos que se hacen con los usuarios de los servicios en los cuales se estipula el nivel de calidad para la aceptación del servicio.

Amenaza[1]**:** Causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la Entidad.

Amenaza informática[2]**:** Evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o denegación de servicio.

Antimalware: Software anti malware está diseñado para detectar, prevenir y eliminar software malicioso de su dispositivo. Esto incluye virus, gusanos, troyanos, spyware y mucho más.

Antispam: Software que permite a los usuarios prevenir o restringir la entrega de correos electrónicos no deseados.

Antispyware: Programa que se instala en un servidor para evitar que terceras personas puedan espiar contraseñas, movimientos, datos de navegación y hasta la configuración de un equipo de cómputo.

Antivirus: Programas cuyo objetivo es detectar y eliminar virus informáticos.

Autenticación[3]**:** Mecanismo técnico que garantiza que una persona o Entidad es la correcta.

Autenticidad[4] Propiedad de que una Entidad es lo que afirma ser.

Beneficiarios: Aquellos que cumplen con los requisitos establecidos para acceder a programas y servicios del Ministerio de Relaciones Exteriores - Migración Colombia.

CAST: Centro de atención de Servicios Telemáticos - Oficina de Tecnología de la Información.

Centro de cómputo: Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamada también data center.

[1] Norma Técnica NTC ISO/IEC 27001:2016
[2] Ministerio de las Tecnologías y Comunicaciones - Guía para la Implementación de Seguridad de la Información.
[3] Norma Técnica NTC ISO/IEC 27001:2016
[4] Norma Técnica NTC ISO/IEC 27001:2016

Ciberdefensa[5]**:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberseguridad[6]**:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberamenazas: Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

Ciberespacio[7]**:** Ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

Cifrado: Transformación de datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, acceso no autorizado a los repositorios de información.

Confiabilidad[8]**:** Principio fundamental de la seguridad de la información, que permite garantizar que la información sea precisa, completa y accesible cuando se necesita.

Confidencialidad[9]**:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

Contratistas[10]: Es un colaborador o instrumento de la Entidad estatal para la realización de actividades o prestaciones que interesan a los fines públicos, pero no en un delegatario o depositario de sus funciones.

Control: sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento (procesos, políticas, dispositivos, prácticas u otras acciones).

Control informático: Las políticas, los procedimientos, las prácticas y las estructuras organizativas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Copia de Respaldo[11]**:** Backup, se refiere a la copia de información creada para proteger contra la pérdida o daño de la información original, utilizada para restaurar la información en caso de desastre o fallo del sistema.

Correo electrónico: Medio de comunicación que debe ser protegido para garantizar la confidencialidad, integridad y disponibilidad de la información transmitida.

[5] CONPES 3701 de 2011
[6] CONPES 3701 de 2011
[7] Resolución CRC 2258 de 2009
[8] Norma Técnica NTC/IEC 27000:2018
[9] Norma Técnica NTC ISO/IEC 27001:2016
[10] Concepto 193201 de 2022 Departamento Administrativo de la Función Pública
[11] Norma Técnica NTC/IEC 27000:2018

Criptografía: Práctica que consiste en proteger la información mediante el uso de algoritmos codificados y firmas.

Custodio: Persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, integridad y disponibilidad de los activos de información e implementar los controles para proteger dichos activos a su cargo.

Declaración de aplicabilidad: (SOA[12] por sus siglas en inglés, Statement of Applicability) de la norma ISO 27001, de Sistemas de Gestión de Seguridad de la Información (SGSI), es un documento que contiene la relación completa de los controles de seguridad de la información evaluables, que se indican en el anexo A de la norma ISO IEC/27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

Evento[13]**:** Ocurrencia identificada del estado de en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Firewall: Dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Firmware: Soporte lógico inalterable encargado de la comunicación entre el sistema operativo y el hardware el cual indica a un dispositivo cómo debe funcionar a un nivel muy básico.

Gestión de claves[14]**:** Controles que se realizan mediante la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información[15]**:** Proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos[16]**:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de los riesgos.

Grupos de Valor: Entiéndase como funcionarios, contratistas, visitantes y proveedores de la Entidad.

Habeas Data[17]**:** Derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos de naturaleza pública o privada.

[12] SOA: Statement of Applicability: Declaración de Aplicabilidad
[13] Norma Técnica NTC ISO/IEC 27001:2016
[14] Norma Técnica NTC ISO/IEC 27001:2016
[15] Norma Técnica NTC ISO/IEC 27001:2016
[16] Norma Técnica NTC ISO/IEC 27001:2016
[17] Ley 1581 de 2012 en Colombia

Información: todos los datos y recursos que una organización maneja, que tienen valor y necesitan ser protegidos contra acceso no autorizado, alteración, divulgación o destrucción. Como datos electrónicos: Archivos, bases de datos, correos electrónicos, entre otros. Documentos físicos: Archivos en papel, manuales, informes, etc. Activos digitales: Software, aplicaciones, sistemas, redes, etc.

Infraestructura tecnológica: Elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la Entidad, entre los cuales se encuentran: equipos de trabajo, portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.

Impacto[18]**:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información[19]**:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad[20]**:** Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos[21]**:** Lista de todos aquellos recursos (físicos, de información digital e impresa, software, documentos, servicios, personas, intangibles, infraestructura, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos - Software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Log: Archivos que registran eventos específicos dentro de un sistema.

MSPI[22]**:** Modelo de Seguridad y Privacidad de la Información.

No repudio[23]**:** Capacidad de probar la ocurrencia de un evento o acción reclamada y sus Entidades de origen. El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

Partes interesadas[24]: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

[18] Norma Técnica NTC ISO/IEC 27001:2016
[19] Norma Técnica NTC ISO/IEC 27001:2016
[20] Norma Técnica NTC ISO/IEC 27001:2016
[21] Norma Técnica NTC ISO/IEC 27001:2016
[22] Norma Técnica NTC ISO/IEC 27001:2016
[23] Norma Técnica NTC ISO/IEC 27001:2016
[24] Norma Técnica NTC ISO/IEC 27001:2016

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro[25]

Plan de tratamiento de riesgos[26]**:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Propietario: Dueño del proceso que produce la información y define la seguridad de la misma.

Redundancia: Técnica en la que se duplican datos o hardware de carácter crítico, que se requiere para asegurar la infraestructura ante posibles fallos que puedan surgir por su uso continuo.

RDP: Protocolo de escritorio remoto (RDP) es un protocolo, o estándar técnico, para usar un ordenador de escritorio a distancia.

Responsable del tratamiento[27]**:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos.

Riesgo[28]**:** El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Seguridad de la información[29]**:** Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.

Sensibilización: Proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

Sistema de Gestión de Seguridad de la Información - SGSI[30]**:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Teletrabajo[31]**:** 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.

[25] Norma Técnica NTC ISO/IEC 27001:2016
[26] Norma Técnica NTC ISO/IEC 27001:2016
[27] Ley 1581 de 2012
[28] Norma Técnica NTC ISO/IEC 27001:2016
[29] Norma Técnica NTC ISO/IEC 27001:2016
[30] Norma Técnica NTC ISO/IEC 27001:2016
[31] Ley 1221 de 2008

Terceros: Personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Trazabilidad[32]**:** 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.

TRD: Tablas de Retención Documental. Listado que contiene todas las series y subseries documentales con sus correspondientes tipos documentales, que son producidos o recibidos por las áreas y procesos de Migración Colombia donde adicionalmente se establecen aspectos como: clasificación, tiempos de conservación, disposición final, entre otros. Las TRD aplican tanto para información física como para información electrónica, las TRD se convierten en el insumo base para la identificación y caracterización de los activos de información de la Entidad.

Token: El token digital, también conocido como token de seguridad o token de autenticación, es una herramienta digital que genera una clave irremplazable de 6 dígitos de forma aleatoria.

UAEMC: Unidad Administrativa Especial Migración Colombia - Migración Colombia.

Usuarios: grupos de valor y partes interesadas de la Entidad que utilizan los servicios tecnológicos de la Entidad.

VPN: (Virtual Private Network-Red Privada Virtual). Herramienta que crea una conexión de red privada entre dispositivos a través de Internet. Utilizada para transmitir datos de forma segura y anónima a través de redes públicas.

Vulnerabilidad[33]**:** Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

WAF: (Web Application Firewall- Firewall de aplicaciones web) Es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web.

6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alta Dirección de Migración Colombia aprueba esta Política de Seguridad y Privacidad de la Información y Seguridad Digital, como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen el éxito del Sistema de Gestión de Seguridad de la Información (SGSI); la Entidad como autoridad migratoria del Estado Colombiano, se compromete a proteger los activos de información para preservar su confidencialidad, integridad, disponibilidad en la continuidad de las operaciones, la administración y/o gestión de riesgos, la creación de la cultura organizacional para la generación de conciencia sobre la importancia de la seguridad y privacidad de la información y seguridad digital, en los

[32] Norma Técnica NTC ISO/IEC 27001:2016
[33] Norma Técnica NTC ISO/IEC 27001:2016

funcionarios, grupos de valor y partes interesadas que hagan uso de los activos de información relacionada con el desarrollo de la misión y objetivos estratégicos de la Entidad.

Los controles establecidos en las políticas de seguridad y privacidad de la información y seguridad digital, descritas en el presente documento, fundamentados en la Norma Técnica Colombiana NTC ISO/IEC 27001:2013 y el Modelo de Seguridad y Privacidad de la información, son claves para ser incorporados en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información.

La Entidad se encuentra certificada mediante la Norma Técnica de Calidad ISO/IEC 9001:2015 desde el año 2017. Y en la Norma Técnica de la Calidad del Proceso Estadístico NTC PE 1000 desde el 2018, los cuales garantizan que la seguridad de la información se gestione de manera sistemática y se mejore continuamente, al igual que otros procesos, la política de seguridad, al estar alineada con la norma de calidad, ayudará a identificar, evaluar y gestionar los riesgos de seguridad de manera efectiva. Esto contribuye a minimizar las amenazas y vulnerabilidades que podrían afectar la confidencialidad, integridad y disponibilidad de la información.

PRINCIPIOS QUE SOPORTAN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Dirección General de Migración Colombia ha decidido establecer 12 principios que soportan el SGSI[34] así:

1) Migración Colombia. Definirá, implementará, operará y mejorará de forma continua un Sistema de Gestión de Seguridad de la Información - SGSI, soportado en lineamientos claros alineados a las necesidades de la Entidad y a los requerimientos regulatorios vigentes aplicables a su naturaleza.

2) Migración Colombia. Definirá los responsables y responsabilidades en materia de Seguridad y Privacidad de la Información y Seguridad Digital, que serán socializados y difundidos para conocimiento y acatamiento de los grupos de valor y partes interesadas involucradas.

3) Migración Colombia. Protegerá la información generada, procesada o resguardada por los diferentes procesos, su infraestructura tecnológica y sus activos de información, del riesgo que generan los accesos otorgados a terceros.

4) Migración Colombia. Protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Siendo fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5) Migración Colombia. Protegerá la información de las amenazas originadas por parte de funcionarios, contratistas y/o proveedores que hagan uso de esta.

6) Migración Colombia. Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

[34] SGSI: Sistema de Gestión de Seguridad de la Información.

7) Migración Colombia. Controlará la operación de sus procesos, garantizando la seguridad de los recursos tecnológicos y la infraestructura.

8) Migración Colombia. Implementará el control de acceso a los sistemas de información y recursos de red.

9) Migración Colombia. Contribuirá a que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10) Migración Colombia. Realizará una adecuada gestión de incidentes de seguridad y privacidad de la información y seguridad digital junto con las debilidades asociadas a los sistemas de información para una mejora efectiva de su modelo de seguridad.

11) Migración Colombia. Implementará mecanismos para mantener la disponibilidad de los procesos y la continuidad de la operación basada en el impacto que pueden generar los incidentes de seguridad y privacidad de la información y seguridad digital.

12) Migración Colombia. Velará por el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6.1. SANCIONES POR VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La falta de conocimiento de los presentes lineamientos no exonera al personal de Migración Colombia de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de la Oficina de Tecnología de la Información por el incumplimiento de los lineamientos aquí descritos, por lo tanto:

a. Se aplicarán medidas a que haya lugar, de acuerdo con el Código Único Disciplinario[35].

b. Se aplicarán posibles acciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.

En caso de presentarse un incidente de seguridad derivado por el incumplimiento de las políticas; todos los procesos de la Entidad deben responden en términos de calidad y oportunidad a las solicitudes de la subdirección de Control Disciplinario Interno, en virtud de sus competencias.

6.2. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Migración Colombia a continuación establece los lineamientos de seguridad y privacidad de la información y seguridad digital, clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la Entidad necesarias para abordar los diferentes activos de la información que maneja y los riesgos específicos a los que se enfrenta, lo que permite una mayor

[35] Ley 734 de 2002

claridad y enfoque en cada área y esto facilita que los grupos de valor comprendan y sigan las directrices específicas relacionadas con sus funciones.

6.2.1. ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Migración Colombia, en la implementación del Sistema de Gestión de Seguridad de la Información, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad y privacidad de la información y seguridad digital, así como el Comité Institucional de Gestión y Desempeño. Responsabilidades que rigen la estructura organizacional de seguridad y privacidad de la información y seguridad digital para cada rol.

Migración Colombia alineado al Ministerio de las Tecnologías de la Información con el fin de habilitar la Política de Gobierno Digital, establecerá las competencias que se requieran para dar cumplimiento a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, que imparte los lineamientos a las Entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua. Y de acuerdo a la "Guía de Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información[36]" de MinTIC, donde plantea que todas las Entidades deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información.

6.2.1.1. DIRECCIÓN GENERAL

- Revisar y aprobar las políticas de seguridad y privacidad de la información y seguridad digital contenidas en este documento.
- Asignar los recursos requeridos: financieros, infraestructura física y personal necesarios para la gestión de la seguridad y privacidad de la información y seguridad digital.
- Promover una cultura de seguridad y privacidad de la información y seguridad digital en todos los grupos de valor y partes interesadas de la Entidad.

6.2.1.2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

El Comité Institucional de Gestión y Desempeño como instancia orientadora de la implementación de la estrategia de Gobierno en línea, debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política de seguridad y Privacidad de la información y Seguridad Digital.

[36] Guía del Roles y y Responsabilidades del Modelo de Seguridad y Privacidad de la Información" de MinTIC de 2021

6.2.1.3. RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA ENTIDAD

La responsabilidad de la Seguridad de la información será el liderar la implementación del Modelo de seguridad y privacidad de la información en la Entidad y recae en el grupo de Políticas y lineamientos para el manejo de la información de la Subdirección de Extranjería, hasta que sea nombrado el Oficial de Seguridad de la Información mediante acto administrativo y tendrá las siguientes responsabilidades:

- Asesorar a la Entidad en el diseño, implementación y mantenimiento del MSPI para la Entidad, de conformidad con las normas y regulación vigente.
- Contribuir a la implementación de la Política de Gobierno Digital.
- Identificar la brecha entre el MSPI y la situación actual de la Entidad en su implementación.
- Realizar la estimación, planificación y cronograma de la implementación del MSPI.
- Liderar la implementación y hacer seguimiento a las tareas y cronogramas definidos.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
- De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información, seguridad digital y la gestión de riesgos, así como los controles correspondientes para su mitigación y seguimiento a su plan de tratamiento, de acuerdo con las disposiciones y metodologías en la materia.
- Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgación de la seguridad y privacidad de la información y seguridad digital para funcionarios y contratistas.
- Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información y seguridad digital.
- Definir, socializar e implementar el procedimiento de gestión de incidentes de seguridad de la información en la Entidad.
- Efectuar el acompañamiento a la dirección general, para asegurar su liderazgo y confirmar el cumplimiento en los roles y responsabilidades a los líderes de los procesos en seguridad y privacidad de la información y seguridad digital.
- Poner en conocimiento a las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información y seguridad digital de acuerdo con la normativa vigente.
- Actualizar las políticas de seguridad y privacidad de la información y seguridad digital; por lo menos una vez al año o antes, si así se requiere.
- Definir y establecer el procedimiento de contacto con las autoridades correspondiente, en caso de presentarse un incidente de seguridad de la información, así como los responsables para establecer dicho contacto.

6.2.1.4. GRUPO DE SEGURIDAD DE LA INFORMACIÓN Y CALIDAD DE LA OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

- Contribuir en la aplicación de controles de seguridad informática, para mitigar los riesgos, generando aquellos lineamientos en la implementación de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

- Gestionar los incidentes de seguridad informática y en caso de ser necesario dar aviso a las autoridades competentes, de acuerdo con las normas legales establecidas en acuerdo con el oficial de seguridad de la información de la Entidad.
- Las demás de acuerdo a las funciones establecidas en el cargo.

6.2.1.5. OFICINA ASESORA JURÍDICA

- Brindar la asesoría a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información y seguridad digital.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información y seguridad digital.
- Verificar que los contratos o convenios que por competencia deban suscribir los procesos, cuenten con las cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Representar a la Entidad en los procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información y seguridad digital.
- Apoyar y asesorar a los procesos en la elaboración del índice de información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

6.2.1.6. OFICINA DE CONTROL INTERNO

- Planear y coordinar la ejecución de las auditorías internas al Sistema de Gestión de Seguridad de la información - SGSI, con el fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y privacidad de la información y seguridad digital y regulaciones aplicables.
- Realizar seguimiento a los planes de mejoramiento, producto de las auditorías realizadas a los procesos y/o procedimientos del Sistema de Gestión de Seguridad de la Información - SGSI.
- Socializar y remitir el informe de auditoría interna al Sistema de Gestión de Seguridad de la información a la Oficina de Planeación quien procederá a enviarlo a las áreas responsables.

6.2.1.7. SUBDIRECCIÓN DE TALENTO HUMANO

- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información y seguridad digital.
- Vincular dentro del plan de formación de los funcionarios y contratistas la temática de seguridad y privacidad de la información y seguridad digital en los planes y programas de inducción y reinducción.

6.2.1.8. TODOS LOS USUARIOS

Los grupos de valor y partes interesadas que realicen labores en o para Migración Colombia y utilicen de alguna manera los activos de información de la Entidad, tienen la responsabilidad de

cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad y privacidad de la información y seguridad digital.

- Evitar hacer modificaciones a los activos de la información, sin contar con autorización previa, expresa y por escrito del propietario.
- Evitar hacer uso de los activos de la información de Migración Colombia, para fines diferentes al cumplimiento de las actividades propias de la organización.
- Actualizar anualmente o antes de ser requerido el inventario de activos de información que están bajo su responsabilidad.
- Informar cualquier incidente de seguridad y privacidad de la información y seguridad digital, que pueda presentarse de acuerdo al procedimiento de gestión de incidentes de seguridad de la información, tales como: uso indebido, fuga, alteración y/o divulgación no autorizada.
- Los grupos de valor y partes interesadas que tienen acceso a la información reservada, deben participar obligatoriamente en las capacitaciones y charlas que tengan que ver con esta información.

6.3. POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANO

En esta política se debe realizar la verificación de los antecedentes disciplinarios, judiciales, fiscales entre otros, de los candidatos, durante el proceso de selección de personal de planta o contratistas, sin importar el cargo o posición al cual se postulen.

Verificar que todo el personal que labore en la Entidad o preste servicios a la misma firme el acuerdo de confidencialidad y el documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad y privacidad de la información y seguridad digital y buen uso de los activos de información, mediante el cual se compromete a realizar un adecuado uso de estos, así mismo validará que dentro de los contratos se incluya como obligación.

6.3.1. ANTES DE ASUMIR EL EMPLEO

Asegurar que los grupos de valor y partes interesadas entiendan sus responsabilidades, y que sean aptos para los roles que están siendo considerados.

La vinculación de nuevos funcionarios se realiza siguiendo un proceso formal de selección, mediante los procedimientos de Ingreso de personal con los procedimientos ETHP.01 Ingreso de personal, ETHP.09 Retiro de personal e inducción, entrenamiento de bienvenida con el procedimiento ETHP.02 Bienvenida - Inducción y Entrenamiento y el formato de autorización de tratamiento datos personales en el proceso de vinculación ETHF.152 Autorización tratamiento datos personales proceso vinculación; acorde con la legislación vigente, el cual está orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

6.3.2. DURANTE EL EMPLEO

Fomentar en los grupos de valor y partes interesadas la no divulgación de la información confidencial de la Entidad en lugares públicos, conversaciones o situaciones que pongan en riesgo la seguridad y privacidad de la información, seguridad digital y el buen nombre de esta, por medio de la guía de nombramiento y posesión de personal y el formato de acuerdo de

confidencialidad y no divulgación, promoviendo los recursos para la ejecución de las capacitaciones, control de asistencia a eventos de seguridad y privacidad de la información y seguridad digital y la aplicación de la guía de formación de los servidores públicos de Migración Colombia, sin perjuicio en lo reglado en las normas que en materia de contratación existan.

6.3.3. CON LA TERMINACIÓN Y CAMBIO DEL EMPLEO, LICENCIAS Y VACACIONES

Migración Colombia, asegura que los funcionarios, contratistas y terceros sean desvinculados y/o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

Desde los grupos de administración de personal, selección e incorporación de la subdirección de Talento Humano y contratos de la Subdirección Administrativa y Financiera (para los contratistas o colaboradores); se precisa la importancia del perfil en el retiro definitivo de la Entidad, garantizando la integridad de la información recibida, con el fin de mantener la continuidad de la gestión institucional y conservar la memoria documental de Migración Colombia, mediante los formatos de retiro definitivo de la Entidad, formato de mecanismo de transferencia de conocimiento y el acta de entrega del cargo y el formato de encuesta de retiro de la Entidad.

6.4. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

6.4.1. RESPONSABILIDAD POR LOS ACTIVOS

La información física o digital; generada, almacenada o procesada por los funcionarios, contratistas y/o proveedores de la Entidad, utilizando los recursos dispuestos por la misma para tal fin o en el desempeño de sus funciones o servicios contratados, son activos de información de propiedad de Migración Colombia. Así mismo de la propiedad intelectual, avances tecnológicos e intelectuales desarrollados por estos.

Por lo tanto, los funcionarios y contratistas son responsables del uso adecuado y protección en su ciclo de vida, utilizados de forma ética de acuerdo a las directrices vigentes en la MEG.10 guía para la gestión de los activos de información.

Migración Colombia identificará, clasificará, valorará y controlará su inventario de activos de información, conforme a la guía MEG.10 de gestión activos de Información, para garantizar su uso, protección y recuperación ante desastres; estos deberán ser discriminados por procesos y dependencias, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio y demás atributos que considere necesarios.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los directores, subdirectores y jefes de oficina, deben actuar como propietarios de la información física y electrónica de la Entidad, para lo cual deben:

- Designar, autorizar o revocar el acceso a la información y a los recursos tecnológicos.
- Recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran de la Entidad o son trasladados del área.

- Generar un inventario de los activos de información para los procesos que lideran, acogiendo las indicaciones de la guía MEG.10 de gestión activos de información, así mismo, mantenerlo actualizado.

Normas dirigidas a: TODOS LOS USUARIOS

- Utilizar los recursos tecnológicos de la Entidad asignados a funcionarios y contratistas para realizar sus funciones, no deben ser utilizados para fines personales o ajenos a este.
- No utilizar equipos de cómputo fijos, móviles o software de propiedad personal para realizar labores propias de la Entidad.
- Hacer uso adecuado y eficiente de los recursos tecnológicos para el cumplimiento de las funciones asignadas.
- Realizar la entrega de su puesto de trabajo en el momento de desvinculación o cambio del área al jefe inmediato o a quien este delegue; haciendo entrega de los recursos tecnológicos y otros activos de información que hayan sido suministrados en el momento de su vinculación.

6.4.2. CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

Migración Colombia en la guía MEG.10 gestión de los activos de información; define los niveles adecuados para clasificar la información de acuerdo con los requisitos legales, criticidad, susceptibilidad a divulgación no autorizada; la genera para su gestión, clasificación y de esta manera los propietarios aplican los controles requeridos.

Los propietarios de los activos de información deben mantener actualizado el inventario de activos al interior de sus procesos o áreas, con una frecuencia anual o antes si así se requiere.

Normas dirigidas a: OFICIAL DE SEGURIDAD DE LA INFORMACIÓN O QUIEN HAGA SUS VECES

Consolidar y actualizar el inventario y clasificación de activos de Información y asegurar su aprobación y publicación en la intranet y el Portal Web de acuerdo a lineamientos y clasificación, dando cumplimiento a la Ley 1712 de 2014 Transparencia.

Buen uso de los activos de información

6.4.3. ESCRITORIO Y PANTALLA LIMPIA

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los grupos de valor y partes interesadas.

- Conservar el escritorio libre de información propia de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal sin autorización “escritorio” tanto físico como el escritorio virtual.
- Cerrar las aplicaciones y servicios de red y/o bloquear la pantalla de su equipo de cómputo, en los momentos en que no lo utilice o cuando deba ausentarse de su puesto de trabajo.

- Retirar los documentos clasificados de la impresora inmediatamente y dejarlos bajo llave cuando no estén bajo su custodia.
- Evitar dejar equipos tecnológicos como celulares, escáneres, cámaras digitales desatendidos.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

6.4.4. BORRADO SEGURO

El borrado seguro de un equipo de cómputo en Migración Colombia, se realiza de acuerdo a lo solicitado por el propietario del activo de información, ya sea funcionario o contratista; en las siguientes situaciones:

- Reasignar a otro funcionario y/o contratista.
- Enviar a bodega o almacén.
- Cambiar el dispositivo.
- Devolver a bodega por terminación de contrato laboral.
- Reparar por parte del proveedor.
- Regresar al proveedor por finalización del contrato de suministro.

6.4.5. USO ADECUADO DE INTERNET

Migración Colombia permite el acceso al servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información.

La Oficina de Tecnología de la información, implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos de cómputo institucionales; así mismo asigna los permisos de navegación de acuerdo a los perfiles autorizados por los propietarios de los activos de información, y controla el acceso a la información contenida en portales de almacenamiento en internet para prevenir la fuga de información.

Lineamientos dirigidos a todos los usuarios para el uso adecuado de internet de acuerdo al perfil de navegación asignado:

- Hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Restringir el acceso a portales de Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Evitar el acceso y el uso de servicios interactivos o mensajería instantánea como Hotmail, Facebook, P2P, MSN, Yahoo, Skype, FTP, HTTP, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades misionales de Migración Colombia, o que por sus funciones lo requieran.
- Evitar la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que atenten contra la propiedad intelectual, archivos ejecutables y/o herramientas que atenten contra la integridad, confidencialidad y disponibilidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e

imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe de oficina respectivo y la oficina de Tecnología de la Información, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- Verificar por parte de la oficina de Tecnología de la información, los logs o registros de navegación para investigaciones o temas legales cuando sea requerido.
- Evitar descargar, utilizar, intercambiar y/o instalar software no autorizado, información y/o productos, que de alguna forma atenten contra las leyes que protegen la propiedad intelectual en Colombia.
- Evitar descargar, usar, intercambiar y/o instalar archivos que contengan código malicioso o herramientas de hacking.

6.4.6. USO DE TOKEN Y FIRMAS DIGITALES

Cada proceso o área usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar su utilización, en caso de ausencia por parte del responsable, se tendrá un token de respaldo.

Los directores cuentan con certificados digitales para gestionar firmas en contratos y convenios entre otros.

Desde la Subdirección Administrativa y Financiera se utiliza Token[37] para las firmas digitales, SIIF Nación y temas bancarios.

6.4.7. USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

Migración Colombia, establece el uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica, el cual es autorizado por los directores y jefes de oficina de acuerdo a las labores realizadas por los funcionarios, contratistas y su necesidad de uso.

Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional. Evitar el uso de medios de almacenamiento (discos externos, USB, tarjetas micro SD, pendrive, entre otros) personales en la plataforma tecnológica de la Entidad.

6.5. POLÍTICA DE CONTROL DE ACCESO

Para la protección de los activos de información, se establecerán medidas de control de acceso a nivel de red, sistemas operativos y de información, servicios tecnológicos e infraestructura física, con el fin de mitigar los riesgos asociados al acceso a la información de personal no autorizado y de esta manera salvaguardar la confidencialidad, integridad y disponibilidad de la información descritos en el manual de gestión tecnológica y la guía de gestión de perfiles, asignación de claves de acceso y configuración de grupos.

[37] El token digital: token de seguridad o token de autenticación, es una herramienta digital que genera una clave irremplazable de 6 dígitos de forma aleatoria.

6.5.1. ACCESO A REDES Y RECURSOS DE RED

La oficina de Tecnología de la Información, como responsable de las redes de datos y los recursos de red de la Entidad, propende porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de accesos lógicos monitoreados, con capacidad de generar alertas.

Normas dirigidas a: A TODOS LOS USUARIOS

- Diligenciar el formato de solicitud de creación, actualización y/o eliminación de accesos, perfiles y recursos tecnológicos y de creación de cuentas de usuario y realizar los trámites
- Informar oportunamente a la oficina de Tecnología de la Información y al Líder de Proceso sobre cualquier inconveniente, ya sea por falta o exceso de permisos, para acceder a la información.
- Utilizar las redes y servicios de comunicaciones de Migración Colombia únicamente para el cumplimiento de las funciones asignadas a su cargo evitando usos inapropiados.

6.5.2. ACCESO AL DATACENTER Y CENTROS DE CABLEADO

Migración Colombia administra información de reserva institucional y establece controles de acceso físico y/o lógico (acceso biométrico) al Data Center, la responsabilidad del control y monitoreo de las instalaciones, es del Grupo de Seguridad Física de la Entidad.

La Oficina de Tecnología de la Información, es la encargada de administrar el acceso, cuya autorización se realiza a través del formato AGAG.09 Guía de seguridad a instalaciones, personas y administración CCTV.

Normas dirigidas a: A LA OFICINA DE TECNOLOGIA DE LA INFORMACIÓN

- Portar una identificación visible en todo momento dentro del Data Center.
- Registrar el acceso de todas las personas que accedan al Data Center, incluyendo fecha, hora, nombre y motivo del acceso.
- Acompañar las visitas al Data Center en todo momento por personal autorizado.
- Utilizar mecanismos de autenticación robustos, como contraseñas fuertes para el acceso a los sistemas y datos del Data Center.
- Monitorear el acceso a los sistemas y datos del Data Center para detectar y prevenir actividades sospechosas.

6.5.3. ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO A USUARIOS

Migración Colombia, suministrará a los funcionarios y contratistas las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, estas son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta de acuerdo a los parámetros ya establecidos, ningún usuario debe acceder a la red o a los servicios TIC de Migración Colombia, utilizando una cuenta de usuario o clave de otro usuario.

6.5.4. RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información de Migración Colombia realizan un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Normas dirigidas a: A TODOS LOS USUARIOS

- Administrar la cuenta de usuario asignada, contraseña y privilegios otorgados, con la debida responsabilidad.
- Evitar compartir la cuenta de usuario y contraseña con otros funcionarios.
- Evitar escribir la contraseña en notas adhesivas o cualquier otro medio visual, o mantenerla a la vista de otras personas.
- Cambiar periódicamente la contraseña y/o cuando el sistema lo requiera.
- Seguir los lineamientos y dar cumplimiento a lo establecido en la guía EGTG.12 de gestión de contraseñas implementada en la Entidad.

6.5.4.1. CONTRASEÑAS PARA ADMINISTRADORES O USUARIOS CON ALTOS PRIVILEGIOS

En las plataformas de tecnología se debe garantizar que el acceso a la administración se realice con la vinculación directamente de las credenciales de los usuarios del directorio activo.

- Otorgar los privilegios de acceso para la administración de recursos tecnológicos, sólo a aquellos funcionarios designados para dichas funciones.
- Establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos.
- Verificar y asegurar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a los sistemas de información en producción.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica al personal debidamente autorizado y solo para las labores asignadas.
- Establecer los controles para que los usuarios finales de los recursos tecnológicos y los servicios de red no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios, sistemas o ambientes tecnológicos.
- Generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.
- Verificar que las cuentas de los usuarios con perfil administrador con privilegios y sus correspondientes contraseñas a las consolas administrables, se dejen en sobre sellado, en un área segura y custodiada que designe la Entidad, estas deben ser modificadas de manera periódica, contar con un alto nivel de complejidad y doble factor de autenticación.

- Verificar que en los sistemas o aplicaciones las contraseñas de cuentas “predefinidas”, adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.
- Revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica.
- Evitar utilizar herramientas o software que permitan evadir los controles de seguridad de los recursos tecnológicos y servicios de red.

6.5.4.2. CONTRASEÑAS PARA ADMINISTRADORES DE SISTEMAS DE INFORMACIÓN

Migración Colombia vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen conforme a los niveles de acceso a la información.
Se registran los accesos exitosos y fallidos a los sistemas de información y tecnologías con el fin de identificar y alertar posibles amenazas de accesos y cambios no autorizados

- Establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- Asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.
- Establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información.
- Asegurar que los desarrolladores internos y externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- Controlar el acceso al código fuente de los programas, sistemas de información o software desarrollado por Migración Colombia solo a personas autorizadas y llevar el control de cambios autorizados al código fuente.
- Asegurar que los sistemas de información construidos exijan autenticación para todos los recursos y operaciones ejecutadas con el software.
- Validar que no se almacenen contraseñas, cadenas de conexión u otra información pública clasificada y pública restringida en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Establecer los controles de autenticación que eviten la visualización de contraseñas.
- Desarrollar el software siguiendo estándares de desarrollo seguro.
- Implementar en el software controles que eviten múltiples intentos de autenticación fallida.
- Implementar en el software controles que obliguen al usuario a cambiar la contraseña por defecto en el primer acceso.
- Los administradores de los sistemas de información deben cambiar la clave periódicamente y custodiarla en un sitio seguro, con acceso del jefe de la oficina de Tecnología de la Información y del coordinador del grupo de Sistemas de Información y bases de datos, estas claves no deben ser compartidas sin previa autorización.
- Velar por la asignación controlada de privilegios de acceso, modificación, revocación a los sistemas de información bajo su responsabilidad.

- Monitorear periódicamente los perfiles definidos en los sistemas de información bajo su responsabilidad y los privilegios asignados a los usuarios que acceden a ellos.
- Verificar y ratificar semestralmente todas las autorizaciones sobre sus recursos tecnológicos.
- Los usuarios deben informar oportunamente de cualquier inconveniente, ya sea por exceso o falta de permisos, para acceder a la información al responsable de la dependencia.
- Los usuarios deben usar correctamente los perfiles asignados de acuerdo con sus funciones.
- Está prohibido guardar contraseñas en lugares visibles, almacenar en navegadores, archivos o sitios no controlados.

6.6. POLÍTICA PARA USO DE CONEXIONES REMOTAS

Migración Colombia, define los requisitos para realizar las conexiones remotas a la plataforma tecnológica y desde ésta a otras; así mismo, monitorea, suministra las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Normas dirigidas a: A TODOS LOS USUARIOS

- Contar con las aprobaciones requeridas para establecer la conexión remota a los dispositivos de la plataforma tecnológica de Migración Colombia y acatar las condiciones de uso establecidas para dichas conexiones.

6.7. POLÍTICA DE TELETRABAJO

Migración Colombia, garantizará la seguridad y privacidad de la información y seguridad digital cuando se tenga acceso a los recursos tecnológicos y activos de información, implementando controles adecuados para su protección que minimicen los posibles riesgos.

La Entidad de acuerdo a lo conceptuado por la Ley 1221 de 2008 adoptó la resolución 2175 de 11 de junio del 2024, para el desarrollo de las actividades de teletrabajo. Los funcionarios y contratistas en esta modalidad cumplirán la normatividad en materia de protección de datos personales, políticas de privacidad y de seguridad de la información.

Quienes adopten la modalidad de teletrabajo deben diligenciar los formatos ETHF.154 Solicitud de incorporación a la modalidad de Teletrabajo, ETHF.155 Acuerdo de Voluntariedad, ETHF.156 Evaluación de Talento Humano-Psicosocial, EGTF.21 Verificación de Requisitos Tecnológicos, ETHF.158 Inspección Virtual de Teletrabajo y ETHF.159 Seguimiento de Teletrabajo al Grupo de Bienestar Social de la Subdirección de Talento Humano cumpliendo con la reglamentación correspondiente al uso, confidencialidad, custodia, normatividad en materia de protección de datos, políticas de seguridad y privacidad de la información al utilizar equipos, programas informáticos, plataformas y herramientas TIC, sistemas de información, repositorios virtuales y propiedad intelectual, que utilicen los servicios de internet y VPN, mientras se desarrolle el teletrabajo.

Tener en cuenta las excepciones mencionadas en la Resolución 2175 de 2024 Artículo 4. TELETRABAJABILIDAD DEL EMPLEO Y SUS FUNCIONES, numerales 4.1 Empleos que de acuerdo con sus funciones manejen información o bases de datos de carácter reservado o

confidencial, 4.2 Empleos cuyas funciones requieran presencia física permanente del/la funcionario/a público/a y 4.3 Empleos con funciones de responsabilidad de personal y de manejo de confianza.

6.7.1. ACCESO POR VPN

Migración Colombia establece normas y directrices para el acceso seguro a la red de la Entidad a través de una Red Privada Virtual (VPN) para proteger la información y los recursos de la entidad, preservando la confidencialidad, integridad y disponibilidad de los datos al acceder remotamente.

Normas dirigidas a: A LA OFICINA DE TECNOLOGIA DE LA INFORMACIÓN

- Implementar un sistema de autenticación robusta para verificar la identidad de los usuarios antes de permitir el acceso a la VPN.
- Cifrar todo el tráfico a través de la VPN con algoritmos de cifrado fuertes para proteger la confidencialidad de la información. Se recomienda utilizar, como mínimo, AES 256.
- Implementar controles de acceso basados en roles para limitar el acceso a la información y los recursos según las necesidades de cada usuario.
- Contar con software de seguridad actualizado para los dispositivos que se conecten a la VPN, incluyendo antivirus, antimalware y firewall personal.
- Mantener actualizados el software de la VPN y los sistemas operativos de los dispositivos con los últimos parches de seguridad.
- Monitorear el tráfico de la VPN para detectar y prevenir actividades sospechosas.

Normas dirigidas a: A TODOS LOS USUARIOS

- Utilizar la conexión a la VPN solo para fines laborales autorizados.
- Evitar el acceso a sitios web o servicios no relacionados con el trabajo.
- Evitar compartir las credenciales de acceso VPN con otras personas.
- Informar inmediatamente a la Oficina de Tecnología de la Información sobre cualquier incidente de seguridad o actividad sospechosa.
- Cumplir con las políticas de gestión de contraseñas de la Entidad para el acceso a la VPN.
- Acceder a la VPN únicamente desde dispositivos autorizados por la Entidad.
- Cumplir con los requisitos de seguridad establecidos para los dispositivos personales.
- Cumplir con los requerimientos de los formatos EGTF.01 IMAC y EGTF.04 Solicitud de servicio de acceso remoto VPN, EGTF.05 Solicitud de servicio de acceso remoto VPN SITE, luego se realiza la verificación de los requerimientos tecnológicos con el formato EGTF.21 Verificación de Requerimientos Tecnológicos.

6.8. POLÍTICA DE CRIPTOGRAFÍA

Migración Colombia, implementa herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información.

Migración Colombia, vela por proteger la información clasificada, mediante mecanismos de cifrado al momento de ser transferida o transmitida a terceras partes.

Las claves de acceso a los sistemas de información y sistemas operacionales se almacenan de forma cifrada para preservar su confidencialidad.

Así mismo, la oficina de Tecnología de la Información, determina los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así lo requiera.

El cifrado de los medios de almacenamiento y/o equipos de cómputo debe ser autorizado por los propietarios de los activos de información de acuerdo con las labores realizadas por los funcionarios y contratistas.

6.8.1. CONTROLES CRIPTOGRÁFICOS

Migración Colombia, vela porque la información clasificada de la Entidad sea cifrada al momento de transferirse y/o transmitirse por cualquier medio.

- Almacenar, transferir y/o transmitir la información clasificada por el dueño de la información, bajo técnicas de cifrado fuerte con el propósito de proteger su confidencialidad e integridad.
- Aplicar mecanismos de verificación de la integridad de la información con herramientas de cifrado, basadas en las buenas prácticas.
- Mantener los activos y controles sobre el ciclo de vida de las llaves criptográficas incluidas la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las mismas.
- Verificar que las llaves de cifrado sólo puedan ser utilizadas para una sola función, (firma electrónica o cifrado de datos, autenticación, etc.), nunca para varias funciones o sean reutilizadas. Como caso especial, se acepta el uso de la misma llave de cifrado para elementos que ofrecen más de un servicio criptográfico, por ejemplo: una llave de firma digital puede ser utilizada, para conservar la integridad, autenticidad y no repudio.
- Definir la vigencia durante la cual son válidas las llaves criptográficas; fechas y periodo de desactivación.
- Poner a disposición la información cifrada en forma no cifrada, previa autorización de los responsables y líderes de procesos en los casos en los que existan solicitudes de entes de control, organismos de seguridad del estado u órdenes judiciales.
- Definir las directrices y herramientas de software que se utilizarán para implementar técnicas de cifrado de información en los desarrollos de software.
- Aprovisionar y entregar los equipos de cómputo portátiles con las correspondientes medidas de seguridad de acuerdo con lo solicitado por el director y/o jefe de oficina.

6.9. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Migración Colombia adopta medidas para el control de acceso físico a las instalaciones y áreas seguras o sitios donde se gestiona la información sensible, con el fin de prevenir el acceso y mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.

- Definir las áreas seguras y los controles de acceso físicos correspondientes para la protección de la información allí resguardada.

- Velar por que todas las personas que ingresen a las instalaciones de Migración Colombia cumplan con los lineamientos establecidos para el control de acceso físico sin excepción.

6.9.1. ÁREAS SEGURAS

Migración Colombia, provee la implantación de las medidas de seguridad y vela por la efectividad de sus mecanismos de seguridad física y control de acceso, que aseguren el perímetro de las instalaciones en las sedes y regionales. Así mismo, controla las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información, 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 como: grupo de tesorería, oficina de control interno, centro de cómputo, centro de cableado, grupo de seguridad y vigilancia, grupo de archivo y correspondencia, grupo de contratos, grupo de recursos físicos, grupo de almacén, grupo de investigación de política policía judicial, bodega, entre otros.

- Autorizar y gestionar el acompañamiento permanente de visitantes a las áreas de procesamiento de información y centros de cómputo.
- Registrar el ingreso de visitantes a los centros de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Verificar los privilegios de acceso físico a los centros de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de los funcionarios autorizados.
- Proveer las condiciones físicas y medioambientales necesarias para garantizar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en los centros de cómputo, que deben ser monitoreados de manera permanente.
- Velar junto con el coordinador del grupo de inventarios y almacén, que las áreas de carga y descarga de los equipos de cómputo se encuentren aisladas de los centros de cómputo y otras áreas de procesamiento de información.
- Velar mediante monitoreo en las áreas, por la efectividad de los controles de acceso físico y equipos de vigilancia implementados.
- Autorizar los ingresos temporales a las áreas, evaluando la pertinencia del ingreso; y definir los responsables del registro y supervisión de los ingresos autorizados a las áreas con información sensible.
- Velar porque las contraseñas de los sistemas de alarma, tarjetas de proximidad, llaves y otros mecanismos de seguridad de acceso a las áreas sean utilizados por funcionarios autorizados y salvo en situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran estos sean transferidos a otros funcionarios de la Entidad.
- Gestionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implementados en las instalaciones.
- Asegurar la efectividad de los mecanismos de seguridad física y control de acceso a los centros de cómputo, centros de cableado y demás áreas de procesamiento de información o carga y despacho.
- Verificar que los centros de cableado que están bajo su custodia, se encuentren separados de las áreas que tengan líquidos inflamables o con riesgos de inundación o incendio.

- Controlar el acceso a las áreas de despacho y carga e implementar mecanismos que permitan la separación de las áreas de almacenamiento o procesamiento de la información.
- Asegurar que las labores de mantenimiento de las redes eléctricas, de voz y datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, el control de la programación de los mantenimientos preventivos.

6.9.2. SEGURIDAD A LOS EQUIPOS DE CÓMPUTO

Migración Colombia, para evitar la pérdida, robo o exposición de los recursos de la plataforma tecnológica que se encuentren dentro o fuera de las instalaciones, provee los controles que garantizan la mitigación de los riesgos sobre dicha plataforma.

- Proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos.
- Generar e implementar estándares de configuración segura para los equipos de cómputo de la Entidad.
- Establecer las condiciones que deben cumplir los equipos de cómputo de proveedores que requieran conectarse a la red de datos de Migración Colombia y verificar el cumplimiento de dichas condiciones antes de dar el acceso a los servicios de red.
- Establecer las responsabilidades para controlar la instalación del software operativo y mantener un inventario del software actualizado.

Normas dirigidas a: TODOS LOS USUARIOS

- Evitar la disposición o movimientos de los recursos tecnológicos de Migración Colombia, sin la debida autorización por la oficina de Tecnología de la Información.
- Seguir los lineamientos técnicos que proporcione la oficina de Tecnología de la Información en cuanto al manejo y disposición de los equipos de cómputo, dispositivos móviles y demás recursos tecnológicos asignados para el desempeño de sus funciones.
- Informar a la Mesa de Ayuda, en caso de presentarse una falla o problema de hardware o software al equipo de cómputo asignado u otro recurso tecnológico de propiedad de Migración Colombia, quien atenderá o escalará al interior de la oficina de Tecnología de la Información el evento, con el fin de realizar una asistencia adecuada. Evitar solucionar el inconveniente por sí mismo.
- Tener en cuenta que la instalación, reparación o retiro de cualquier componente de hardware o software de los equipos de cómputo, dispositivos móviles y demás recursos tecnológicos de Migración Colombia, solo puede ser realizado por los funcionarios de la oficina de Tecnología de la Información, o personal de terceras partes autorizado por dicha oficina.
- Bloquear su equipo de cómputo en el momento de abandonar su puesto de trabajo.
- Apagar el equipo de cómputo u otros recursos tecnológicos en horas no laborables o cuando deba ausentarse por largos periodos de su puesto de trabajo.
- Evitar que los equipos de cómputo estén desatendidos en lugares públicos o a la vista, en caso de ser transportados, bajo ninguna circunstancia.
- Tener especial cuidado al transportar los equipos de cómputo con las medidas de seguridad apropiadas, que garanticen su integridad física.

- Tener especial cuidado con los equipos portátiles, los cuales deben ser llevados como equipaje de mano y evitar exponerlos a fuertes campos electromagnéticos, calor excesivo, humedad o condiciones físicas que los puedan dañar.
- Informar de inmediato al jefe de oficina y/o supervisor de contrato, en caso de pérdida o robo de un equipo de cómputo de Migración Colombia, para que se inicie el trámite interno correspondiente.
- Asegurar que, al terminar la jornada laboral, su escritorio se encuentre libre de documentos utilizados durante el desarrollo de sus funciones y estos sean almacenados de forma segura.
- Evitar el almacenamiento de documentos con información confidencial en la pantalla del escritorio.

6.9.3. CONTROL AL SOFTWARE OPERATIVO

Migración Colombia, siguiendo las normas y estándares normativos y legales, tanto en la instalación como en la utilización de software operativo en equipos y servidores; con el fin de asegurar la continuidad operativa en los sistemas operativos, aplicaciones e infraestructura y prevenir fallas y/o ataques informáticos debido a vulnerabilidades expuestas en los sistemas informáticos.

- Establecer responsabilidades para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la Entidad.
- Asegurar que el software operativo instalado en la plataforma tecnológica de Migración Colombia cuenta con soporte de los proveedores.
- Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- Validar los riesgos que genera la migración hacia nuevas versiones de software operativo.
- Asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- Considerar los requisitos del negocio para la gestión de cambios sobre el software operativo.
- Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Entidad.
- Mantener un inventario del software implementado y actualizado, así como sus respectivas versiones y niveles de soporte por parte del proveedor.

6.10. POLÍTICA DE SEGURIDAD EN LAS OPERACIONES

Migración Colombia, planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos dados en los procedimientos establecidos para el SGSI[38]; con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio.

[38] Sistema de Gestión de Seguridad de la Información.

6.10.1. ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

Migración Colombia, asigna funciones específicas a sus funcionarios, quienes efectúan la operación y administración de dichos recursos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades.

Así mismo, vela por la eficiencia y eficacia de los controles implementados en los procesos operativos asociados a los recursos tecnológicos, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información manejada y asegura que los cambios efectuados sobre estos sean controlados y autorizados debidamente.

- Elaborar y actualizar la documentación de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de Migración Colombia.
- Poner a disposición de sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware[39], servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la Entidad de acuerdo con las funciones asignadas al usuario.
- Proveer los recursos necesarios para la implementación de los controles que permitan la separación de los ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los de producción y un acceso diferente para cada uno de estos.
- Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados con una planificación de la capacidad de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN

- Emitir los conceptos y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para herramientas colaborativas y sistemas de información de Migración Colombia.

6.10.2. GESTIÓN DE CAMBIOS

Migración Colombia, controla los cambios sobre los activos de información, infraestructura, instalaciones y sistemas de procesamiento, la cual puede afectar la confidencialidad, integridad y disponibilidad de seguridad de la información en toda la Entidad y mediante mesa técnica; quien es la encargada de revisar, valorar y gestionar los cambios a través del procedimiento de gestión de cambios que permite:

- Identificar y registrar el cambio
- Planificar y probar los cambios

[39] Soporte lógico inalterable encargado de la comunicación entre el sistema operativo y el hardware el cual indica a un dispositivo cómo debe funcionar a un nivel muy básico.

- Valorar y validar el impacto potencial de los cambios.
- Aprobar formalmente la propuesta del cambio, para aprobación ante la Mesa Técnica de Control de Cambios (CAB)
- Verificar los requisitos de seguridad del cambio y de la continuidad.
- Ejecutar el cambio y comunicarlo a las partes pertinentes o interesadas.
- Revisar la post implementación - identificación de oportunidades de mejora.
- Realizar actividades de apoyo ante cambios no exitosos o de emergencia.
- Cerrar el cambio.
- Ejecutar las pruebas técnicas y validar que el solicitante realice las pruebas funcionales de los cambios a aprobar.
- Revisar antes de la ejecución del cambio que este haya sido aprobado por el solicitante y la Mesa Técnica de Control de Cambios (CAB).
- Catalogar y ejecutar el cambio gestionando los riesgos que puedan afectar la operación.
- Participar en la aprobación de los cambios propuestos en la Mesa Técnica de Control de Cambios (CAB).
- Participar en el seguimiento de los resultados de los cambios ejecutados.

Normas dirigidas a: RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN Y LA OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

- Participar en la evaluación y análisis de impacto del riesgo del cambio.
- Participar en la aprobación de los cambios propuestos a la Mesa Técnica de Control de Cambios (CAB).
- Participar en el seguimiento de los resultados de los cambios ejecutados.

6.10.3. PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Migración Colombia, proporciona los mecanismos necesarios que garantizan la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el daño producido por software malicioso y amenazas cibernéticas. Además, proporciona los mecanismos para generar una cultura de seguridad entre los grupos de valor y partes interesadas frente a los ataques de software malicioso.

- Proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo por daño de software malicioso y respalden la seguridad y privacidad de la información y seguridad digital contenida y administrada en la plataforma tecnológica y los servicios que se ejecutan en la misma.
- Asegurar que el software de antimalware y antispam cuenten con las licencias de uso requeridas, certificando así su autenticidad para garantizar las actualizaciones y evitar que sean explotadas ciertas vulnerabilidades.
- Garantizar que la información almacenada en la plataforma tecnológica sea verificada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- Asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

Normas dirigidas a: TODOS LOS USUARIOS

- Evitar cambiar o eliminar la configuración del software de antimalware y antispam definida por la oficina de Tecnología de la Información.
- Asegurar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el daño o pérdida de la información por virus informáticos y/o la instalación de software malicioso en los recursos tecnológicos.
- Notificar a la mesa de ayuda, ante sospechas o detección de alguna infección por software malicioso, para que, a través de ella, la oficina de Tecnología de la Información tome las medidas de control correspondientes.
- Evitar abrir correos de fuentes desconocidas y publicidad engañosa.

6.10.4. COPIAS DE RESPALDO Y RESTAURACIÓN

Migración Colombia, certifica la generación de copias de respaldo y almacenamiento de la información considerando las medidas de contingencia, seguridad y necesidades de la Entidad y proporciona los recursos, procedimientos y mecanismos para la realización de estas actividades.

Así mismo, vela porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación geográfica distinta a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan las copias de respaldo cuente con los controles de seguridad física y medioambiental apropiados.

Los lineamientos de copias de respaldo se documentan e incluyen los requisitos de retención y protección.

Las copias de respaldo tienen un proceso de verificación de completitud, exactitud y restauración.

- Proveer los procedimientos para la generación, restauración, almacenamiento y tratamiento de las copias de respaldo de la información, velando por su integridad y disponibilidad.
- Disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, información y ubicación física de los mismos, para permitir un eficiente acceso a los medios que contienen la información resguardada.
- Ejecutar los procedimientos para realizar pruebas de recuperación a las copias de respaldo y así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- Definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- Definir las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

6.10.5. REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y SISTEMAS DE INFORMACIÓN

Migración Colombia, realiza el monitoreo del uso que dan los funcionarios y contratistas a los recursos de la plataforma tecnológica y los sistemas de información. Además, vela por la custodia

de los registros de auditoría cumpliendo con los períodos de retención establecidos para dichos registros.

Los logs de los eventos generados por los componentes informáticos, capturan y retienen información relevante para la revisión periódica en beneficio de identificar posibles anomalías, generar alertas tempranas que permiten reconstruir operaciones sensibles y tomar acciones en lo correspondiente a la gestión de riesgos.

Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques para evitar la adulteración de los mismos, también deben generar las capacidades suficientes para detectar y grabar eventos significativos en aspectos de seguridad de la información.

- Habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.
- Establecer los registros de auditoría en los recursos tecnológicos y los sistemas de información considerando los estándares de desarrollo seguro para registros de auditoría.

Normas dirigidas a: RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN Y LA OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

- Determinar los períodos de retención de los registros (logs) de auditoría de los recursos tecnológicos y los sistemas de información de la Entidad.

6.10.6. GESTIÓN DE LAS VULNERABILIDADES

Migración Colombia, revisa la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas de vulnerabilidades periódicamente, con el fin de gestionar los hallazgos de dichas pruebas de acuerdo con los criterios establecidos. La oficina de Tecnología de la Información gestiona las vulnerabilidades técnicas encontradas ante la mesa técnica.

- Adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético, por un ente externo, con el fin de garantizar la objetividad del desarrollo de las mismas.
- Generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.
- Revisar y hacer seguimiento a la aparición de nuevas vulnerabilidades técnicas y reportar a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de evaluar las acciones necesarias para corregir las mismas de acuerdo con los criterios de las pruebas de vulnerabilidad.

Normas dirigidas a: OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

- Evaluar los resultados de las pruebas de vulnerabilidades y hacking ético y definir acciones para la resolución de hallazgos.

Normas dirigidas a: RESPONSABLE DE LA SEGURIDAD DE LA INFORMACIÓN

Revisar las acciones ejecutadas para la resolución de vulnerabilidades técnicas.

6.10.7. AUDITORÍAS A LOS SISTEMAS DE INFORMACIÓN

Migración Colombia, controla las auditorías a los activos de información e infraestructura tecnológica, para reducir el impacto sobre las operaciones del negocio y preservar la seguridad y privacidad de la información y seguridad digital.

Estas son planificadas y acordadas con las oficinas de Tecnología de la Información y Control Interno.

El acceso a los sistemas de información y datos son acordados y controlados con el propietario del activo de información.

El alcance de las pruebas técnicas de auditoría se acuerda y controla con el propietario del activo de información.

El acceso a los activos de información que tenga perfil de escritura, se autoriza únicamente en copias aisladas y se realiza el borrado seguro una vez se ha finalizado la auditoría o en su defecto se establece el control apropiado de ser necesario, como evidencia de prueba de auditoría.

Las pruebas de auditoría que puedan afectar la disponibilidad de los activos de información en la prestación de servicios, se realizan en horas no laborales.

6.11. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

Migración Colombia, establecerá los controles para el acceso lógico y protección de las redes, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios - ANS que sean establecidos para los servicios de red.

Desde la oficina de Tecnología de la Información se definen e implementan los procedimientos y lineamientos en las instalaciones y redes públicas, para evitar accesos no autorizados en la transmisión o transferencia de la información; la cual se salvaguarda a través de controles para prevenir la pérdida de la confidencialidad, integridad y la pérdida de disponibilidad de estos.

6.11.1. GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

Migración Colombia, establece los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que viaja a través de dichas redes.

De igual manera, propende por el aseguramiento de las redes, el control del tráfico y la protección de la información clasificada de la Entidad.

- Adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Entidad.
- Implantar controles para minimizar los riesgos de seguridad y privacidad de la información y seguridad digital, transportada por medio de la red.
- Mantener segmentadas las redes de datos, por dominios, grupos de servicios y de usuarios, o cualquier otra tipificación que considere conveniente.
- Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de niveles de servicios -ANS, cuando éstos se contraten.
- Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica, siguiendo las buenas prácticas de configuración segura.
- Identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la Entidad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- Instalar la debida protección entre las redes internas y cualquier red externa, que se encuentre fuera del control y administración de la Entidad.
- Definir los parámetros técnicos requeridos para la conexión segura de los servicios de red, así como las reglas de conexión de seguridad y controles para cifrado de información que circule sobre las redes.

6.11.1.1. USO DEL CORREO ELECTRÓNICO

Migración Colombia, teniendo en cuenta la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporciona un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad, autenticidad y privacidad de quienes realizan las comunicaciones a través de este medio.

- Gestionar el acceso a las cuentas de correo electrónico mediante el procedimiento de asignación y/o retiros de acceso a los sistemas de información.
- Proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- Adoptar medidas de seguridad que permitan proteger la plataforma de correo electrónico contra código malicioso.
- Establecer mecanismos para el monitoreo de envío de información clasificada.
- Verificar el contenido de los buzones de los correos en los casos que se requiera acudir a la información para continuar con la prestación del servicio o para investigaciones específicas de acuerdo a la ley y normatividad vigente de ser requerido.

Normas dirigidas a: RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN - LA OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN - SUBDIRECCIÓN DE TALENTO HUMANO Y LA OFICINA DE COMUNICACIONES

- Generar campañas en apoyo de la oficina de Comunicaciones y la Subdirección de Talento Humano, para concientizar y dar a conocer a los funcionarios y contratistas el uso adecuado que deben adoptar en el intercambio de información clasificada por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

- Usar la cuenta de correo electrónico de manera individual e intransferible y no usar la cuenta de correo electrónico de otros usuarios.
- Usar el servicio de correo, los mensajes y la información contenida para el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Entidad. El correo institucional no debe ser utilizado para actividades personales.
- Mantener en los buzones de correo, los mensajes relacionados con el desarrollo de sus funciones, la información contenida en estos es de propiedad de Migración Colombia.
- Utilizar el correo para uso institucional, está prohibido el envío de cadenas, y/o mensajes masivos de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana, vayan en contravía de los derechos humanos y resulten ofensivos para los grupos de valor y partes interesadas de la Entidad.
- Evitar el envío de archivos que contengan extensiones ejecutables o aquellos que puedan afectar los activos de información internos o externos. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Entidad y conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Reportar correos sospechosos al grupo de Seguridad de la información y calidad de la Oficina de Tecnología de la Información.
- Asegurar la adecuada clasificación de la información que produzca, transmita o transfiera aplicando los parámetros de seguridad señalados por la Entidad.

6.11.1.2. NO REPUDIO

Migración Colombia, garantiza que los grupos de valor y partes interesadas apliquen la política de no repudio en el intercambio electrónico de la información, ni puedan negar la responsabilidad sobre la creación, modificación y envío de los mensajes.

Deberán incluir como mínimo los siguientes aspectos:

- **Trazabilidad**: Seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención**: Incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o proveedores de la Entidad.
- **Auditoría**: Incluir la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
- **Intercambio electrónico de información**: Incluir en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

Normas dirigidas a: TODOS LOS USUARIOS

- Aplicar la política de no repudio en el intercambio electrónico de información, donde no puede negar la responsabilidad sobre la creación, modificación y envío de los mensajes.

6.11.2. INTERCAMBIO DE INFORMACIÓN

Migración Colombia, asegura la protección de la información transferida o transmitida a Entidades externas y procesos internos, implementando procedimientos y controles para dicho intercambio; mediante acuerdos de confidencialidad con proveedores y partes interesadas.

La información recibida de proveedores y partes interesadas se conserva por un período de tiempo equivalente al de retención de las bases de datos con información clasificada, sobre las cuales se efectúen actualizaciones, cambios, supresiones a la información fuente, o el tiempo establecido por los requisitos legales aplicables a la Entidad.

Migración Colombia en cumplimiento de la Ley 1581 de 2012, utilizará la información personal para cumplir con las obligaciones legales y contractuales; para transferir/transmitir información de datos personales de los beneficiarios a las Entidades, terceros o partes interesadas en virtud de un convenio, programa, proyecto, ley o vínculo lícito que así lo requiera o para implementar servicios de interoperabilidad en el cumplimiento de las finalidades descritas.

- Ofrecer servicios y herramientas para el cifrado de información clasificada, evitando la divulgación o modificaciones no autorizadas.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA – GRUPO DE CONTRATOS - OFICINA ASESORA JURÍDICA

- Definen los modelos de acuerdos de confidencialidad y/o de intercambio de información desde el grupo de Contratos con la Oficina Asesora Jurídica, entre la Entidad y las partes interesadas incluyendo los compromisos y acciones por el incumplimiento de dichos acuerdos. Entre los aspectos se incluye la prohibición de divulgar la información entregada por Migración Colombia a las partes interesadas con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su finalidad.
- Establecer con las partes interesadas, los acuerdos de confidencialidad o de intercambio de información, dejando explícitas las responsabilidades y obligaciones legales asignadas por la divulgación no autorizada de la información de los beneficiarios de la Entidad que les ha sido entregada debido al cumplimiento de los objetivos misionales.

Normas dirigidas a: OFICIAL DE PROTECCIÓN DE DATOS PERSONALES - RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN

- Definir y establecer el procedimiento de intercambio de información con Entidades externas y partes interesadas que hacen parte de la misión de Migración Colombia, reciben o envían información de los beneficiarios de la Entidad, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.

- Velar porque la transmisión y transferencia de la información de Migración Colombia con Entidades externas y partes interesadas se realice en cumplimiento de las políticas de seguridad y privacidad de la información.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Resguardar la información de Migración Colombia y de sus beneficiarios; de la divulgación no autorizada por parte de proveedores y partes interesadas a quienes se entrega, verificando el cumplimiento de las cláusulas relacionadas en los contratos, acuerdos de confidencialidad o de intercambio establecidos.
- Asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregados a proveedores y partes interesadas, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga la ley o sea solicitado por entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, verifican que el intercambio de información con proveedores y partes interesadas deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Formular los requerimientos de solicitud/envío de información de Migración Colombia por proveedores y partes interesadas, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Asegurar que el intercambio de la información se realice si es autorizada y dando cumplimiento a la política de tratamiento de datos personales de la Entidad.
- Los propietarios de los activos de información deben verificar la destrucción de los mismo y/o borrado limpio; suministrados a terceros y partes interesadas y realizada por estos, una vez esta cumpla su finalidad.

Normas dirigidas a: TERCEROS O PARTES INTERESADAS

- Dar manejo adecuado a la información recibida y utilizarla en el marco de los servicios contratados sin extralimitarse, en cumplimiento de las políticas de seguridad y privacidad de la información y seguridad digital de la Entidad.
- Realizar la disposición final y segura de la información suministrada, una vez esta cumpla con la finalidad para la cual fue transmitida y/o transferida y mediante acta demostrar la realización de su destrucción y/o borrado limpio de cualquier repositorio.

Normas dirigidas a: A TODOS LOS USUARIOS

- Está restringido el intercambio de información clasificada vía telefónica.

6.11.3. ESPECÍFICAS PARA EL WEBMASTER

- Proteger la integridad de las páginas Web institucionales y la intranet, el software y la información contenida.
- Establecer los lineamientos para la publicación de la información dentro del sitio web y la intranet de Migración Colombia, así como para aquellos dominios o subdominios que se desarrollen para el cumplimiento de los objetivos misionales.
- Cumplir con los lineamientos seguros y control de calidad en el desarrollo de la página web.

- Validar que el uso de los recursos suministrados por las Entidades gubernamentales sea debidamente utilizado, bajo el esquema de tratamiento de los datos personales.
- Gestionar y brindar el soporte técnico para el uso adecuado y mantenimiento de la página web de Migración Colombia.

6.11.4. PROVEEDORES O TERCERAS PARTES

Mantener la seguridad de la información y los servicios de procesamiento a los cuales tienen acceso los proveedores, terceras partes, Entidades externas o que son procesados, comunicados o dirigidos por estas.

Establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad y privacidad de la información y seguridad digital de Migración Colombia, durante y después del contrato; las cuales deben ser divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el incumplimiento de las políticas de seguridad y privacidad de la información y seguridad digital.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por el Migración Colombia.

Se deben identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo el acceso a los servicios de tecnológicos y comunicaciones.

Identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Entidad. El resultado del análisis de riesgos será la base para el establecimiento de los controles antes de iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.

Los supervisores de contratos relacionados con los sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

Normas dirigidas a: A PROVEEDORES DE SERVICIOS DURANTE O AL FINALIZAR EL CONTRATO

- Indicar la disposición final del activo de información de forma adecuada y segura con su respectiva evidencia digital o física con la cual pueda ser auditada, generar acta donde firman las partes interesadas y evidencia fotográfica o video.
- Borrar la información con herramientas especiales que sigan estándares de seguridad específicos.

- Aplicar estándares legales y de cumplimiento, asegurando una eliminación completa de la información o activo de información en todos los repositorios.
- Implementar herramientas específicas para grandes volúmenes de información o activos de información según sea requerido.

6.11.5. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE TERCERAS PARTES

Propender por mantener los niveles acordados de la seguridad y privacidad de la información, seguridad digital y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con éstos. Así mismo, velar por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

- Verificar las condiciones de comunicación segura, cifrado y transmisión de la información desde y hacia los proveedores de servicios y partes interesadas.

Analizar mediante Mesa Técnica de Control de Cambios (CAB), los cambios en los servicios tecnológicos y por parte del supervisor de contratos notificar a los proveedores.

6.12. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Migración Colombia, monitorea que los sistemas de información que sean implementados en la Entidad cumplan con los requerimientos de seguridad y privacidad de la información, seguridad digital y las buenas prácticas durante todo el ciclo de vida.

- Todos los procesos de la Entidad que realicen desarrollos deberán cumplir con los procedimientos y metodologías de desarrollo establecidos y formalizados para poder pasar a producción.
- Todos los procesos de la Entidad deberán informar a la oficina de Tecnología de la Información sobre los proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesarios para su desarrollo e implementación.
- Los servicios asociados a transacciones electrónicas se protegen para evitar transmisión incompleta, alteración o divulgación no autorizada o enrutamiento errado.

6.12.1. DESARROLLO SEGURO, REALIZACIÓN DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

Migración Colombia, vela porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad definidos basado en las buenas prácticas para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad. Se asegura que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido.

Todo sistema de información que capture información de los usuarios o beneficiarios incorpora mecanismos de autorización de tratamiento de datos personales.

- Implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios de software.
- Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Entidad.
- Asegurar que los sistemas de información adquiridos o desarrollados por proveedores cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- Generar, adoptar o recomendar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión estable publicada por el fabricante.
- Asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes y lenguajes de programación.
- Generar monitoreo Periódico.
- Almacenar las copias de seguridad del código fuente de manera segura previendo riesgos asociados a pérdida de disponibilidad, confidencialidad o integridad de la información.
- Aplicar el procedimiento de control de cambios de software y a los sistemas de información de la Entidad cuando sea requerido.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Implementar las buenas prácticas y lineamientos en el desarrollo seguro durante todo el ciclo de vida de los sistemas de información.
- Proporcionar un nivel adecuado y oportuno de soporte para solucionar los inconvenientes que se presenten en el sistema de información desarrollado.
- Desarrollar los aplicativos para que se efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Verificar que los sistemas de información desarrollados validen la información suministrada por los usuarios antes de procesarla.
- Proteger el código fuente de los desarrollos realizados.
- Generar el soporte correspondiente en los desarrollos.

Normas dirigidas a: ANALISTA

- Verificar que los sistemas de información desarrollados validen la información suministrada por los usuarios antes de procesarla.

Normas dirigidas a: RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN

- Realizar pruebas de seguridad sobre los sistemas de información de acuerdo con los estándares de la industria.

6.12.2. PROTECCIÓN DE LOS DATOS DE PRUEBA

Migración Colombia, protege los datos de prueba que son entregados a los desarrolladores, asegurando que no revelen información clasificada de los ambientes de producción.

- Garantizar que la información a ser entregada a los desarrolladores para pruebas se enmascare y no revele información clasificada en los ambientes de producción.
- Realizar las pruebas correspondientes para asegurar que cumplen con los estándares de seguridad antes del paso a producción.
- Realizar la adecuada disposición final de la información de los ambientes de pruebas, una vez han finalizado.

6.13. POLÍTICA GESTIÓN DE INCIDENTES DE SEGURIDAD

Migración Colombia, gestiona adecuadamente los eventos e incidentes de seguridad y privacidad de la información y seguridad digital, que pueda afectar la confidencialidad, integridad o disponibilidad de los activos de información, incluyendo la comunicación interna y autoridades competentes de ser necesario.

Se tienen definidas las responsabilidades a través del procedimiento MEP.11 gestión de incidentes de seguridad, para asegurar una respuesta eficaz y oportuna.

6.13.1. REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

Migración Colombia, promueve entre los grupos de valor y partes interesadas el reporte de incidentes de seguridad y privacidad de la información y seguridad digital; en sus medios de procesamiento, almacenamiento, plataforma tecnológica, sistemas de información y personas.

De igual manera, asigna responsables para el tratamiento de los incidentes de seguridad y privacidad de la información y seguridad digital, quienes tienen la responsabilidad de aislar, investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalándolos de acuerdo con su criticidad. Los responsables con sus respectivas actividades están establecidos en el procedimiento de gestión de incidentes de seguridad de la información.

La Dirección General o su delegado, son los únicos autorizados para reportar incidentes de seguridad y privacidad de la información y seguridad digital ante las autoridades competentes; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos.

- Analizar el incidente con el fin de establecer las posibles causas del mismo, identificando el impacto y ejecutando las acciones establecidas en el procedimiento de gestión de incidentes de seguridad de la información, para contener el incidente.
- Proponer los planes de mejora e implementar medidas correctivas.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Informar al jefe inmediato, al grupo de Seguridad informática y al Oficial de Seguridad de la Información sobre los incidentes de seguridad y privacidad de la información y seguridad digital que se identifiquen o reconozcan su posibilidad de materialización.

Normas dirigidas a: RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN

- Evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar a la Mesa Técnica de Control de Cambios (CAB), aquellos en los que se considere pertinente.
- Designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su recurrencia.
- Generar campañas de concientización a todos los funcionarios y contratistas de la Entidad para que conozcan los mecanismos para el reporte de incidentes de seguridad y privacidad de la información y seguridad digital.
- Activar el Plan de Recuperación de Desastres – DRP, de acuerdo con los criterios de la guía de recuperación de desastres de la Entidad para aquellos incidentes que afecten la disponibilidad y/o integridad de información y de los servicios tecnológicos.

Normas dirigidas a: A TODOS LOS USUARIOS

- Reportar al jefe inmediato, al grupo de seguridad de la información y calidad y al oficial de seguridad de la información, por cualquiera de los medios dispuestos, cualquier evento o incidente de seguridad y privacidad de la información y seguridad digital, relacionado con la información y/o los recursos tecnológicos, para que sea registrado y se le dé el trámite necesario.
- Reportar al centro de servicios, el cual es asignado a la persona encargada de la seguridad y calidad de la información de la oficina de Tecnología de la Información y al oficial de seguridad de la información; dependiendo de su valoración informará a las instancias respectivas para los trámites correspondientes y quedarán documentados en la herramienta del centro de servicios hasta su cierre.

6.14. POLÍTICAS DE CUMPLIMIENTO

Lo establecido en el presente documento, anexos y/o posteriores actualizaciones es aplicable y de obligatorio cumplimiento para todos los grupos de valor y partes interesadas de Migración Colombia. En caso de incumplimiento a las políticas de seguridad y privacidad de la información y seguridad digital, la Entidad tomará las acciones disciplinarias y legales correspondientes.

6.14.1. CUMPLIMIENTO DE DERECHO DE PROPIEDAD INTELECTUAL Y USO DE SOFTWARE PATENTADO

Migración Colombia, propende porque el software instalado, en uso, en los recursos de la plataforma tecnológica de la Entidad, cumpla con los requerimientos legales y de licenciamiento aplicables.
En el procedimiento de inventario de software y hardware y control de software legal, se cumple con los requisitos legales vigentes relacionados con los derechos de propiedad intelectual y uso de software patentados.

- Asegurar que todo el software que se ejecuta en la Entidad cumpla con los requisitos de derechos de autor y licenciamiento de uso.
- Mantener un inventario con el software y sistemas de información que se encuentran permitidos en los equipos de cómputo, servidores o equipos móviles de la Entidad para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado corresponda únicamente al permitido. Este inventario debe contener la evidencia de la propiedad de las licencias.
- Definir los controles que garanticen la continuidad en el uso del software bajo el riesgo de desaparición del proveedor.
- Establecer la reserva de los derechos de propiedad intelectual, donde se plasme de forma expresa la reserva de todos los derechos existentes en el software de la Entidad.
- Definir e implementar mecanismos que impidan la instalación de software no autorizado por parte de los usuarios finales.
- Vigilar el software instalado por usuarios privilegiados como administradores de los equipos de cómputo y servidores.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA GRUPO DE CONTRATOS

- Incluir una cláusula donde el proveedor garantiza que tiene las patentes o derechos de propiedad sobre el bien o servicio adquirido o contratado por la Entidad.
- Desarrollar cláusulas de indemnización con el propósito de asegurar que el proveedor defienda a la Entidad en sus derechos ante reclamos sobre patentes (hardware) o derechos de autor (software). En el supuesto que se compruebe una infracción, deberá asegurarse una solución que no afecte los servicios de la Entidad y la definición de los cargos por daños y perjuicios.
- En los contratos con proveedores de desarrollo se debe aclarar los derechos de propiedad intelectual de los desarrollos enumerando: reproducción, distribución, comunicación pública y transformación sobre el resultado del desarrollo a favor de la Entidad.

Normas dirigidas a: RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN

- Emitir concepto de seguridad sobre los sistemas de información de libre distribución con la intención de ser utilizados en la Entidad, basados en las especificaciones técnicas del producto y sus debilidades reconocidas en el mercado.
- Sensibilizar a los funcionarios, temporales y contratistas en la instalación y uso de software legal para proteger los derechos de propiedad intelectual y sus acciones disciplinarias en caso de incumplir la norma.

Normas dirigidas a: A TODOS LOS USUARIOS

- Evitar la instalación de software o sistemas de información en los equipos de cómputo o equipos móviles suministrados para el desarrollo de las funciones asignadas.
- Cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software implementados en la Entidad.

6.15. POLÍTICA DE PRIVACIDAD Y DE PROTECCIÓN DE DATOS PERSONALES

Migración Colombia, en cumplimiento de la Ley 1581 de 2012 y de la normativa que la reglamenta para la protección de datos personales de sus funcionarios, contratistas, proveedores y beneficiarios de los cuales reciba y administre información.

Adopta las medidas administrativas, técnicas, legales y de procesos para resguardar la privacidad y proteger los datos durante la captura, almacenamiento y procesamiento de la información en las operaciones.

Establece la MEPI.14 Política Tratamiento Datos Personales UAEMC, respecto de la cual la Entidad tenga la calidad de responsable del tratamiento, disponible en el sitio web institucional.

Normas dirigidas a: ÁREAS QUE ADOPTAN DATOS PERSONALES

- Obtener la autorización para el tratamiento de los datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitirlos en el desarrollo de las actividades de la Entidad.
- Asegurar que solo aquellas personas que por sus funciones pueden tener acceso a dichos datos.
- Establecer condiciones contractuales y de seguridad a las partes interesadas para el tratamiento de los datos personales.
- Acoger las directrices técnicas y procedimientos establecidos para el intercambio de los datos con terceros delegados para el tratamiento de estos.
- Acoger las directrices técnicas y procedimientos establecidos para enviar información a beneficiarios, proveedores y partes interesadas, mensajes, a través de correo electrónico y/o de texto.

Normas dirigidas a: RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN

- Apoyar en la formulación de controles para el tratamiento y protección de datos personales de los funcionarios, contratistas, proveedores, beneficiarios y partes interesadas de la Entidad, de los cuales reciba y administre información.
- Implementar los controles necesarios para proteger la información personal de los funcionarios, contratistas, proveedores, beneficiarios y partes interesadas, ejecutando los controles sobre el almacenamiento de las bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin previa autorización.

Normas dirigidas a: OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

- Mantener actualizada y alineada con los requisitos legales vigentes la política de tratamiento de datos personales y sus finalidades relacionadas en la autorización de los mismos.
- Asesorar en la identificación de riesgos relacionados con la privacidad y protección de datos personales de la Entidad.
- Identificar los incidentes presentados en cuanto a la protección de datos personales y reportar a la Superintendencia de Industria y Comercio si esto amerita, de acuerdo al procedimiento establecido.
- Capacitar y sensibilizar los lineamientos de la ley de protección de datos personales al personal de Migración Colombia, y coordinar la divulgación de estos lineamientos a los proveedores y partes interesadas.
- Custodiar la base de datos de autorización de tratamiento de los datos personales.

Normas dirigidas a: A TODOS LOS USUARIOS

- Guardar la reserva con respecto a la información sensible de la Entidad o de los funcionarios, contratistas, proveedores, beneficiarios de la cual tengan conocimiento en el ejercicio de sus funciones.

Aplicar los controles de seguridad definidos por la Entidad para el suministro de información de funcionarios, contratistas, proveedores y/o beneficiarios

6.16. POLITICA DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y LUCHA CONTRA LA CORRUPCIÓN

Migración Colombia, garantiza el derecho de acceso a la información pública y lucha contra la corrupción a través de los canales habilitados por la Entidad, excluyendo sólo aquella que está sujeta a las excepciones constitucionales, legales y bajo el cumplimiento de los requisitos establecidos en la Ley 1712 de 2014, Ley de Transparencia y acceso a la información pública.

Normas dirigidas a: RESPONSABLE DE LASEGURIDAD DE LA INFORMACIÓN

- Generar los Instrumentos de Gestión y trámites para su publicación.

Normas dirigidas a: DIRECTORES, SUBDIRECTORES Y JEFES DE OFICINA

- Actualizar periódicamente la información pública bajo su responsabilidad a través de los procedimientos establecidos en la Entidad.
- Atender las solicitudes de acceso a la información pública por medio de los respectivos dueños y responsables de la información.
- Clasificar la información a publicar en la página WEB de acuerdo a la Guía MEG.10 Guía Gestión de los Activos de Información, verificando que se publique únicamente la información con categoría de "pública".

6.17. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Migración Colombia, establecerá un plan de continuidad donde se debe incluir la continuidad de la seguridad y privacidad de la información y seguridad digital y la restauración oportuna de los servicios en un escenario de contingencia.

El propósito fundamental de la continuidad del negocio en la Entidad es garantizar la prestación ininterrumpida de servicios esenciales a la ciudadanía, incluso ante situaciones de disrupción[40].

Ante la ocurrencia de un desastre natural, un ciberataque, una crisis sanitaria, la interrupción parcial o total del acceso a la información y a la tecnología de la información sin un plan de continuidad del negocio Migración Colombia podría verse imposibilitada de operar, lo que afectaría gravemente a los grupos de valor y partes interesadas.

6.17.1. POLÍTICA DE REDUNDANCIA

Migración Colombia, procura por la existencia de una plataforma tecnológica redundante; que satisfaga los requerimientos de disponibilidad para la Entidad.

Normas dirigidas a: OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

- Analizar y establecer los requerimientos de redundancia para los sistemas de información que se usan en los procesos críticos y la plataforma tecnológica de la Entidad.
- Realizar pruebas sobre las soluciones de redundancia, para asegurar el cumplimiento de los requerimientos de disponibilidad.
- Seleccionar y administrar las soluciones de redundancia tecnológica sobre los sistemas de información de acuerdo con las necesidades de la Entidad.

[40] Disrupción: Interrupción corta del servicio o proceso.

6.18. CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

6.18.1. SENSIBILIZACIÓN, SOCIALIZACIÓN Y COMUNICACIÓN

Migración Colombia, define un "Plan de sensibilización, socialización y comunicación en seguridad y privacidad de la información y seguridad digital" a través de la oficina de Comunicaciones, donde anualmente se planificará la manera en que se difundirán las respectivas recomendaciones por diferentes medios a todos sus grupos de valor y partes interesadas, con el fin de socializar las políticas institucionales en seguridad y privacidad de la información y seguridad digital y las buenas prácticas de estas, para aumentar las capacidades en todos los procesos de la Entidad.

6.18.2. CAPACITACIONES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Migración Colombia, a través del grupo de capacitaciones de la subdirección de Talento Humano, incluirá dentro de los programas de capacitación e inducción, las temáticas de seguridad y privacidad de la información y seguridad digital, con el objetivo de concientizar a los grupos de valor y partes interesadas que se vinculen a la Entidad y tengan pleno conocimiento de estas.

La finalidad de las capacitaciones en una Entidad pública es mejorar la calidad del servicio que se presta a los grupos de valor y partes interesadas y optimizar el funcionamiento de la Entidad.

Esto se logra a través del desarrollo de competencias, habilidades y conocimientos en los servidores públicos, permitiéndoles desempeñar sus funciones de manera más eficiente, ética y responsable.

6.19. REVISIÓN, APROBACIÓN, Y VIGENCIA DE LA POLITICA

Las políticas definidas en este documento se harán efectivas a partir de su aprobación por la Dirección General y serán revisadas anualmente, cuando existan incidentes de seguridad y privacidad de la información y seguridad digital y/o cuando se presenten cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicación dentro de Migración Colombia.

6.20. REGISTRO Y/O EVIDENCIA Y AUDITORÍA

El responsable de efectuar la auditoría y registro de los hallazgos evidenciados en temas relacionados con la seguridad y privacidad de la información y seguridad digital; será la oficina de Control Interno de Migración Colombia.

La auditoría se llevará a cabo de acuerdo al plan de auditorías o cuando sea requerido, debiéndose levantar un acta de los hallazgos que se evidencien, de tal manera que se administre un registro consecutivo del cumplimiento de esta obligación.

6.21. PROCESO DISCIPLINARIO

Migración Colombia, dentro de la estrategia de seguridad de la información, establece un proceso disciplinario formal para los funcionarios y contratistas que violen las políticas y procedimientos de seguridad y privacidad de la información y seguridad digital; en cumplimiento a la ley 1952 de 2019, por medio de la cual se expide el Código general disciplinario.

6.22. CUMPLIMIENTO DE LA POLITICA

Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los grupos de valor y partes interesadas de Migración Colombia.

Las políticas de seguridad y privacidad de la Información y seguridad digital deben prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales relacionadas con los controles de seguridad.

6.23. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciada en la norma ISO/IEC 27001:2013 es un documento que lista los objetivos de control y controles a implementar en la Entidad, y las justificaciones de los controles que no van a ser implementados, dando cumplimiento a la misma, controles establecidos en los 14 dominios a desarrollar de manera detallada y clara.

6.24. INSTANCIAS PARA LA EVALUACIÓN Y SEGUIMIENTO

Migración Colombia, mediante Resolución 415 de 2018 se creó el Comité Institucional de Gestión y Desempeño y mediante resolución 3403 de 2024 se modifica parcial la resolución 415., como instancia evaluadora y de seguimiento en la implementación de la política de seguridad y Privacidad de la información y Seguridad Digital.

6.25. DOCUMENTOS RELACIONADOS

Entre otros:

Formatos:

- EGTF.01 IMAC
- EGTF.04 Solicitud de servicio de acceso remoto VPN
- EGTF.05 Solicitud de servicio de acceso remoto VPN SITE
- EGTF.21 Verificación de Requisitos Tecnológicos
- MEF.25 Registro de Activos de Información
- ETHF.152 Autorización tratamiento datos personales

- ETHF.154 Solicitud de incorporación a la modalidad de Teletrabajo
- ETHF.155 Acuerdo de Voluntariedad
- ETHF.156 Evaluación de Talento Humano-Psicosocial
- ETHF.158 Inspección Virtual de Teletrabajo
- ETHF.159 Seguimiento de Teletrabajo

Guías:

- AGAG.09 Guía de seguridad a instalaciones
- EGTG.12 de gestión de contraseñas
- MEG.10 Guía Gestión de los Activos de Información
- EDG.10 Guía administración de riesgos

Procedimientos:

- MEP.11 Gestión de Incidentes de Seguridad de la Información
- MEI.06 Diligenciamiento formato Activos de Información v1
- ETHP.01 Ingreso de personal
- ETHP.02 Bienvenida - Inducción y Entrenamiento
- ETHP.09 Retiro de personal e inducción, entrenamiento de bienvenida con el procedimiento

Política:

- MEPI.14 Política Tratamiento Datos Personales UAEMC

7. PLANES, PROGRAMAS, PROYECTOS ASOCIADOS A LA OPERATIVIDAD DE LA POLÍTICA

Migración Colombia, atiende el habilitador transversal de Seguridad y Privacidad de la Información inmerso en la Política de Gobierno Digital del Modelo Integrado de Planeación y Gestión, que tiene como fin la incorporación en las Entidades de la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información que se generen en el desarrollo de la gestión institucional, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

De igual forma, atiende los lineamientos y requerimientos de la Política Nacional de Seguridad Digital, en aras de blindar a la Entidad de posibles amenazas informáticas que conlleven a la materialización de riesgos en la gestión por perdida o afectación a la información administrada por la Entidad; además, busca ampliar las capacidades y competencias institucionales y de las partes interesadas para identificar, gestionar, tratar y mitigar los riesgos en la materia.

Para ello, atiende los requerimientos del Modelo Integrado de Planeación y Gestión – MIPG en sus políticas transversales de Gobierno Digital, Seguridad Digital y Gestión Documental buscando optimizar la relación Estado Ciudadano, para generar confianza en la Entidad frente al manejo de la información que genera y recolecta mediante sus diferentes sistemas de información; al respecto, atiende los principios de seguridad de la información en todos sus procesos, herramientas tecnológicas y activos de información y prevenir la materialización de riesgos en la gestión.

En este sentido, Migración Colombia cuenta con un programa de Gestión Documental, que atiende los lineamientos en temas de gestión y preservación documental de conformidad con los parámetros y metodologías del Archivo General de la Nación.

Adicionalmente en la formulación de su Plan Estratégico Institucional contempla objetivos desarrollados a partir de estrategias encaminadas al cumplimiento de la Seguridad y Privacidad de la Información y Seguridad Digital y la bajo criterios de calidad y confiabilidad de la información. Para el cumplimiento de los objetivos y estrategias mencionados, se cuenta con los siguientes planes de acción:

- PAI – Plan de Acción Institucional
- Plan de Acción Transversal de Seguridad y Privacidad de la Información
- Plan de Acción Transversal de Seguridad Digital
- Plan de Acción de Gestión Documental
- Plan de Acción de Gestión Tecnológica
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones
- Plan de Transparencia, Acceso a la Información y Lucha contra la corrupción
- Plan de Formación y capacitación

Dichos planes contemplan actividades para el cierre de brechas de los requerimientos de seguridad y privacidad de la información y seguridad digital, con el fin de establecer acciones que generen valor y contribuyan a fortalecer los controles existentes en la materia, a través de los documentos adoptados en el Sistema Integrado de Gestión Institucional.

Por último, en aras de una adecuada ejecución de la planeación estratégica institucional, la Entidad cuenta con dos proyectos de inversión que soportan la ejecución de las estrategias planteadas para cada vigencia en materia de seguridad y privacidad de la información, los cuales se relacionan a continuación:

- Fortalecimiento de las Capacidades y Evolución de las Tecnologías de la Información en Migración Colombia a nivel nacional.
- Optimización de los procesos de gestión documental en UAEMC a nivel nacional.

8. BIBLIOGRAFIA

- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos, 2013-12-11, ICONTEC Internacional.
- Norma Técnica Colombiana NTC-ISO/IEC 27002:2013, Guía de Implementación Sistemas de Gestión de la Seguridad de la Información, 2013-12-11, ICONTEC Internacional.
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Versión 6, expedida por el Departamento Administrativo de la Función Pública (DAFP).
- Norma Técnica Columbiana NTC-ISO/IEC 27000:2016, Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, 2016-02-15, International Organization for Standardization.
- Plantilla del Manual de Políticas del Sistema de Gestión de Seguridad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones.
- Guía Roles y Responsabilidades de la Dirección de Gobierno digital - Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones Octubre del 2021.

9. CONTROL DE CAMBIOS

Versión	Fecha y número de acta y/o acto administrativo aprobación	Elaborado por:	Revisado por:	Aprobado por:
1	Directiva 17 04/06/2012	Rolando Garnica Arias Grupo Desarrollo Organizacional Nelson Enrique Hernández Barrera Coordinador de Grupo de Políticas de Lineamientos para el manejo de la información Cristian David Castro Sánchez Grupo de Políticas de Lineamientos para el manejo de la información	Antonio Hernández Llamas Subdirección Extranjería Representante de la Alta Dirección My. Yasid Alberto Montaño Granados Asesor de la Dirección Rosemberg Leguizamón Vargas Oficina Asesora de Planeación Rodrigo Amórtegui Aros Oficina Tecnología de la Información Julio Roberto Aponte Monroy Jefe (E) Oficina de Control Interno Winston Andrés Martínez Oficina Asesora Jurídica José Alfredo Guerrero Monroy Grupo de Archivo y Correspondencia María Deissy Castiblanco	Sergio Bueno Aguirre Director

			Subdirectora de Talento Humano Juan Carlos Rangel Gil Coordinador Seguridad de la Información y Calidad	
	Descripción del cambio:			
	Adopción de la Política.			
2	Directiva 54 07/06/2013	Nelson Enrique Hernández Barrera Coordinador del Grupo de Políticas y Lineamientos para el manejo de la Información Wilson Alonso Silva Silva Profesional Especializado	Yasid Alberto Montaño Granados Asesor Dirección Antonio Hernández Llamas Subdirección Extranjería Rolando Garnica Arias Oficina Asesora de Planeación (E) Rodrigo Amórtegui Aros Oficina Tecnología de la Información Winston Andrés Martínez Oficina Asesora Jurídica Leonardo Sierra Jiménez Coordinador Grupo de Seguridad de la información y Calidad	Sergio Bueno Aguirre Director
	Descripción del cambio:			
	Establecieron los parámetros y definieron lineamientos de la Política para la Seguridad de la Información			
3	Directiva 17 07/07/2014	Rolando Garnica Arias Coordinador Grupo de Desarrollo Organizacional. Nelson Enrique Hernández Barrera Coordinador del Grupo de Políticas y Lineamientos para el manejo de la Información. Cristian David Castro Sánchez Grupo de Políticas y Lineamientos para el manejo de la Información.	Antonio Hernández Llamas Subdirector de Extranjería, Representante de la Alta Dirección para SGSI. My Yasid Alberto Montaño Granados Asesor de la Dirección. Rodrigo Amórtegui Aros Jefe de la Oficina Tecnología de la Información. Winston Andrés Martínez Jefe Oficina Asesora Jurídica. Rosemberg Leguizamón Vargas Jefe Oficina Asesora de Planeación. Julio Roberto Aponte Monroy Jefe (E) Oficina de Control Interno. Maria Deissy Castiblanco Subdirectora de Talento Humano. José Alfredo Guerrero Monroy	Sergio Bueno Aguirre Director

			Grupo de Archivo y Correspondencia. Juan Carlos Rangel Gil Coordinador Seguridad Información y Calidad.	
Descripción del cambio:				
Establecer parámetros y definir los lineamientos de política para la seguridad de la información.				
4	Resolución 1351 28/05/2018	Leopoldo E. Klee Ebratt Coordinador de Grupo de Políticas de Lineamientos Subdirección de Extranjería Zulma A. Parales Profesional Especializado	Leonor Arias Barreto Subdirección Extranjería Juan Camilo González Garzón Oficina Asesora de Planeación Duberly Eduardo Murillo Barona Oficina Tecnología de la Información Guadalupe Arbeláez Izquierdo Oficina Asesora Jurídica Sandra Patricia Mesa Murcia Coordinadora Grupo Desarrollo Organizacional Jairo Alexander Casallas Machete Secretario General	Christian Kruger Sarmiento Director
	Descripción del cambio:			
	Se actualiza la Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Unidad Administrativa de Migración Colombia, y se definen los lineamientos frente al uso y manejo de la información.			
5	Resolución 4685 24/12/2024	Jhenit Jasmín López Herreño Coordinador de Políticas y Lineamientos para el manejo de la información - Subdirección de Extranjería	Néstor David Medina Herrera Subdirector de Extranjería Elsa Piedad Morales Bernal Asesora Dirección General Andrea Pérez Arismendi Secretaria General Carlos Julio Ávila Coronel Jefe Oficina Asesora Jurídica Leonardo Carvajal Hernández Jefe Oficina Asesora de Planeación Martha Hernández Arango – Subdirectora de Control Migratorio	Martha Hernández Arango Directora General (E)

		Diana Rojas Luis Oficial de Seguridad de la Información Dirección General	Camilo Eduardo Romero Velásquez - Subdirector de Verificación Sandra Milena Moreno Acevedo Subdirectora Administrativa y Financiera Rosa María Martínez González Subdirectora de Talento Humano Diego Emilio Ojeda Moncayo Jefe Oficina de Tecnología de la Información Oscar Orlando Gómez Pinto Jefe oficina de Control Interno Mónica Lucia Rocha Ardila Coordinadora Grupo de Atención y Relacionamiento con la Ciudadanía.	

Descripción del cambio:

Actualización de la Política de Seguridad código PI.12 a la MEPI.12 Política de Seguridad y Privacidad de la Información y Seguridad Digital.

En el Marco Normativo y Legal se actualizaron las leyes, normas y decretos:

- Constitución Política de Colombia 1991. Artículo 15.
- Ley 23 de 1982; Ley 57 de 1985; Ley 80 de 1993; Ley 527 de 1999; Ley 594 de 2000; Ley 962 de 2005; Ley 1032 de 2006; Ley 1150 de 2007; Ley 1266 de 2008; Ley 1221 DE 2008; Ley 1273 de 2009; Ley 1581 de 2012; Ley 1712 de 2014; Ley 1952 de 2019; Decreto 1599 de 2005.
- Decreto 2952 de 2010; Decreto 1377 de 2013; Decreto 886 de 2014; Decreto 2573 de 2014; Decreto 1074 de 2015; Decreto 1078 de 2015; Decreto 338 de 2022; Decreto 767 de 2022.
- Resolución 1053 de 2012; Resolución 2661 de 2024; Resolución 0715 de 2017; Resolución 1351 de 2018; Resolución 0415 de 2018; Resolución 500 de 2021; Resolución 3671 de 2021; Resolución 746 de 2022; Resolución 4357 del 2023; Resolución 3403 de 2024.
- Directiva 17 de 2014; Directiva 54 de 2013; Directiva 17 de 2014.
- CONPES 3701 de 2011; CONPES 3854 de 2016; CONPES 3995 de 2020.
- Norma Técnica ISO/IEC 27001; Norma Técnica ISO/IEC 27002.
- Modelo de Seguridad y Privacidad de la información (MSPI Dentro de la Política de Seguridad y Privacidad de la Información, se generaron los siguientes ítems.

- Definiciones y/o siglas.
- Actualización de la Política general de seguridad y privacidad de la información con el compromiso de la dirección general.
- Principios que soportan el sistema de gestión de seguridad de la información.
- Compromiso de la dirección general.
- Sanciones por violaciones a las políticas de seguridad de la información.
- Políticas específicas de seguridad y privacidad de la información y seguridad digital.
- Estructura organizacional de seguridad y privacidad de la información y seguridad digital
  Dirección general
  Comité institucional de gestión y desempeño
  Responsable de la seguridad de la información para la entidad - oficial de seguridad de la información
  Grupo de seguridad de la información y calidad de la oficina de tecnología de la información
  Oficina asesora jurídica
  Oficina de control interno
  Subdirección de talento humano
  Todos los usuarios

	- Políticas de seguridad de los recursos humano Antes de asumir el empleo Durante el empleo Con la terminación y cambio del empleo, licencias y vacaciones - Políticas de gestión de activos de información Responsabilidad por los activos Clasificación y manejo de la información Escritorio y pantalla limpia Borrado seguro Uso adecuado de internet Uso de token y firmas digitales Uso de periféricos y medios de almacenamiento - Política de control de acceso Acceso a redes y recursos de red Acceso al datacenter y centros de cableado Establecimiento, uso y protección de claves de acceso a usuarios Responsabilidades de acceso de los usuarios Contraseñas para administradores o usuarios con altos privilegios Contraseñas para administradores de sistemas de información - Política para uso de conexiones remotas - Política de teletrabajo Acceso por VPN - Política de criptografía Controles criptográficos - Política de seguridad física y del entorno Áreas seguras Seguridad a los equipos de cómputo Control al software operativo - Política de seguridad en las operaciones Asignación de responsabilidades operativas Gestión de cambios Protección frente a software malicioso Copias de respaldo y restauración Registro de eventos y monitoreo de los recursos tecnológicos y sistemas de información Gestión de las vulnerabilidades Auditorías a los sistemas de información - Política de seguridad de las comunicaciones Gestión y aseguramiento de las redes de datos Uso del correo electrónico No repudio Intercambio de información Específicas para el Webmaster Proveedores o terceras partes Gestión de la prestación de servicios de terceras partes - Políticas de adquisición, desarrollo y mantenimiento de sistemas de información Desarrollo seguro, realización de pruebas y soporte de los sistemas Protección de los datos de prueba - Política gestión de incidentes de seguridad Reporte y tratamiento de incidentes de seguridad - Políticas de cumplimiento Cumplimiento de derecho de propiedad intelectual y uso de software patentado - Política de privacidad y de protección de datos personales - Política de transparencia, acceso a la información pública y lucha contra la corrupción - Política de la seguridad de la información en la gestión de la continuidad del negocio - Política de redundancia

	- Capacitación, sensibilización y comunicación en seguridad y privacidad de la información y seguridad digital Sensibilización, socialización y comunicación Capacitaciones en seguridad y privacidad de la información y seguridad digital - Revisión, aprobación, y vigencia de la política - Registro y/o evidencia y auditoría - Proceso disciplinario - Cumplimiento de la política - Declaración de aplicabilidad - Instancias para la evaluación y seguimiento - Documentos relacionados - Planes, programas, proyectos asociados a la operatividad de la política - Bibliografía