INDUSTRIAS MORARBE S.A.S.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Nota: Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la página web de Industrias Morarbe S.A.S.

Tabla de contenido

1.INTRODUCCIÓN
2. OBJETIVO
3.ALCANCE
4. RESPONSABLES.
5. DEFINICIONES.
6. CONSIDERACIONES GENERALES.
7. DESARROLLO DEL DOCUMENTO.
Lineamientos generales
7.1. Seguridad para el uso de dispositivos móviles privados que accedan información de Industrias Morarbe S.A.S.
7.2. Seguridad para dispositivos móviles de propiedad de lIndustrias Morarbe S.A.S.
Lineamientos generales .
7.3. Durante la ejecución del empleo
Lineamientos generales
7.3.1. Terminación y cambio de empleo
Lineamientos generales
7.4.1. Clasificación de la Información
Lineamientos generales.
7.4.3 Manejo de medios
Lineamientos generales
7.5.2. Gestión de acceso de usuariosLineamientos generales.
7.5.3. Responsabilidades de los usuarios
Lineamientos generales
7.5.4. Control de Acceso a Sistemas y Aplicaciones
Lineamientos generales
7.6. CRIPTOGRAFÍA.
Lineamientos generales
7.7. SEGURIDAD FÍSICA Y DEL ENTORNO
7.7.2. Equipos Lineamientos generales
7.7.2.1 Política de escritorio y pantalla limpia.
Lineamientos generales .
Escritorios limpios
Bloqueo de sesión .

Aseguramiento de la información confidencial
No reciclaje de papel con información confidencial
Equipos desatendidos
7.8. SEGURIDAD DE LAS OPERACIONES
7.8.2. Protección contra Códigos Maliciosos
7.8.3. Copias de respaldo (Backups).
Lineamientos generales
Backups de información contenida en equipos de cómputo.
7.8.4. Registro y SeguimientoLineamientos generales
7.8.5. Control de software operacionalLineamientos generales
7.8.6. Gestión de Vulnerabilidad TécnicaLineamientos generales
7.9.1.1. Política de Controles en la Red de Datos y Transferencia de Información.
Lineamientos generales
Gestión de la Seguridad en las Redes.
Transferencia de Información.
7.9.1.2. Servicio de acceso a internet.
Lineamientos generales .
7.9.1.3. Seguridad en la nube.
Lineamientos generales
7.10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.
7.10.2. Seguridad en los procesos de desarrollo y soporte.
Lineamientos generales .
7.11. RELACIONES CON LOS PROVEEDORES.
Lineamientos generales:
7.11.2. Gestión de la prestación de servicios de proveedoresLineamientos generales
7.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
7.13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.
7.14. CUMPLIMIENTO
Lineamientos generales
7.14.2. Revisiones de seguridad de la informaciónLineamientos generales
7.15. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES.
Lineamientos generales .
7.15.1. Alcance de la Política de Protección de Datos Personales
7.15.2. Tratamiento de los datos personales por parte de INDUSTRIAS MORARBE S.A.S.
7.15.3. Efectos de la Autorización
7.15.4. Autorización.

7.15.5. Finalidades de la autorización
7.15.6. Información personal recolectada
7.15.7. Deberes de INDUSTRIAS MORARBE S.A.S. cuando actúe como responsable del tratamiento
7.15.8. Derechos del titular de la información personal
7.15.9. Seguridad de la información y reserva de la información personal
7.15.10. Tratamiento de datos personales de menores de edad
7.15.11. Consulta, Rectificación y reclamos
8. NORMATIVIDAD APLICABLE
9. ANEXOS.

1. INTRODUCCIÓN

Consciente que la información es uno de los activos más importantes para las organizaciones y particularmente para INDUSTRIAS MORARBE S.A.S., en cumplimiento de su misión y sus objetivos, es indispensable establecer estrategias y mecanismos que contribuyan a la protección de la seguridad de la información institucional, independientemente del personal que interactúa con ella y del medio en que se trate, transporte o almacene.

Para ello INDUSTRIAS MORARBE S.A.S, implementa el Sistema de Gestión de Seguridad de la Información – SGSI para todos los procesos de la Empresa y establece mediante el presente manual, un conjunto de políticas y lineamientos acordes a los requisitos de la norma NTC-ISO-IEC 27001 de 2013, para el uso adecuado de la información institucional y de los recursos y servicios tecnológicos que la soportan, que se constituyen en la base para el diseño y ejecución de procedimientos, protocolos, controles y en general, el desarrollo de las actividades diarias de los empleados, contratistas y personas que interactúen con la información institucional de INDUSTRIAS MORARBE S.A.S.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia.

Para el desarrollo del componente de Seguridad y Privacidad de la Información, se ha elaborado un conjunto de documentos asociados al Modelo de Seguridad y Privacidad de la Información, los cuales a lo largo de los últimos años, han sido utilizados por las diferentes entidades tanto del orden nacional como territorial, para mejorar sus estándares de seguridad de la información. El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; así mismo recoge además de los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

Las políticas del presente manual deben ser conocidas por todos los empleados), contratistas y personas que interactúen con la información institucional de la

INDUSTRIAS MORARBE S.A.S, y una vez publicado y difundido se constituirá en la base formal para dar cumplimiento a las normativas, lineamientos y políticas establecidas en relación al uso y seguridad la información, y su aplicación será de obligatorio cumplimiento, siendo responsabilidad de todos velar por el cumplimiento de estas políticas y directrices.

El incumplimiento de las políticas del presente manual puede constituir un riesgo para la disponibilidad, integridad y/o confidencialidad de la información institucional, por lo tanto, la dirección de sistemas, establecerá los mecanismos que considere necesarios, para verificar su cumplimiento.

2. OBJETIVO

Establecer las políticas y lineamientos de seguridad de la información para INDUSTRIAS MORARBE S.A.S., con el fin de contribuir al cumplimiento de los requisitos de seguridad que ayudarán mediante su implementación y cumplimiento, a preservar la confidencialidad, integridad y disponibilidad de la información de INDUSTRIAS MORARBE S.A.S

3. ALCANCE

3.1. ALCANCE / APLICABILIDAD

Las políticas contenidas en el presente manual son de obligatorio cumplimiento para todos los directivos, empleados, contratistas y terceros de INDUSTRIAS MORARBE S.A.S, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Las políticas aplican para todas las sedes de INDUSTRIAS MORARBE S.A.S., locales y puntos de atención con que cuente la Empresa.

3.2. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a las políticas establecidas en el presente manual.

4. RESPONSABLES

4.1. RESPONSABLES DE LOS PROCESOS Y /O DIRECTORES O JEFES DE DEPENDENCIAS

Informar a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC las novedades de los empleados y contratistas, así como los permisos de las carpetas o recursos compartidos para los cuales están autorizados. Así mismo, deben conocer, promover y asegurar la implementación y cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo dentro de sus dependencias.

4.2. DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Liderar las actividades relacionadas con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información –SGSI en l INDUSTRIAS MORARBE S.A.S, garantizando la divulgación y el seguimiento de las políticas de seguridad de la información al interior de la Empresa, estableciendo los procedimientos, lineamientos y controles que permitan su operatividad y cumplimiento.

4.3. DIRECCIÓN ADMINISTRATIVA Y FINANCIERA

Responsable del inventario de equipos y su actualización según se establezca en las normas vigentes y de proporcionar los suministros que permitan la operación adecuada de los sistemas de información de la Empresa por medio de los procesos contractuales necesarios tanto para la ampliación de la red como su mantenimiento. Informar a la Dirección de Tecnologías de la Información y las Comunicaciones, las novedades de ingreso y retiro de los contratistas que en el desarrollo de sus actividades requieran acceso a información y sistemas de la entidad, de acuerdo al procedimiento establecido.

4.4. DIRECCIÓN DE TALENTO HUMANO

Informar a la Dirección de Tecnologías de la Información y las Comunicaciones toda novedad de personal mediante el procedimiento establecido.

4.5. EMPLEADOS Y CONTRATISTAS

Conocer y aplicar las políticas, procedimientos de seguridad de la información vigentes y proteger el buen manejo de la información física y digital so pena de incurrir en faltas disciplinarias y/o contractuales.

Reportar oportunamente las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento y resguardar el acceso a los recursos informáticos asignados, mediante la utilización de contraseñas seguras; para tal fin debe concluirlas sesiones activas al finalizar las tareas, y/o dejar los equipos bloqueados al retirarse del puesto de trabajo así sea temporalmente.

Asumir la responsabilidad por el manejo del espacio en disco en su equipo de trabajo, realizando revisiones periódicas y eliminación de archivos no necesarios.

5. DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elementos relacionados con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización.

Activo de información: Cualquier elemento que tenga valor para la empresa tales como: software, hardware personas y servicios, que almacenan, manipulan, modifican, ingresan, o transportan información, y que, en caso de verse afectada en su confidencialidad, integridad y/o disponibilidad, afectan a INDUSTRIAS MORARBE S.A.S., en menor o mayor medida.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los(las) ciudadanos(as), o como fuentes de la historia.

También se puede entender cómo la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura.

Archivo Central: Unidad administrativa que coordina y controla el funcionamiento de los archivos de gestión y reúne los documentos transferidos por los mismos, una vez finalizado su trámite y cuando su consulta es constante.

Archivo de gestión: Archivo de la oficina productora que reúne su documentación en trámite, sometida a continua utilización y consulta administrativa. Los documentos que conforman los archivos de gestión reposan en las dependencias mientras se adelantan los trámites, actuaciones o procedimientos que los originan, y una vez cerrados, durante el tiempo que indiquen las Tablas de Retención Documental.

Archivo histórico: Archivo al cual se transfiere del archivo central o del archivo de gestión, la documentación que, por decisión del correspondiente Comité de Archivo, debe conservarse permanentemente, dado el valor que adquiere para la investigación, la ciencia y la cultura. Este tipo de archivo también puede conservar documentos históricos recibidos por donación, depósito voluntario, adquisición o expropiación.

Acuerdo de Nivel de Servicio (ANS): Es un convenio entre un proveedor de servicios de TI y un usuario. Describe las características del servicio de TI, los niveles de cumplimiento y especifica las responsabilidades del proveedor y del usuario.

Aplicaciones o aplicativos: Las aplicaciones son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

Autenticación: Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales.

Autorización: Consentimiento expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Base de datos: Todo conjunto organizado de datos Personales que sea objeto de Tratamiento.

Clave de autenticación o Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Cloud Computing: Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través "la Nube" de Internet, de una forma sencilla y cómoda.

Clúster: Conjunto de servidores que trabajan como una única maquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.

Contenido: Todo tipo de información o dato que se divulga en la intranet y/o página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños y animaciones.

Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Copyright: Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.

CPD: Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

CRM: "Customer Retationship Management". Gestión de la Relación con el Cliente,son herramientas informáticas dedicadas a la gestión integrada de información sobre clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (en adelante "Datos Personales" o "Información Personal").

Datos sensibles: Se entiende como datos sensibles aquellos que afecten la intimidad del titular o cuyo uso indebido pueda afectar la intimidad del titular o la potencialidad de generar su discriminación.

Datos públicos: Aquellos datos que no sean semiprivados, privados o sensibles. Son considerados datos públicos, entre otros, los datos relativos al estado civil de la personas, a su profesión u oficio y a su calidad de comerciante o servidor público.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.

Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dirección IP: La dirección IP (IP es un acrónimo para Internet Protocol) es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red. Es la parte principal de una direcciónen la Web, que usualmente indica la organización o compañía que administra dicha página (www.morarbe.com.co).

DVR: (Digital Video Recorder), grabador de cámaras análogas, digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que porsí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

Información personal: Es aquella suministrada por el usuario o el visitante para elregistro o consulta de información, la cual incluye datos como nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Internet: Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP.

Intranet: Es una red de ordenadores privados que utiliza tecnología Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.

Log: Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste.

Medios de almacenamiento físico: Se considera como medio de almacenamiento físico las cintas, los disco extraíbles, los CD y los DVD entre otros.

MFA o Multifactor Autenticator: Es el doble factor de autenticación a un aplicativo o sistema para validar la identidad de un funcionario público.

NVR: (Network Video Recorder), grabador de cámaras IP, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red.

Nombres de Grupos: Seudónimos utilizados para la clasificación de conjuntos de computadoras dentro del dominio.

Portal intranet: Es un sitio compuesto por varias páginas web, el cual, permite a los(as) funcionarios(as), empleados(as) y contratistas de la empresa el fácil acceso a diferentes recursos y servicios en línea que tiene la Empresa.

Portal web: Sitio web que permite a los grupos de interés consultar puntos de atención, canales, acceder a servicios y demás información relacionada con el quehacer institucional, se encuentra en la dirección URL: http://www.morarbe.com.co.

Publicar: Es la acción de hacer visible un contenido o documento desde un portal o sitio web.

Responsable del tratamiento: 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.

Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Servicio al ciudadano: Es la asistencia, orientación o intervención que actualmente suministra INDUSTRIAS MORARBE S.A.S., en línea o que proveerá en el futuro, por medio de su portal, como publicación de información, registro, certificados, asistencia, noticias, entre otros.

Servicio de TI: Un servicio de tecnologías de la información es un conjunto de productos (Bienes o servicios) que buscan solucionar las necesidades de los clientes de una organización a través del uso de elementos tecnológicos o informáticos.

Servidor: Computadora central en un sistema de red que provee servicios a otras computadoras.

Sistema Informático o de Información: Se entenderá todo sistema utilizado paragenerar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transmisión de datos: tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, cuando tenga por objeto la realización de un tratamiento por el encargado o por cuenta del responsable.

Transferencia de datos: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, incluyendo, pero sin limitar, la recolección, almacenamiento, uso, circulación o supresión.

Usuario: Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona. Se autentica e ingresa a los sistemas y sus servicios mediante un nombre de usuario (cuenta) y una contraseña de autenticación.

VPN: Red privada virtual, por sus siglas en inglés (Virtual Private Network), es un tipo de tecnología de red utilizada para interconectar de forma segura un computador o dispositivo de red a una red local o privada a través de una red pública como internet.

6. CONSIDERACIONES GENERALES

La Dirección de Tecnologías de la Información y las Comunicaciones DTIC de INDUSTRIAS MORARBE S.A.S., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información - SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y las personas, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la empresa.

Por lo anterior, este Manual de Políticas aplica a toda la empresa según lo establecido en el alcance, sus funcionarios(as), empleados(as) contratistas y terceros de INDUSTRIAS MORARBE S.A.S., teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema de Gestión de Seguridad de la Información - SGSI estarán determinados por las siguientes premisas:

➢ Identificar e implementar mecanismos para lograr el cumplimiento de la normatividad en materia de seguridad de la información.
➢ Desarrollar las actividades necesarias para lograr la continuidad y disponibilidad delos sistemas de información de INDUSTRIAS MORARBE S.A.S..
➢ Fortalecer la cultura de seguridad de la información en los(as) funcionarios(as), empleados, terceros(as), contratistas de INDUSTRIAS MORARBE S.A.S. y las personas, a través de la capacitación y sensibilización en el SGSI.

➢ Realizar una adecuada gestión de riesgos de seguridad de la información Implementando controles que contribuyan a mitigar su probabilidad de materialización.
➢ Implementar mecanismos que fomenten la transparencia en el acceso a la información, mediante procesos de clasificación y control de acceso a la información.
➢ Fortalecer y mantener los niveles de confianza de las personas en los procedimientos y servicios que presta INDUSTRIAS MORARBE S.A.S.
➢ Gestionar de manera adecuada los incidentes de seguridad de la información, generando, documentando y aplicando lecciones aprendidas con el fin de reducir la posibilidad de ocurrencia y/o el impacto de incidentes futuros.
➢ Mejorar continuamente el desempeño del SGSI, mediante la implementación de acciones correctivas y de mejora que se generen como resultado de las auditorías internas y externas y las revisiones de seguridad de la información.
➢INDUSTRIAS MORARBE S.A.S., ha decidido implementa un Sistema de Gestión de Seguridad de la Información - SGSI, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos legales vigentes.

6.1. COMUNICACIÓN Y SOCIALIZACION DE LAS POLÍTICAS

Todo(a) funcionario(a), empleado (a) o contratista que ingrese a INDUSTRIAS MORARBE S.A.S., deberá recibir capacitación sobre las políticas establecidas en el presente manual en el momento de su inducción.

La Dirección de Talento Humano remitirá con la debida anticipación a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, la información de fecha, hora y lugar de las jornadas de inducción.

6.2. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

El incumplimiento de las políticas establecidas en el presente manual podrá acarrear sanciones disciplinarias, civiles o penales según sea el caso.

6.3. REVISIÓN DE LAS POLÍTICAS

El Manual de Políticas de Seguridad de la Información es revisado anualmente o antes de ser necesario, con el fin de mantenerlo actualizado y acorde a los cambios en la infraestructura tecnológica, los procedimientos y servicios que involucran el manejo de la información institucional.

7. DESARROLLO DEL DOCUMENTO

7.1. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

INDUSTRIAS MORARBE S.A.S., en ejercicio de sus funciones constitucionales, es consciente y reconoce la importancia de preservar la seguridad de la información, la cual se define como el conjunto de medidas adoptadas por una organización, que permiten resguardar y proteger la información para garantizar la confidencialidad, disponibilidad e integridad de la misma, y que constituye factor fundamental para el cumplimiento de su Misión, Visión y Objetivos Estratégicos.

Por tal razón, la Gerencia de INDUSTRIAS MORARBE S.A.S., se compromete en todos sus niveles institucionales con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información y con el cumplimiento de los requisitos aplicables en la materia, adoptando las buenas prácticas de gestión y administración de las tecnologías de la información; de esta manera generará un marco de confianza en el desarrollo de sus obligaciones con el Estado y las personas, junto con el cumplimiento de los requisitos legales y contractuales que le aplican.

INDUSTRIAS MORARBE S.A.S., define los objetivos de seguridad de la información, los cuales se encuentran alineados con los objetivos estratégicos de la empresa, se apoya en la identificación periódica de las amenazas y vulnerabilidades que signifiquen un riesgo para los principios de la seguridad de la información y en el análisis, valoración y tratamiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

La presente política aplicará para todos(as) los(as) empleados(as), funcionarios(as), contratistas, proveedores y demás partes interesadas, así como los activos que se encuentran incluidos en el alcance del SGSI.

Todas las personas naturales y jurídicas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento de la política.

La presente política es comunicada y socializada al interior de INDUSTRIAS MORARBE S.A.S., y las partes interesadas a través de los canales de comunicación de la empresa; está disponible para su consulta cumpliendo con los parámetros de documentación

establecidos en el Modelo Integrado de Gestión - MIPG y el Sistemade Gestión de Calidad – SGC, y su incumplimiento, traerá consigo, las consecuencias legales que apliquen a la normativa de la empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

7.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.2.1. Organización interna Lineamientos generales

➢ INDUSTRIAS MORARBE S.A.S. establece el responsable del Sistema de Gestión de Seguridad de la Información – SGSI.
➢ Los responsables de los procesos y/o supervisores del contrato definirán los roles de usuario que estimen pertinentes en cada uno de sus equipos de trabajo y los niveles de operación siguiendo lo establecido en el procedimiento "Gestión de usuarios".
➢Los roles asociados a cada servicio o sistema de información serán identificados y clasificados por su tipo y uso teniendo como base los siguientes criterios:

- Tipo
- Rol
- Criterios Internos

- Grupo Core IT

Aquellos usuarios que por su función tecnológica y de investigación, gestión y apoyo tienen acceso ilimitado a los servicios y que requieren operar en aspectos técnicos y tecnológicos, instalación, configuración, decisión, administración de servicios y atención al usuario final en procesos, capacitación y procedimientos de sistemas.

- Grupo VIP

Directivos, asesores, coordinadores, jefes de área, oficina de comunicaciones, funcionarios(as), empleados(as) y contratistas que por su gestión requieren el acceso especial o privilegiado a recursos tecnológicos y servicios especiales.

- Funcionario(a)y contratista Activo(a)

Todos aquellos usuarios que requieren acceso a la red de datos y comunicaciones, aplicaciones y servicios de TI en general, de acuerdo con las funciones propias del cargo y los niveles de servicio

- Asociados
- Externos
- Ciudadanos

Personas o terceros con acceso a los servicios de TI, mediante el uso herramientas tecnológicas y/o sistemas de información diseñados especialmente para satisfacer los requerimientos ciudadanos, proveer servicios en pro del cumplimiento de las funciones propias de la Empresa.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, identificará las autoridades competentes a quienes podrá contactar en caso de presentarse algún incidente de seguridad de la información que amerite su intervención; de igual manera establecerá contacto con grupos de interés especializados en seguridad de la información, que puedan contribuir a la gestión de la seguridad de la información en INDUSTRIAS MORARBE S.A.S.

➢ Para los proyectos desarrollados por INDUSTRIAS MORARBE S.A.S., se deben tener en cuenta las políticas del presente manual, y en todo caso considerar los asuntos relacionados con la seguridad de la información mediante la identificación y tratamiento de riesgos asociados a la información de los proyectos.

➢ La planeación estratégica de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, estará alineada con la planeación estratégica institucional y acorde con los objetivos estratégicos y la asignación de recursos. Para ello, se trabaja articuladamente con los demás procesos y de acuerdo a la normatividad legal vigente.

➢ Para el desarrollo de proyectos que requieran el uso de componentes tecnológicos, los procesos contarán con el apoyo de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

➢Todos los requerimientos de equipos informáticos, sistemas de información y aplicativos o servicios de software, serán solicitados a la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, quien realizará el análisis pertinente para determinar su viabilidad técnica.

7.2.2. Dispositivos móviles y teletrabajo

7.2.2.1.Política de dispositivos móviles

La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, establece las condiciones necesarias para el acceso a los recursos de red y activos de información de INDUSTRIAS MORARBE S.A.S. a través de los dispositivos de tecnología móviles (computadores portátiles, smartphones, tabletas, o cualquier tipo de dispositivos electrónicos con capacidad de acceso a las redes). La autorización de conexión de dispositivos móviles a las redes de datos de la Empresa se realiza una vez se identifican, gestionan y mitigan los riesgos de seguridad de la información asociados al uso de los dispositivos.

Lineamientos generales

➢ El líder de Seguridad de la Información debe definir y dar seguimiento al cumplimiento de la Política de dispositivos móviles de INDUSTRIAS MORARBE S.A.S.
➢ Los dispositivos móviles de INDUSTRIAS MORARBE S.A.S., son una herramienta de trabajo y deben ser utilizados exclusivamente para las comunicaciones de los(as) funcionarios(as), empleados(as) y/o contratistas, en desarrollo de las funciones laborales o de las obligaciones contractuales correspondientes.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, está autorizada para realizar la desactivación, eliminación y/o retiro de los permisos de acceso de las aplicaciones y/o cuentas de INDUSTRIAS MORARBE S.A.S., cuando el dispositivo móvil haya sido extraviado, hurtado o se presente algún evento que comprometa la seguridad de la información institucional y empresarial.
➢ El acceso a todos los dispositivos móviles con acceso a información institucional y empresarial debe estar configurado con contraseña segura y bloqueo automático, y tener configurada la aplicación para el borrado remoto de la información.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, adopta e implementa los mecanismos de seguridad necesarios para salvaguardar la información contenida y transmitida mediante el uso de dispositivos móviles de los(as) funcionarios(as), empleados(as) contratistas y terceros de INDUSTRIAS MORARBE S.A.S., a través de los cuales se les autoriza el acceso a los recursos tecnológicos de la Empresa.

➢ En cualquier momento el líder de Seguridad de la Información de INDUSTRIAS MORARBE S.A.S. podrá hacer revisión del cumplimiento de la presente política directamente en los dispositivos móviles.
➢ El personal encargado de realizar las auditorías internas o externas que se realicen al Sistema de Gestión de Seguridad de la Información – SGSI de INDUSTRIAS MORARBE S.A.S., podrá realizar la verificación de las configuraciones de seguridad de los equipos móviles y su cumplimiento con los lineamientos de esta política.

Seguridad para el uso de dispositivos móviles privados que accedan información de INDUSTRIAS MORARBE S.A.S.
➢ El acceso a la información de INDUSTRIAS MORARBE S.A.S. a través de dispositivos móviles de propiedad de los(as) funcionarios(as), empleados(as), contratistas y/o terceros, se autorizará previa solicitud de los líderes de los procesos a través del servicio de mesa de ayuda y posterior visto bueno del líder de seguridad de la Información.
➢ No está permitido transferir ni almacenar la información clasificada, reservada o sensible de INDUSTRIAS MORARBE S.A.S., en los dispositivos móviles privados, ni en sitios o redes públicas como café internet, servicios de nube gratuitos, correos electrónicos personales, WhatsApp, OneDrive, Google Drive, Dropbox, ni cualquier otro medio NO autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones de INDUSTRIAS MORARBE S.A.S.
➢ Se debe hacer uso de las herramientas y medios suministrados por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC de INDUSTRIAS MORARBE S.A.S. para almacenar, transmitir, procesar y en general para tratar la información a que tenga acceso mediante el uso de dispositivos móviles personales.
➢ En el momento de cesar la vinculación laboral o relación contractual que dio lugar a la autorización para el uso de dispositivos móviles privados para acceder a la información de INDUSTRIAS MORARBE S.A.S., se deben eliminar los accesos a aplicaciones de la empresa en los que se almacene o transmita la información institucional, como por ejemplo correo electrónico institucional, OneDrive de Office 365, Microsoft Teams, SharePoint, etc.
➢ En caso de cambio, pérdida o hurto de un dispositivo móvil personal con acceso a la información de INDUSTRIAS MORARBE S.A.S., el (la) funcionario(a), empleado(a) contratista o tercero a quien se le haya autorizado el uso del dispositivo, será responsable de informar con carácter urgente a su jefe inmediato en INDUSTRIAS MORARBE S.A.S., y a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC a través de los canales de comunicación autorizados.

Seguridad para dispositivos móviles de propiedad de INDUSTRIAS MORARBE S.A.S.

➢ Está prohibido almacenar información personal en los dispositivos móviles asignados por INDUSTRIAS MORARBE S.A.S.
➢ Está prohibido cambiar en los equipos de propiedad de INDUSTRIAS MORARBE S.A.S., la configuración de seguridad o realizar instalación de aplicaciones, o software no autorizadas por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC; únicamente está autorizado la instalación de actualizaciones del software instalado.
➢ Los(as) funcionarios(as), empleados(as) o contratistas que tengan asignados dispositivos móviles de INDUSTRIAS MORARBE S.A.S. no deben conectarse en estos dispositivos a través de redes inalámbricas públicas.
➢ El sistema de mensajería instantánea autorizado para uso en los dispositivos móviles de propiedad de INDUSTRIAS MORARBE S.A.S. es Microsoft TEAMS, la cual debe ser instalada y configurada por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC.
➢ Los(as) funcionarios(as), empleados(as) y contratistas deben proteger física y lógicamente los dispositivos móviles asignados y que son de propiedad de INDUSTRIAS MORARBE S.A.S., para prevenir el hurto y/o acceso o divulgación no autorizada de la información institucional.
➢ En caso de pérdida o hurto de un dispositivo móvil de propiedad de INDUSTRIAS MORARBE S.A.S., el(la) funcionario(a), empleado(a) contratista o tercero a quien se le haya asignado el dispositivo, será el responsable de informar con carácter urgente a su jefe inmediato en INDUSTRIAS MORARBE S.A.S., y a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC a través de los canales de comunicación autorizados.

7.2.2.2.Política de Teletrabajo

INDUSTRIAS MORARBE S.A.S., implementó la modalidad de teletrabajo para que un número determinado de funcionarios(as), empleados(as) y contratistas tengan la posibilidad de desarrollar sus actividades y funciones laborales mediante el uso de las tecnologías de la información y las comunicaciones – TIC, de manera remota y sin requerirse la presencia física en sitio específico de trabajo.

En razón de lo anterior, INDUSTRIAS MORARBE S.A.S.. en el marco del Sistema de Gestión de Seguridad de la Información – SGSI, de la norma ISO/IEC 27001 de 2013, establece la política de teletrabajo mediante la cual se dictan lineamientos de obligatorio cumplimiento para el personal de la Empresa que ejerza sus labores diarias mediante la modalidad de teletrabajo, con el fin de contribuir al cumplimiento de los objetivos del SGSI, a través del cuidado y manejo responsable de la información institucional.

Lineamientos generales

➢ El(La) funcionario(a), empleado(a) debe mantener la seguridad física del área de teletrabajo manteniendo en lugar seguro la información institucional, y velar por que esta se encuentre protegida contra el acceso no autorizado y los incidentes que puedan afectar su disponibilidad, integridad y confidencialidad.
➢ Los(as) funcionarios(as), empleado(a) y contratistas serán responsables de mantener las copias de respaldo necesarias y alojarlas en el servicio de nube institucional para garantizar la restauración de la información institucional en caso de pérdida o daño.
➢ En el momento en que el (la) empleado(a) se levante del puesto de trabajo se debe bloquear la sesión en el equipo de cómputo y asegurarse que los documentos físicos estén protegidos contra daños y acceso no autorizado.
➢ Al terminar la jornada de trabajo, se debe asegurar que las cesiones y accesos a los aplicativos y sistemas de información queden debidamente finalizadas y cerrados, y los documentos físicos deben quedar guardados en un lugar seguro y protegidos de daños y /o accesos no autorizados.
➢ No está permitido guardar en los navegadores de internet, los usuarios y contraseñas de acceso, ni configurar la apertura automática de los sistemas de información y aplicativos de INDUSTRIAS MORARBE S.A.S.
➢ No está permitido almacenar la información confidencial, clasificada, reservada o sensible de la cual tenga conocimiento en ejercicio de las actividades de teletrabajo, en los equipos de cómputo, dispositivos móviles, medios de almacenamiento extraíbles, servicios de almacenamiento en la nube y en general cualquier medio de almacenamiento de información digital de propiedad de los tele trabajadores, dicha información debe permanecer almacenada en los repositorios de OneDrive de Office 365 institucional o cualquier medio de almacenamiento de propiedad y suministrado por INDUSTRIAS MORARBE S.A.S.
➢ No está permitido transmitir la información confidencial, clasificada, reservada o sensible en el ejercicio de las actividades de teletrabajo, por medios diferentes al

servicio de correo electrónico institucional de Office 365 suministrado por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC de INDUSTRIAS MORARBE S.A.S.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, suministrará las herramientas tecnológicas necesarias para garantizar la comunicación y transferencia segura de la información institucional, que los(as) funcionario(as) realicen mediante la modalidad de teletrabajo.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones, DTIC realizará la configuración de accesos, permisos, restricciones de seguridad y demás acciones que considere necesarias para garantizar la seguridad y protección de los activos de información de INDUSTRIAS MORARBE S.A.S.

➢ La conectividad hacia INDUSTRIAS MORARBE S.A.S. debe hacerse desde un sistema de acceso remoto seguro, privado y licenciado a nombre de INDUSTRIAS MORARBE S.A.S. el cual debe ser proveído por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC. No está permitido realizar esta conexión desde plataformas gratuitas como TeamViewer, AnyDesk, etc., ni desde sitios públicos de internet o redes de internet públicas.

➢ La estación de trabajo del teletrabajador debe contar con el software de protección contra virus y código malicioso actualizado.

➢Los(as) funcionarios(as), empleados(as) y/o contratistas deben informar oportunamente a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC de INDUSTRIAS MORARBE S.A.S. cuando se realice cambio del equipo de cómputo en el cual realiza las actividades de teletrabajo, con el fin de que esta realice la verificación de los requisitos de seguridad mínimos en el nuevo equipo de cómputo.

7.2.2.3. Política de Trabajo en Casa

Atendiendo lo dispuesto por el gobierno nacional y la Ley 2088 del 12 de mayo de 2021 "Por el cual se regula el trabajo en casa y se dictan otras disposiciones", y demás disposiciones del gobierno nacional, implementadas con el fin de garantizar la prestación de los servicios en el marco de la emergencia sanitaria generada por la pandemia del Coronavirus COVID – 19, INDUSTRIAS MORARBE S.A.S., adoptó mecanismos para el cumplimiento de las funciones y obligaciones contractuales de sus funcionarios(as), empleados(as) y/o contratistas mediante la modalidad de trabajo en casa, lo cual permite que la empresa continúe con la operación normal de sus actividades haciendo uso de las tecnologías de la información y las comunicaciones, situación que actualmente se mantiene para algunos cargos. Habilitación al servidor

público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones".

Sumado a esto, y según lo establecido por el Ministerio del Trabajo en la circular No. 21 de 2020, "(...) el trabajo en casa, como situación ocasional, temporal y excepcional, no presenta los requerimientos necesarios para el teletrabajo, y se constituye como una alternativa viable y enmarcada en el ordenamiento legal, para el desarrollo de las actividades laborales en el marco de la actual emergencia sanitaria".

De igual manera, y en el marco del Sistema de Gestión de Seguridad y Privacidad de la Información SGSI y en cumplimiento de las obligaciones establecidas en el Acuerdo No. 755 de 2019 artículo 23, numerales 6, 7 y 8, la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, debe implementar medidas y controles para fortalecer y contribuir con la preservación de la disponibilidad, confidencialidad e integridad de la información institucional.

Por lo tanto, y teniendo en cuenta que para la prestación de servicios mediante la modalidad de trabajo en casa, se requiere que los funcionarios(as), empleados(as) y/o contratistas hagan uso de herramientas y servicios tecnológicos de su propiedad como computadores, internet, dispositivos de almacenamiento, etc, se requiere establecer controles, medidas y lineamientos que mitiguen losriesgos de seguridad a los que se expone la información de INDUSTRIAS MORARBE S.A.S., y contribuyan a mantener la confidencialidad, integridad y disponibilidad de los datos.

En razón de lo anterior, INDUSTRIAS MORARBE S.A.S. en el marco del Sistema de Gestión de Seguridad de la Información – SGSI, de la norma ISO/IEC 27001 de 2013, y las medidas implementadas por el gobierno nacional, para atender la contingencia generada por el COVID-19 a partir del uso de las tecnologías y las comunicaciones, establece la política de seguridad de la información para el trabajo en casa, mediante la cual se dictan lineamientos de obligatorio cumplimiento para los(las) funcionarios(as), empleados(as) y/o contratistas de la empresa que desarrollen sus funciones u obligaciones contractuales mediante la modalidad de trabajo en casa.

Lineamientos generales

➢ La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, suministrará las herramientas tecnológicas de carácter institucional (VPN y herramientas de colaboración) para garantizar la comunicación y transferencia segura de la información institucional mediante la modalidad de trabajo en casa.
➢ INDUSTRIAS MORARBE S.A.S., no se hará responsable de suministrar ni mantener el servicio de internet, equipos de cómputo de propiedad del (de la) funcionario(a), empleado(a) o contratista, ni herramientas o servicios tecnológicos personales, utilizados para el desarrollo de sus actividades mediante la modalidad de trabajo en casa.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones, DTIC realizará la configuración de accesos, permisos, controles de seguridad y demás acciones que considere necesarias para garantizar la seguridad de los activos de información de INDUSTRIAS MORARBE S.A.S..
➢ La Dirección de Tecnologías de la Información y las Comunicaciones, brindará la capacitación que los (las) funcionarios(as), empleados(as) y/o contratistas de la empresa requieran, para garantizar el acceso y uso adecuado de las tecnologías de la información y las comunicaciones, necesarias para el desarrollo de sus actividades mediante la modalidad de trabajo en casa.
➢ Los (Las) funcionarios (as),empleados(as) y/o contratistas deben cumplir los lineamientos y políticas de seguridad establecidas por la empresa, acatando los controles técnicos implementados por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, para garantizar la seguridad de la información institucional durante las actividades de trabajo en casa incluido:
✓ Disponer de los recursos necesarios para conectarse a la empresa de forma segura, tales como computador con sistema operativo y antivirus actualizados y conexión a internet.
✓ Cuando los recursos tecnológicos sean de propiedad de INDUSTRIAS MORARBE S.A.S., deberán ser configurados por la Dirección DTIC, con todos los requisitos mínimos de seguridad (Software licenciado y actualizado, antivirus con protección de administración y control de cuentas usuario, entre otras) y las demás que se requieran para el desarrollo de sus funciones u obligaciones contractuales; de igual forma el funcionario deberá firmar el formato "compromiso de confidencialidad y no divulgación de la información para empleados y contratistas de prestación de servicios".

✓ Mantener la seguridad física del área de trabajo en casa almacenando en lugar seguro la información institucional (Física o digital), y velar por que esta se encuentre protegida contra el acceso no autorizado y los riesgos que puedan afectar su disponibilidad, integridad y confidencialidad.

✓ Procurar utilizar los servicios de almacenamiento en la nube institucional (Onedrive de office 365), y realizar periódicamente copias de respaldo de la información de trabajo contenida en los equipos de cómputo y dispositivos de almacenamiento, utilizados durante la jornada de trabajo en casa.

✓ Reportar inmediatamente a través de la mesa de ayuda en la intranet, cualquier evento, incidente o comportamiento sospechoso que pueda afectar la disponibilidad, integridad o confidencialidad de la información institucional.

✓ En el momento en que se levante del lugar de trabajo, se debe bloquear la sesión en el equipo de cómputo y asegurarse que los documentos físicos estén protegidos contra daños y/o acceso no autorizado.

✓ Al terminar la jornada de trabajo en casa, asegurarse que la sesión de trabajo en el equipo de cómputo y los accesos a los aplicativos y sistemas de información queden debidamente finalizados y cerrados, y los documentos físicos queden guardados en lugar seguro y protegidos de daños y/o accesos no autorizados.

✓ No guardar en los navegadores de internet, las credenciales de acceso (Usuarios y contraseñas) de los sistemas de información y aplicativos de INDUSTRIAS MORARBE S.A.S. ✓ Las contraseñas de acceso a los sistemas de información de INDUSTRIAS MORARBE S.A.S., son personales e intransferibles y en ninguna circunstancia deben ser reveladas a otras personas; en caso de que llegasen a ser reveladas deberá realizarse el cambio de contraseña de inmediato.

✓ No almacenar en los equipos de cómputo personales, dispositivos móviles, medios de almacenamiento extraíbles, servicios de almacenamiento en la nube y en general cualquier medio de almacenamiento de información digital personal, la información clasificada, reservada o con datos sensibles, generada, transformada o de la cual tenga conocimiento en ejercicio de las actividades de trabajo en casa; dicha información debe permanecer almacenada en los repositorios de OneDrive de Office 365 institucional o cualquier medio de almacenamiento suministrado por INDUSTRIAS MORARBE S.A.S.

✓ No transmitir la información digital de INDUSTRIAS MORARBE S.A.S., clasificada, reservada o sensible, por medios diferentes a las herramientas tecnológicas suministradas por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC de INDUSTRIAS MORARBE S.A.S.

✓ Destruir totalmente la información institucional contenida en papel o cualquier otro medio físico que vaya a ser eliminada, garantizando que esta no pueda ser leída ni reconstruida por personas no autorizadas.

La conectividad hacia la red de INDUSTRIAS MORARBE S.A.S. debe hacerse mediante una herramienta de acceso seguro, privado y licenciado a nombre de INDUSTRIAS MORARBE S.A.S. el cual debe ser proveído por la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC. No está permitido realizar esta conexión desde plataformas gratuitas como TeamViewer, AnyDesk, etc, ni desde sitios públicos de internet o redes de internet públicas.

Utilizar exclusivamente la herramienta Microsoft TEAMS, para las reuniones, videoconferencias, charlas y demás actividades virtuales organizadas con fines institucionales por los procesos, dependencias y/o colaboradores de INDUSTRIAS MORARBE S.A.S. No se permite el uso de herramientas que no estén autorizadas por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

7.3. SEGURIDAD DE LOS RECURSOS HUMANOS

7.3.1. Antes de asumir el empleo

Lineamientos generales

➢ La Dirección de Talento Humano de INDUSTRIAS MORARBE S.A.S., realizará las actividades necesarias para la selección de personal, asegurando la verificación de los requisitos mínimos para proveer los cargos y el cumplimiento de la normatividad vigente.

➢Para el ingreso de nuevo personal de planta y la suscripción de contratos o convenios relacionados con servicios de tecnología y/o acceso a información institucional, se debe garantizar que la persona acepte y firme una cláusula en la cual se informe sobre las políticas de seguridad de la información y acuerde mantener la confidencialidad de la información, con la suscripción de un acuerdo o compromiso de confidencialidad; este acuerdo se hará extensivo a todos los colaboradores de los contratistas o terceros para el caso de contratos o convenios.

7.3.2. Durante la ejecución del empleo

Lineamientos generales

➢ La Dirección de Talento Humano es la responsable de Informar a la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, toda novedad de personal mediante el procedimiento establecido.
➢ La Dirección Administrativa y Financiera, será la responsable de Informar a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, las novedades de los Contratistas, mediante el procedimiento establecido.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, será responsable de la divulgación y el seguimiento de las políticas de seguridad de la información al interior de la empresa, estableciendo los procedimientos que permitan su operatividad y cumplimiento.
➢ Los (las) Funcionarios(as), Empleados(as) y Contratistas de INDUSTRIAS MORARBE S.A.S., deben conocer y aplicar los procedimientos de seguridad de la información vigentes so pena de incurrir en faltas disciplinarias y/o contractuales; de igual manera deben reportar oportunamente las debilidades e incidentes de seguridad de la información que detecten o que sean de su conocimiento y resguardar el acceso a los recursos informáticos asignados.
➢ Los responsables de los procesos y jefes de dependencias deben Informar a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, de los permisos a las carpetas o recursos compartidos de los (las) funcionarios(as), empleados(as) y/o contratistas para los cuales están autorizados(as); así mismo, deben conocer y asegurar el cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo.
➢Los(as) funcionarios(as) y/o contratistas de INDUSTRIAS MORARBE S.A.S., deben recibir inducción en donde se forme y sensibilice sobre las políticas de seguridad de la información y las obligaciones frente al Sistema de Gestión de Seguridad de la Información - SGSI; de igual manera, la empresa deberá mantener informado al personal sobre los cambios y actualizaciones realizadas a las políticas, procedimientos y demás documentos que hacen parte del SGSI.
➢ La inducción relacionada con el uso de las herramientas tecnológicas será impartida por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, previa información de hora y lugar por la Dirección de Talento Humano o el área encargada de la logística del evento.

- El representante legal de INDUSTRIAS MORARBE S.A.S., y demás miembros del nivel directivo de INDUSTRIAS MORARBE S.A.S., serán responsables de conocer y asegurar la implementación y cumplimiento de las políticas de seguridad de la información al interior de sus dependencias, equipos de trabajo y personal a cargo.

7.3.3. Terminación y cambio de empleo

Lineamientos generales

➢ Los responsables de los procesos o dependencias de INDUSTRIAS MORARBE S.A.S., y supervisores de contratistas, serán responsables de la custodia de la información institucional a cargo de funcionarios(as) y/o contratistas cuando se produzca su retiro definitivo o parcial.
➢ La Dirección de Talento Humano es la responsable de Informar a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, sobre las novedades de personal, de acuerdo con el procedimiento establecido.
➢ La Dirección Administrativa y Financiera, será la responsable de Informar a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, sobre las novedades de los Contratistas, de acuerdo al procedimiento establecido.

- Se debe mantener la confidencialidad de la información clasificada, reservada o sensible, de INDUSTRIAS MORARBE S.A.S. aun después de que la persona haya finalizado la vinculación laboral o contractual con INDUSTRIAS MORARBE S.A.S., o haya sido trasladado de dependencia.

7.4. GESTIÓN DE ACTIVOS

7.4.1. Responsabilidad por los activos

Lineamientos generales

➢ Los activos de información de INDUSTRIAS MORARBE S.A.S., tendrán un responsable o custodio y serán identificados, clasificados y valorados de acuerdo con la normatividad legal vigente.
➢ Todo(a) funcionario(a), empleado(a) contratista o tercero que haga uso de los recursos y sistemas de información de INDUSTRIAS MORARBE S.A.S., tendrá acceso

únicamente a la información necesaria para el desempeño de sus funciones, obligaciones contractuales o actividades autorizadas.

➢ Todo(a) funcionario(a), empleado(a) o contratista deberá devolver los activos informáticos a su cargo, por motivo de retiro definitivo, cambio de puesto de trabajo, suspensión y/o finalización del contrato, haciendo entrega formal del (de los) equipo(s) a su cargo y claves de acceso necesarias.

➢Todos(as) los(as) funcionarios(as), empleados(as) y contratistas de INDUSTRIAS MORARBE S.A.S., deben reportar sin demoras injustificadas a los responsables de sus dependencias o procesos, y a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de los activos de información de la empresa.

7.4.2 Clasificación de la Información

Lineamientos generales

➢ La información resultante de los procesos misionales y de apoyo de la Empresa se tratará conforme a los lineamientos y parámetros establecidos en el Manual de Gestión Documental.

➢Los activos de información institucional deben ser identificados, clasificados y valorados de acuerdo con los procedimientos, protocolos, guías, manuales y demás medios formalmente establecidos por la empresa y acordes con la normatividad legal vigente.

7.4.3 Manejo de medios

Lineamientos generales

➢ Se deben implementar acciones, protocolos o procedimientos para el uso y administración de medios informáticos removibles.

➢ Se deben adoptar procedimientos o mecanismos de eliminación o borrado seguro de la información institucional alojada en cualquier medio extraíble, que ha de ser retirado o reutilizado en la empresa.

➢ Los medios removibles que contengan información institucional, se deben almacenar en un ambiente seguro y protegido contra el acceso no autorizado y de acuerdo con las especificaciones de los fabricantes o proveedores.

➢Todo medio extraíble que vaya a ser utilizado en los equipos de cómputo de INDUSTRIAS MORARBE S.A.S., debe ser analizados con la herramienta de antivirus de la empresa, por lo tanto, se debe habilitar la opción de escaneo automático de amenazas en el software de antivirus.

7.5. CONTROL DE ACCESO

7.5.1. Política de Control de Acceso

El Sistema de Gestión de Seguridad de la Información SGSI de INDUSTRIAS MORARBE S.A.S., busca reducir los riesgos que atenten contra la confidencialidad, integridad y disponibilidad de los activos de información de la empresa que se encuentran a cargo de sus funcionarios(as), empleados(as) contratistas o terceros; para lograr este objetivo se establecen controles que regulan el acceso a las redes, los datos y la información institucional, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente aquellas clasificadas como áreas de trabajo seguras, como los centros de procesamiento de datos, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado y otras áreas esenciales para el cumplimiento de las funciones misionales de la Empresa.

INDUSTRIAS MORARBE S.A.S., lleva a cabo el control de acceso a la información permitiendo mantener la trazabilidad de las acciones realizadas, identificando entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso y accesos denegados.

7.5.2. Gestión de acceso de usuarios

Lineamientos generales

➢ Todos los usuarios a quienes se les autorice el ingreso a los sistemas y aplicaciones de TI, deberán contar con un identificador único (usuario y contraseña), el cual será personal e intransferible.

➢ Los responsables de los sistemas de información deberán realizar revisiones y actualizaciones periódicas de los roles y privilegios de acceso de los usuarios, inactivando las que no se encuentren en uso o pertenezcan a usuarios retirados no autorizados.

➢ La creación del registro de usuarios para otorgar y revocar el acceso a los sistemas de información, bases de datos y servicios de TI, debe hacerse de acuerdo con lo establecido en el procedimiento "Gestión de usuarios".

➢ Para la creación o definición del usuario de red se deben seguir las siguientes especificaciones en su estructura:

✓ Primera letra del nombre.

✓ Primera letra del segundo nombre, de no tener segundo nombre se continuará con el siguiente ítem.

✓ Primer apellido.

✓ En caso de coincidir con otro identificador de usuario, se agregará la primera letra inicial del segundo apellido.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC debe asegurarse, que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos y/o equipos de la plataforma tecnológica, sean deshabilitados o eliminados.

➢Es responsabilidad de la Dirección de TIC y de todos los funcionarios(as) y contratistas activar y usar en todas las herramientas que se disponga doble factor de autenticación o validación de captcha para acceder a las páginas o herramientas propias de INDUSTRIAS MORARBE S.A.S.

7.5.3. Responsabilidades de los usuarios

Lineamientos generales

➢ Todos los usuarios serán responsables de las actuaciones realizadas con sus credenciales de red (usuario, contraseña y números de celular) asignadas para el uso de los sistemas de información y demás recursos tecnológicos a los cuales se les proporcione acceso.

➢ Las contraseñas de red son secretas y bajo ninguna circunstancia deben ser compartidas o reveladas a otra persona.

➢ Los usuarios a los cuales se les otorgue acceso a la red de datos y comunicaciones, sistemas de información y demás servicios de TI que hacen parte de la plataforma tecnológica de INDUSTRIAS MORARBE S.A.S., deben acogerse y acatar las políticas y directrices establecidas por la empresa para la gestión de contraseñas.

➢Los (las) funcionarios(as), empleados(as) contratistas y terceros que tengan acceso a la información de INDUSTRIAS MORARBE S.A.S., no deben realizar modificaciones sobre la información institucional sin estar autorizados para ello, deberán guardar la

confidencialidad de la información a la cual tengan acceso y no vulnerar los controles de seguridad establecidos por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC.

7.5.4. Control de Acceso a Sistemas y Aplicaciones

Lineamientos generales

➢ Todos los usuarios a quienes se les autorice el ingreso a los sistemas y aplicaciones de TI, deberán contar con un identificador único (usuario y contraseña), el cual será personal e intransferible.
➢ El acceso a los sistemas de información y demás recursos de TI de INDUSTRIAS MORARBE S.A.S., será autorizado por el(la) funcionario(a) responsable de su protección y salvaguarda a través del procedimiento establecido para la gestión de usuarios.
➢ Se debe implementar mecanismos para que los usuarios cambien las contraseñas de acceso a los sistemas de información que les han sido asignadas por primera vez.
➢ Se debe solicitar a los usuarios la actualización de número de celular para aquellas aplicaciones y herramientas que utilicen doble factor de autenticación MFA.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, debe asegurarse de identificar al usuario cuando solicita restablecer la contraseña por olvido o bloqueo, e implementará los mecanismos necesarios que garanticen su confidencialidad.
➢ Las contraseñas establecidas deber ser fuertes, no repetibles en un periodo de tiempo o en cambios anteriores, deben tener una longitud mayor a 8 caracteres que incluyan mínimo una letra mayúscula, una letra minúscula, un número y un carácter especial, no deben contener palabras que se asocien a la vida personal de los usuarios (número de cédula, fechas de nacimiento, nombre de los hijos, etc.), no debe contener números repetidos por ejemplo 000, ni números o letras consecutivos tales como 123 o abc.
➢ Las cuentas de red se bloquearán después de tres (3) intentos fallidos con desbloqueo automático a los quince (15) minutos, además el sistema solicitará cambio de clave después de cumplido un periodo de tiempo de noventa (90) días calendario.
➢ Si se sospecha que las contraseñas han sido reveladas a otras personas, se debe proceder al cambio inmediato.
➢Las contraseñas no deben escribirse ni dejarse en lugares visibles a otros usuarios o terceros.

- Se deben implementar medidas de protección y almacenamiento seguro para las contraseñas de administración de sistemas o servicios de TI (aplicaciones, bases de datos, equipos y dispositivos, servidores, etc.), garantizando que solamente podrán ser conocidas por el(los) responsable(s) del (de los) servicio(s) y por el Director de Tecnologías de la Información y las Comunicaciones DTIC, y solo serán reveladas en estrictamente necesarios.
- Las contraseñas de administración deben ser cambiadas cuando se haga uso de estas de manera regular y deben cumplir con todos los demás lineamientos generales de políticas de contraseñas establecidos en este documento.
- La eliminación, reasignación o inactivación de los privilegios de acceso otorgados sobre los recursos tecnológicos, como servicios de red, sistemas de información, bases de datos, etc, por novedades de personal, ya sean temporales o definitivas, se realizarán de acuerdo al procedimiento de Gestión de Usuarios formalmente establecido y acorde con las novedades reportadas a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, por parte de la Dirección de Talento Humano, los jefes de dependencias y/o los supervisores de contratos.
- La contraseña de administrador local de las estaciones de trabajo se usará exclusivamente para efectos de soporte técnico por parte del personal autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC y bajo ninguna circunstancia será revelada a personas no autorizadas.
- Se prohíbe el uso de software o programas utilitarios que puedan violar o evadir los controles de seguridad para el acceso seguro a los sistemas y aplicaciones.
- La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, implementa las medidas necesarias para limitar el acceso al código fuente de los sistemas de información y/o aplicativos de INDUSTRIAS MORARBE S.A.S.
- Solo se permitirá el acceso al código fuente de los sistemas de información y/o aplicativos de INDUSTRIAS MORARBE S.A.S., al personal autorizado del Grupo de Sistemas de información de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

7.6. CRIPTOGRAFÍA

7.6.1. Política sobre el uso de los controles criptográficos

La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC es la encargada de definir los mecanismos de cifrado de información más apropiados frente a

las necesidades de INDUSTRIAS MORARBE S.A.S., con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información de la empresa, adopta los controles de cifrado de datos que reduzcan los riesgos de seguridad de la información.

El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los(as) funcionarios(as), empleados(as) y contratistas de INDUSTRIAS MORARBE S.A.S.

Lineamientos generales

➢ La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, suministrará las herramientas necesarias para garantizar el cifrado y envío seguro de la información confidencial, sensible, o reservada que será almacenada y/o transmitida al interior o exterior de la empresa.
➢ Toda información sensible, confidencial o reservada que se transmita al interior o fuera de la empresa debe ser encriptada y protegida con una contraseña segura, antes de enviarla al destinatario.
➢La contraseña de encripción debe ser compartida con el destinatario por un medio diferente al del envío de la información.

7.7. SEGURIDAD FÍSICA Y DEL ENTORNO

7.7.1. Áreas seguras Lineamientos generales

➢ Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos de comunicaciones y seguridad perimetral y demás infraestructura de TI, serán consideradas como áreas seguras y de acceso restringido para personal no autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones.
➢ No se permite fumar, ni el ingreso o consumo de alimentos o bebidas en las instalaciones de centros de cómputo y/o de cableado.
➢ En las dependencias donde se gestione, almacene y procesa información de INDUSTRIAS MORARBE S.A.S., deben implementarse controles de acceso seguro, con el fin de prevenir accesos no autorizados, adulteración, perdida, consulta, daños e interferencia en el funcionamiento de los aplicativos e información de la empresa.

➢ Las puertas de acceso a las oficinas e instalaciones de INDUSTRIAS MORARBE S.A.S., consideradas como áreas seguras y/o de acceso restringido, deben permanecer cerradas y aseguradas con el fin de prevenir el acceso de personal no autorizado.

➢El personal responsable designado por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, deberá monitorear periódicamente la temperatura de los espacios destinados al procesamiento o almacenamiento de información como centros de cómputo y/o cableado.

7.7.2. Equipos Lineamientos generales

➢ La instalación de hardware conectado a la red y la atención de nuevos requerimientos y adecuación de equipos e infraestructura de TI, debe realizarse de acuerdo con los procedimientos formalmente establecidos en el sistema de gestión de calidad de INDUSTRIAS MORARBE S.A.S..; en consecuencia, no está permitido conectar computadores, servidores, dispositivos de comunicaciones como concentradores, switches, enrutadores o cualquier otro hardware a la red de datos y comunicaciones, sin la participación y/o supervisión de personal autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

➢ Todos los servidores, equipos de comunicaciones y demás elementos que soportan la infraestructura tecnológica de INDUSTRIAS MORARBE S.A.S., deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales, incluyendo perímetros de seguridad, controles de acceso físico, seguridad en el suministro de energía eléctrica y cableado y sistemas de detección y extinción de incendios.

➢ Se debe prevenir el daño de los equipos por interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas, obstrucción o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en ellos. Por esto, no se deben mantener encima o cerca de los computadores, objetos como ganchos, clips, alimentos, líquidos o cualquier elemento que pueda afectar el funcionamiento del equipo.

➢ El suministro de energía eléctrica deberá estar regulado a 110 voltios y con sistema de polo a tierra, salvo especificación en contrario del fabricante o proveedor de los equipos, y se debe contar con sistema de energía ininterrumpida (UPS) y/o planta eléctrica con combustible suficiente y continuo para su operación para asegurar el apagado controlado y sistemático o la ejecución continua del parque tecnológico que soporte las operaciones de la empresa.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC deberá elaborar el cronograma de mantenimiento preventivo, el cual será notificado a las dependencias con la debida anticipación, con el fin de asegurar la prestación del servicio a los usuarios. Adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de pérdida de equipos o información institucional.

➢ Las solicitudes de mantenimiento o de soporte técnico para solucionar problemas relacionados con los servicios tecnológicos a cargo de la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, deben realizarse a través del servicio de mesa de ayuda disponible en la Intranet.

➢ Ningún(a) funcionario(a), empleado(a) y/o contratista diferente al personal autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, está autorizado(a) para destapar, intervenir, efectuar reparaciones y/o modificaciones en los equipos de cómputo de la empresa. El mantenimiento preventivo y correctivo debe ser realizado exclusivamente por personal especializado y autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones.

➢ Para efectuar el traslado y/o retiro de equipos de cómputo y demás elementos que hacen parte del inventario de INDUSTRIAS MORARBE S.A.S. se deberá cumplir con los procedimientos establecidos por la dirección a cargo, egreso y traslado de bienes.

➢ Cuando por necesidades del servicio un(a) funcionario(a), empleado(a) y/o contratista requiera temporalmente el uso de un equipo fuera de la empresa, este debe ser solicitarlo por medio de correo electrónico a la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, quien autorizará mediante un oficio dirigido a la administración del edificio el retiro del dicho elemento.

➢ Cualquier cambio que se realice en el centro de cómputo o centros de cableado, y que potencialmente afecte los sistemas de información de la empresa, debe estar previamente autorizado y registrarse en una bitácora de ingreso al centro de cómputo.

➢ Toda persona que ingrese al centro de cómputo debe estar autorizada y acompañada por un(a) funcionario(a), empleado(a) y/o contratista de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC. Los administradores del centro de cómputo mantendrán un registro de las visitas autorizadas a esta área, en el que se identifique nombre del visitante, documento de identificación, fecha, hora de entrada y salida de las instalaciones, actividad por la cual ingresaron y la persona que autorizó su ingreso. A su vez, todo equipo informático ingresado al centro de cómputo deberá ser registrado.

➢Constituyen áreas de acceso restringido, el centro de cómputo, los cuartos de potencia (Plantas eléctricas, unidades de poder ininterrumpida UPS y cuartos de

electricidad) y centros de cableado; por lo que solo el personal autorizado por el responsable de su custodia puede acceder a estas áreas. El personal autorizado debe estar debidamente identificado como funcionario(a), empleado(a) y/o contratista de la empresa a cargo de realizar las actividades dentro de las instalaciones.

7.7.2.1 Política de escritorio y pantalla limpia

Los(as) funcionarios(as), contratistas y terceros de INDUSTRIAS MORARBE S.A.S., deberán adoptar buenas prácticas para el manejo y administración de la información institucional física, digital o electrónica, que se encuentre a su cargo, con el fin de garantizar su integridad, confidencialidad y disponibilidad, para lo cual se establecen lineamientos que los usuarios deben conocer y cumplir, manteniendo comportamientos adecuados mientras están manipulando la información o mientras se ausentan del puesto de trabajo, independientemente del medio en el cual se encuentren almacenados, protegiéndola del acceso no autorizado, pérdidas o daños ocasionados voluntaria o involuntariamente.

Lineamientos generales

➢Es responsabilidad de todos(as) los(as) funcionarios(as), empleados(as) y/o contratistas y terceros que tienen relación directa con INDUSTRIAS MORARBE S.A.S., salvaguardar los activos que contengan información institucional almacenada en medio físico, digital o electrónico, siguiendo como mínimo los siguientes lineamientos:

Escritorios limpios

➢ Se deben mantener los escritorios físicos y áreas de trabajo libres de todo material o elemento que contenga información clasificada como confidencial, a menos que esta esté siendo utilizada por personal autorizado, el cual deberá garantizar el aseguramiento adecuado de la misma en todo momento.
➢ Los(as) empleados(as) deben mantener el puesto de trabajo y escritorio de los equipos de cómputo, organizado y libre de archivos o información institucional que pueda ser objeto de consulta, copiado, eliminación por personal no autorizado.
➢Se debe evitar el consumo de alimentos o bebidas en áreas de trabajo donde se encuentre ubicada la información institucional en papel, equipos de cómputo,

dispositivos electrónicos o cualquier medio de almacenamiento que pueda llegar a ser afectado por el derrame de líquidos o residuos de alimentos.

Bloqueo de sesión

➢ Todos los(as) funcionarios(as), empleados(as) y/o contratistas deben bloquear su sesión de trabajo en el sistema operativo del equipo de cómputo al momento de ausentarse de su puesto de trabajo, sin importar que esté configurado para bloquear la sesión de forma automática después de un tiempo determinado.

Aseguramiento de la información confidencial

➢ Toda información impresa y/o en medios magnéticos que sea clasificada como confidencial, y que no esté siendo utilizada, deberá permanecer asegurada de forma adecuada, usando para esto archivadores, cajas fuertes o muebles destinados para su almacenamiento seguro.

➢Todo(a) empleado que tenga acceso a información confidencial en medios físicos, deberá prevenir su divulgación o acceso a personas no autorizadas que trabajen en ambientes o módulos de trabajo cercanos o que sean ajenas a la empresa.

➢ La información digital que contengan información sensible o confidencial de INDUSTRIAS MORARBE S.A.S., deberá ser almacenada en rutas que impidan el fácil acceso por personal no autorizado, y no se deben guardar ni dejar accesos directos de la misma en el área de escritorio de la pantalla del computador.

➢ Es responsabilidad de los(as) funcionarios(as), empleados(as) y/o contratistas retirar de forma inmediata cualquier tipo de documento enviado a las impresoras dispuestas para tal fin.

➢Los tableros de salas de reuniones o puestos de trabajo deberán ser borrados al finalizar las sesiones de trabajo o reuniones en caso de contener información confidencial.

No reciclaje de papel con información confidencial

➢Todo documento que contenga información clasificada como confidencial no podrá ser reciclado; y deberá ser destruido de tal manera que se impida la reconstrucción de dicha información.

Equipos desatendidos

➢ Toda vez que el personal se ausente de su lugar de trabajo, debe además de bloquear su estación de trabajo, guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.
➢ Si la estación de trabajo del personal está ubicada cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
➢ Al finalizar la jornada de trabajo, el personal debe apagar su equipo de cómputo, guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los sistemas de información y servidores.
➢ Las estaciones de trabajo y equipos portátiles de la empresa, tendrán aplicado un protector de pantalla definido por Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, que se activará cuando el equipo permanezca inactivo durante un tiempo determinado.
➢ La pantalla de autenticación a la red de la empresa debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información adicional.
➢El papel tapiz se configura automáticamente en cada uno de los equipos conectados a la red LAN de INDUSTRIAS MORARBE S.A.S., este sirve para difundir información institucional y debe ser remitido por la Oficina de Comunicaciones.

7.8. SEGURIDAD DE LAS OPERACIONES

7.8.1. Procedimientos operacionales y responsabilidades

Lineamientos generales

➢ La Empresa establecerá procedimientos relacionados con la operación y administración de la información institucional, estarán documentados y serán puestos a disposición del personal que lo requiera.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, deberá mantener y proveer a su personal, los manuales, guías y procedimientos de configuración de equipos, plataformas informáticas y demás servicios de TI.
➢ Los ambientes de desarrollo, prueba y producción estarán separados físicamente (diferente hardware) siempre que sea posible, y se definirán y documentarán las reglas para la transferencia de software desde el estado de prueba hacia el estado producción.

- La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, cuenta con el procedimiento "Gestión de Cambios" para el control de cambios en el desarrollo de nuevas aplicaciones y en general, para cualquier cambio que impacte los servicios y la infraestructura tecnológica que soporta la información de INDUSTRIAS MORARBE S.A.S.
- La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, debe monitorear permanentemente el estado de los recursos y plataformas tecnológicas, así como proyectar el crecimiento de los mismos, con el fin de prever y proyectar las futuras necesidades de ampliación de recursos para garantizar su capacidad y adecuada operación.

7.8.2. Protección contra Códigos Maliciosos

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC será la responsable de instalar, configurar y administrar la solución de antivirus en los equipos de cómputo de INDUSTRIAS MORARBE S.A.S.

➢ Todos los equipos de cómputo de propiedad de la empresa deben tener instalado el software de antivirus debidamente actualizado y licenciado a nombre de INDUSTRIAS MORARBE S.A.S., por lo tanto, todo nuevo equipo debe ser incluido dentro del dominio de la red de datos y comunicaciones institucional, para que apliquen las actualizaciones y análisis correspondientes.

➢ Para proteger la información institucional al distribuir archivos a otros usuarios internos o externos de la empresa, se debe contar con solución de antivirus que realice el análisis de los archivos y medios de almacenamiento en tiempo real.

➢ Está prohibido desinstalar o deshabilitar el software antivirus de los computadores de la empresa por parte de personal no autorizado para realizar actividades de soporte técnico. Si existen indicios de infección por malware, se debe realizar un análisis del equipo y sus archivos y verificar su eliminación mediante el software de antivirus, además se debe reportar el incidente a la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC.

➢ Todo medio de almacenamiento removible como discos duros externos, dispositivos USB, discos compactos, etc, que vaya a ser conectado a un equipo de cómputo de la Empresa, debe ser analizado manual o automáticamente con el software de antivirus, como medida preventiva antes de su uso.

➢ Está prohibido el uso y/o instalación de software no autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC. En caso de necesitar la instalación de algún software en los equipos de cómputo institucionales, se deberá

solicitar la autorización y apoyo en la instalación a la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, está facultada para revisar periódicamente la información y el software instalado en los equipos de cómputo de INDUSTRIAS MORARBE S.A.S., y realizará la eliminación de los archivos y/o la desinstalación inmediata del software no autorizado, que puedan generar riesgos para la seguridad de la información o incumplan con las políticas de seguridad de la empresa o la normatividad vigente relacionada con derechos de autor y propiedad intelectual.

➢En caso de tener sospechas de instalación de código malicioso este debe notificarse por parte del funcionario al área TIC para su respectiva validación y tratamiento del mismo.

7.8.3. Copias de respaldo (Backups)

7.8.3.1.Política de Backups

INDUSTRIAS MORARBE S.A.S.., adopta la presente política de backups, con el fin de establecer los lineamientos y directrices relacionadas con la planeación, programación, generación, custodia y entrega de los backups de la información, equipos, sistemas tecnológicos y demás activos de información que estén bajo la administración de la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, y que deban ser protegidos con el fin de contribuir a la seguridad de la información institucional y la continuidad de las operaciones de la empresa.

Lineamientos generales

➢ La Dirección de Tecnologías de la Información y las Comunicaciones, DTIC contará con un procedimiento de gestión de backups de información, en el cual se especificarán las actividades relacionadas con la ejecución de las tareas programadas para la creación de los backups, su custodia y entrega o restauración.

➢ Los(as) funcionarios(as), empleados(as), contratistas y terceros responsables de la administración de equipos y demás elementos que almacenen o procesen información institucional y hagan parte o soporten la infraestructura tecnológica de INDUSTRIAS MORARBE S.A.S.., deberán generar las respectivos backups de cada uno de los sistemas a su cargo y asegurarse de su correcto almacenamiento y custodia.

➢ El responsable del Sistema de Gestión de Seguridad de la Información - SGSI de INDUSTRIAS MORARBE S.A.S., realizará revisiones periódicas sobre la correcta ejecución del procedimiento de backups y de los lineamientos establecidos en la presente política.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC debe contar con un listado de aplicaciones críticas y componentes tecnológicos que deben ser respaldados, o un plan de backups, el cual debe ser revisado y actualizado de manera anual y/o cuando se presenten adiciones o modificaciones a la plataforma o infraestructura tecnológica.

➢La frecuencia y alcance de los backups de la información, al igual que los periodos de retención se deben establecer teniendo en cuenta la criticidad de la información respaldada, las necesidades de las diferentes dependencias o procesos de la empresa y/o por la legislación vigente aplicable a INDUSTRIAS MORARBE S.A.S.

➢ Se debe implementar y mantener actualizada una bitácora que contenga la información básica de los backups generados de acuerdo con el plan de backups, y que permita establecer como mínimo el activo al que corresponda la copia, la fecha de generación, la ubicación, la frecuencia, el tamaño de la copia, el formato, etc., para mantener la trazabilidad y garantizar que todas las copias estén localizables y puedan ser recuperadas en caso de necesidad.

➢ Se debe llevar un registro de las solicitudes de entrega o restauraciones realizadas con los backups.

➢ Se deben efectuar backups de la información antes y después de cualquier cambio en la configuración de cualquier componente de la plataforma tecnológica que soporte las operaciones críticas de la empresa.

➢ Se deben almacenar los logs de ejecución y generación exitosa o fallida de los backups por un periodo no menor a 1 año.

➢ Todo evento fallido en la ejecución de los backups de información debe ser registrado en la bitácora de backups y notificado al administrador o responsable de la respectiva plataforma y/o aplicación.

➢ Se deben realizar copias de seguridad adicionales para los componentes catalogados como críticos y procurar que estas sean almacenadas en ubicaciones diferentes.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC será la encargada de definir el formato de etiquetado de los medios dónde se almacenen copias respaldo de la información a su cargo.

➢ Los backups de información deben almacenarse en un lugar seguro, dotado de medidas de seguridad física que garanticen la protección de los datos contra pérdida, daño o acceso no autorizado; en caso de contratar a un tercero para el almacenamiento

y custodia de los backups de información, la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC debe asegurarse que el Tercero cumpla con las medidas de seguridad necesarias para garantizar la seguridad de la información.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, será la encargada de definir el personal que se encuentra autorizado para el ingreso al lugar donde se encuentran almacenadas los backups de información.

➢ Al cumplir el ciclo de vida útil, los medios de almacenamiento de los backups serán inutilizados de forma segura, evitando la recuperación de la información contenida y el acceso por parte de personas no autorizadas.

➢ Se deben programar y realizar pruebas de restauración periódicas de la información contenida en los backups para comprobar su correcto funcionamiento.

➢ La dirección TIC deberá velar por la capacidad suficiente para realizar los respaldos de seguridad de los datos de los funcionarios y/o contratistas como de las plataformas institucionales.

➢Es responsabilidad de los funcionarios(as), empleados(as) y/o contratistas el realizar uso y apropiación de las herramientas que se contraten para el almacenamiento en repositorios tales como onedrive u otros que cuente la empresa y sirvan para el manejo colaborativo y backups.

Cualquier información adicional, deberá remitirse a las políticas de procedimiento para la seguridad de la información.

Backups de información contenida en equipos de cómputo

➢ La custodia y respaldo de la información que se almacene en los equipos de cómputo y demás medios tecnológicos asignados por INDUSTRIAS MORARBE S.A.S., será de responsabilidad de cada funcionario(a), empleado(a) o contratista dueño o generador de dicha información a quien le haya sido asignado el equipo de cómputo o medio tecnológico.

➢ Es responsabilidad de cada funcionario(a), empleado(a) o contratista identificar, clasificar y definir la información institucional a su cargo para respaldar, y solicitar a la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, el acceso a los medios de almacenamiento autorizados con el fin de mantener una copia fiel de esta información.

➢ Es responsabilidad de cada usuario mantener copia de la información institucional a su cargo en los medios de almacenamiento que la Dirección de Tecnologías de la Información y las Comunicaciones DTIC asigne para tal fin.

➢La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC no se hará responsable por la pérdida y/o modificación de la información institucional alojada en los medios de almacenamiento de respaldo NO autorizados, y/o en los equipos de cómputo asignados a los(as) funcionarios(a)s y/o contratistas. Tampoco será responsable de la pérdida y/o modificaciones de la información institucional alojada en los medios de almacenamiento de respaldo autorizados, cuando estas modificaciones sean producto de la manipulación de un usuario autorizado.

7.8.4. Registro y Seguimiento

Lineamientos generales

➢ Las aplicaciones y sistemas de información de INDUSTRIAS MORARBE S.A.S., deben generar logs de eventos o trazas de auditoría con los registros de las actividades de los usuarios, fallas, excepciones y eventos de seguridad de la información que se generen.
➢ Los registros y sistemas gestión de eventos se deben conservar y revisar regularmente, garantizando su posterior consulta y protección contra acceso no autorizado, modificación o borrado accidental o malintencionado.
➢ En lo posible, los registros de eventos deben registrar como mínimo la siguiente información:
✓ Identificación de usuarios
✓ Actividades realizadas en el sistema
✓Fechas y horas de acceso y salida de los sistemas
✓ Registros de acceso exitosos y denegados
✓ Cambios en las configuraciones de los sistemas
✓ Cambios en los privilegios de los sistemas
✓ Archivos a los que se tuvo acceso
✓ Direcciones y protocolos de red
✓ Activación y desactivación de sistemas de protección
➢ Las actividades realizadas por los usuarios administradores y operadores de los sistemas de información, deber ser registradas, protegidas y revisadas con regularidad.
➢Los relojes de los sistemas de procesamiento de información de INDUSTRIAS MORARBE S.A.S. se deben sincronizar con una única fuente de referencia de tiempo.

7.8.5. Control de software operacional

Lineamientos generales

➢ INDUSTRIAS MORARBE S.A.S., establece mecanismos para la instalación de software autorizado en los equipos de cómputo y servidores que hacen parte de la infraestructura tecnológica, implementando los controles técnicos necesarios y definiendo el personal responsable de la instalación y soporte.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, validará y realizará las respectivas pruebas de calidad y funcionamiento del software a instalar, antes de ser puesto en producción.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, será la responsable de analizar el software y autorizar su instalación, la cual debe ser realizada exclusivamente por personal autorizado.
➢ Se debe mantener un registro actualizado del software de propiedad de INDUSTRIAS MORARBE S.A.S.
➢Se deben conservar las versiones anteriores del software de las aplicaciones, junto con la información, parámetros, procedimientos y detalles de configuración.

7.8.6. Gestión de Vulnerabilidad Técnica

Lineamientos generales

➢La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, revisará periódicamente las vulnerabilidades y debilidades técnicas de los sistemas de información y la infraestructura tecnológica, mediante el uso de herramientas de software especializadas, en pruebas de penetración, detección de vulnerabilidades y verificación de controles. En caso de ser necesario, las revisiones podrán realizarse mediante la contratación de una asistencia técnica especializada. El resultado de las revisiones se presentará en un informe técnico para su interpretación y remediación por parte de los especialistas de la Empresa.
➢Se prohíbe la instalación de software por parte de personal diferente a los autorizados por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC.

7.9. SEGURIDAD DE LAS COMUNICACIONES

7.9.1. Gestión de la seguridad de las redes

7.9.1.1. Política de Controles en la Red de Datos y Transferencia de Información

La Dirección de Tecnologías de la Información y las Comunicaciones de INDUSTRIAS MORARBE S.A.S., establecerá los controles y mecanismos necesarios para suministrar el servicio de transferencia de información de una manera segura, con el fin de contribuirá mantener la confidencialidad, integridad y disponibilidad de la información que circula a través de las redes de datos y comunicaciones de la empresa.

Para cumplir con este objetivo, se establecen controles y lineamientos de obligatorio cumplimiento relacionados con las configuraciones de seguridad, el uso y responsabilidades de los (las) funcionarios(as), empleados(as) y contratistas a cargo de la administración y el uso de equipos y servicios de TI que soportan la transferencia interna y externa de la información institucional.

Lineamientos generales

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, gestiona y establece mecanismos y controles para prestar el servicio de redes de datos y comunicaciones en la empresa y propende por la protección de los datos y los servicios conectados en las redes de INDUSTRIAS MORARBE S.A.S., contra el acceso no autorizado.

➢ La transferencia de la información institucional de INDUSTRIAS MORARBE S.A.S., se controla según los niveles de clasificación legal de la información establecidos y las políticas de seguridad de la información de la empresa. En caso de que se requiera intercambiar información sensible, confidencial, reservada o pública clasificada, se deben implementar los controles de cifrado de información de acuerdo con lo establecido en la política de controles criptográficos.

➢Los intercambios de información con terceros deben estar soportados por medio de contratos o acuerdos debidamente formalizados, determinando los medios y controles para el tratamiento de la información. Así mismo, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.

Gestión de la Seguridad en las Redes

➢ Se deben establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.

➢ Se deben establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
➢ Se deben Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
➢ Todos los componentes de red deben contar con un sistema fuerte de autenticación para poder acceder a los mismos.
➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, implementa los mecanismos necesarios y establece acuerdos de niveles de servicio, para garantizar la disponibilidad de los servicios de redes de datos y comunicaciones.
➢ Únicamente personal autorizado puede ingresar a los equipos de comunicación.
➢ El acceso administrativo a los equipos de red debe ser centralizado y auditado.
➢ Tocas las conexiones de administración deben ser bajo conexiones cifradas.

➢ INDUSTRIAS MORARBE S.A.S. implementa mecanismos de segmentación de redes a través de Vlan´s, dependiendo de la criticidad de los recursos y servicios involucrados, con el fin de contribuir al control de acceso, optimizar el rendimiento en la red y garantizar que los servidores y los usuarios no ocupan el mismo segmento de red.
➢ Todos los componentes de red deben estar actualizados a su último paquete de seguridad estable.
➢ Los componentes de red deben ser monitoreados todo el tiempo para asegurar su correcta configuración y seguridad basada en las líneas base definidas por el área de seguridad de la información.
➢ Únicamente los servicios requeridos deben estar habilitados. Aquellos servicios de red que no se necesiten deberán ser deshabilitados.
➢ Todos los accesos remotos a la red deben ser autorizados por el administrador de red y el líder de seguridad de la información.
➢ Los(as) funcionarios(as), empleados(as) contratistas o terceros que desarrollen actividades en los sistemas de información de la empresa de manera remota, deben utilizar equipos de cómputo seguros que garanticen la no afectación de la seguridad de la red.
➢ Todas las conexiones entrantes (incoming) y salientes (outbound) entre la red de INDUSTRIAS MORARBE S.A.S., y cualquier otra red debe realizarse a través de dispositivos firewall y deberán usar protocolos NAT/PAT para realizar traducción de direcciones IP y así evitar divulgación externa de los direccionamientos internos de la empresa; en caso de poder usar NAT/PAT se deberán configurar listas de acceso donde

se garantice que únicamente personal autorizado pueda visualizar estos direccionamientos.

➢ Todo equipo o servicio que sea expuesto en la red externa deberá ser ubicado en una zona desmilitarizada (DMZ) la cual debe ser segmentada mediante dispositivos firewall.

➢ Estos servicios expuestos serán protegidos mediante el Web Application Firewall que ha destinado INDUSTRIAS MORARBE S.A.S. para la protección contra ataques informáticos.

➢ La información de direccionamiento interno, segmentación de red y enrutamiento se encuentra clasificada como confidencial y solo personal autorizado puede acceder a la misma.

➢ La totalidad de reglas configuradas en los dispositivos firewall deben estar documentadas, justificadas y aprobadas; dicha documentación deberá ser verificada con una periodicidad mínima de 6 meses.

➢ Todos los dispositivos sin excepción alguna que sean ingresados a las redes de datos Corporativas (incluyendo equipos de cómputo, impresoras, escáner, dispositivos de comunicaciones, entre otros) deben ser previamente registrados y configurados por la Dirección de TI.

➢ Cuando un componente tecnológico es registrado para uso en las redes corporativas, un nombre de red y dirección IP le será asignado de acuerdo al mecanismo establecido por la Dirección de TI. La información básica del propietario del componente, descripción y función debe ser registrada por el Administrador de dicho Componente o a quién designe.

➢ La definición y diseño del direccionamiento de las redes, así como la aprobación de asignación de direcciones IP fijas en la red es responsabilidad del Administrador de Redes y Telecomunicaciones.

➢ Todo componente tecnológico que sea ingresado a las redes corporativas debe cumplir con los requerimientos de seguridad y estándares mínimos establecidos por cada Administrador de Componente.

➢ Es responsabilidad de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC realizar revisiones periódicas de las configuraciones y estándares aplicados en los diferentes componentes tecnológicos con el fin de evaluar y velar por el cumplimiento de los requerimientos de aseguramiento de plataforma.

Transferencia de Información

➢ INDUSTRIAS MORARBE S.A.S., establecerá mecanismos seguros para la transferencia de información institucional internamente y con terceros, en cumplimiento de sus funciones y obligaciones legales.

➢La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, proporcionará las herramientas para garantizar la seguridad de la información, durante la transferencia a nivel interno y externo.

➢ La empresa proporcionará tecnologías de acceso remoto a sus funcionarios(as), contratistas y terceros a través de medios como VPN (Red virtual privada), y autorizará su uso de forma particular cuando así se requiera. La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, garantizará un adecuado esquema de seguridad para los mismos.

➢ Todos los computadores de la empresa que sean accedidos a través de herramientas de acceso remoto deben ser protegidos por mecanismos de control de acceso aprobados por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC.

➢ La conexión directa entre los sistemas de información de la empresa y otra organización o tercero vía redes públicas de datos como Internet, requieren de la aprobación de la Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, quien definirá los mecanismos de seguridad apropiados.

➢ INDUSTRIAS MORARBE S.A.S., se reserva el derecho de cancelar y/o terminar la conexión a sistemas de terceros, que no cumplan con los requerimientos internos de seguridad y confidencialidad establecidos o acordados.

➢Antes de autorizar y establecer las conexiones con sistemas de información de terceros para la trasferencia o consulta de información institucional, se deben establecer Acuerdos de Confidencialidad entre las partes, para lo cual se contará con la participación de la Oficina Asesora de Jurídica de INDUSTRIAS MORARBE S.A.S.

➢ Está prohibido el uso de herramientas de acceso remoto o de transferencia de información que no hayan sido autorizadas por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

➢ Está prohibido el envío o intercambio de información clasificada, reservada o sensible, sin la autorización del responsable o Jefe inmediato.

➢ Para la transmisión o envío de información clasificada, reservada o sensible a través de medios electrónicos, incluido el correo institucional, se debe asegurar de aplicar las medidas de seguridad necesarias y como mínimo, cumplir con los lineamientos establecidos en la política de controles criptográficos.

➢ Está prohibido utilizar el correo electrónico personal, para el envío y recepción de información institucional clasificada, reservada o sensible.

➢ No está permitido el envío o almacenamiento de información institucional clasificada, reservada o sensible a través de plataformas gratuitas como (wetransfer, google drive, Dropbox, WhatsApp, Messenger, etc.) o cualquier servicio diferente a Office 365 institucional.

➢El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las tareas propias de la función desarrollada por INDUSTRIAS MORARBE S.A.S.

➢El uso del servicio de correo electrónico de INDUSTRIAS MORARBE S.A.S., para fines personales no está autorizado.

➢Todo(a) funcionario(a) o contratista inscrito en INDUSTRIAS MORARBE S.A.S., dispondrá de una cuenta de correo electrónico activa, y para su creación se debe seguir con el procedimiento ""Gestión de usuarios"" establecido de INDUSTRIAS MORARBE S.A.S.

➢ El servicio de correo electrónico oficial de INDUSTRIAS MORARBE S.A.S., es el aprobado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC; los(as) funcionarios(as), contratistas y terceros reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.

➢ Se debe tener actualizado y registrado medios de contacto alternativo como por ejemplo un número de celular o correo electrónico para que se realice correctamente la validación de identidad en el acceso a los servicios de office 365 contratados por la empresa para que por medio de llamada, mensaje o código se complete el ciclo de autenticación y seguridad.

➢ La clave de acceso al servicio de correo electrónico es personal e intransferible, no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información - SGSI de INDUSTRIAS MORARBE S.A.S.

➢ Las contraseñas de las cuentas de correo institucional genéricas o que no estén asociadas a un usuario particular, (Por ejemplo Gerencia@morarbe.com.co), deberán ser cambiadas cuando la persona encargada de administrarla sea retirada de la empresa o trasladada de dependencia, o cese su responsabilidad sobre la cuenta de correo.

➢ De ser estrictamente necesario y cuando exista justificación para ello, INDUSTRIAS MORARBE S.A.S., podrá supervisar el uso del servicio de correo electrónico corporativo respetando los derechos del titular de la cuenta de correo electrónico, para lo cual el usuario propietario de la misma debe ser previamente informado del procedimiento a realizar.

➢ La vigencia de la cuenta para funcionarios(as) y contratistas comprende el periodo desde la fecha de ingreso o firma del contrato y finaliza el último día de la fecha de retiro o terminación/suspensión del contrato.

➢ El uso de la cuenta de correo es con fines del cumplimiento de las funciones y/o obligaciones contractuales, y su uso es de carácter obligatorio, en ella llegará información oficial de conocimiento necesario para los(as) funcionarios(as), empleados(as) y contratistas de la empresa.

➢ Se prohíbe el uso de cuentas de correo gratuito con propósitos institucionales o cuentas de suscripción gratuita a otros proveedores.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones – DTIC, será la encargada de establecer las cuotas y límites de almacenamiento para las cuentas de correo electrónico institucionales de acuerdo a las necesidades propias de la empresa.

➢ Es responsabilidad del funcionario(a), empleado(a) o contratista depurar su cuenta periódicamente siendo él el único responsable de realizar las copias de seguridad de sus correos.

➢ El usuario debe leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.

➢ Solo podrán enviar correos masivos aquellas dependencias que por su naturaleza de socialización y sensibilización lo requieran a través de la cuenta de correo del jefe de la dependencia; tales como (Gerencia General, Dirección de Talento Humano, Oficina de comunicaciones y la dirección de Calidad donde se incluye de Gestión Documental, Recursos Humanos, etc.).

➢ El incumplimiento por parte del funcionario(a), empleado(a) y/o contratista de los lineamientos o el mal manejo de su cuenta de correo institucional, puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo y en un último caso la notificación a la Dirección de Talento Humano y/o Dirección Administrativa y Financiera para que proceda disciplinariamente.

➢ No están autorizados los siguientes usos del servicio de correo electrónico y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:

➢ Exceder los servicios para los cuales se autorizó la cuenta.

➢ Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin identificar plenamente a su autor o autores o enviar anónimos.

➢ Difundir "cadenas" de mensajes que saturen el servicio entre otros problemas.

➢ Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.

➢ Agredir o lesionar directa o indirectamente a otras personas a través del envío de mensajes con contenido que atente contra la integridad y el buen nombre de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la empresa o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la Empresa.
➢ Crear, enviar, alterar, borrar mensajes suplantando la identidad de un usuario.
➢ Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.
➢ Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales ni afines a la misión institucional.
➢ Enviar correos de información masivos sin estar autorizado para ello.
➢Envío de mensajes no deseados o que puedan ser considerados como SPAM.

7.9.1.2. Servicio de acceso a internet

El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en INDUSTRIAS MORARBE S.A.S., los usos diferentes a los necesarios para el cumplimiento de las funciones de la Empresa son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio. El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con INDUSTRIAS MORARBE S.A.S., ya sea como funcionario(a), empleado(a) contratista o tercero.

Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en INDUSTRIAS MORARBE S.A.S., y para los cuales esté formal y expresamente justificado y autorizado.

Todos los (las) funcionarios(as), empleados(as) y contratistas que en el desarrollo de sus funciones utilicen el servicio de acceso a Internet de INDUSTRIAS MORARBE S.A.S., serán responsables del cumplimiento de las políticas de seguridad de la información de Empresa.

Los responsables de la administración de las redes de acceso a internet y los equipos de seguridad de INDUSTRIAS MORARBE S.A.S.., deben implementar y monitorear permanentemente los controles necesarios para evitar la circulación de información o contenidos desde Internet hacia la red de la Empresa que puedan constituirse en riesgos para la seguridad de la Información.

Lineamientos generales

➢Los recursos y servicios de Internet se usarán primordialmente para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de la institución, ni con los deberes y obligaciones de las personas establecidas en los diferentes reglamentos y manuales de la Empresa.

➢ Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados o no correspondan a sus funciones dentro de INDUSTRIAS MORARBE S.A.S.

➢ Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de INDUSTRIAS MORARBE S.A.S., o descargue desde Internet empleando la cuenta de acceso a Internet que se le ha suministrado.

➢ INDUSTRIAS MORARBE S.A.S., puede supervisar el acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las funciones institucionales, en los procesos de verificación del uso apropiado del servicio de acceso a Internet se respetan el derecho a la intimidad y privacidad del titular de la cuenta de acceso a Internet.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC procederá al bloqueo de sitios que se detecten como peligrosos o que atenten contra la seguridad de la información o que puedan interferir con el normal funcionamiento de los sistemas de información.

➢ El uso indebido del servicio de internet por parte de un usuario puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo.

➢ Acceder a sitios de streaming como YouTube u otras páginas, salvo que se requerían previa autorización del director de área y explícitamente por necesidad del servicio como capacitaciones, charlas, audiencias y todo lo que sea relacionado laboralmente y no personal.

➢ No están autorizados los siguientes usos del servicio de acceso a Internet y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:

➢ Descargar y/o distribuir archivos con virus, gusanos, troyanos y/o la trasmisión de archivos de imagen, sonido y video que no sean de tipo institucional.

➢ Acceder, descargar o transmitir información sometida a derechos de autor cuando no se tienen los derechos respectivos (juegos, música, videos, obras literarias, pictóricas, imágenes, etc).

➢ Descargar archivos o instalar programas de sitios web desconocidos o gratuitos sin previa autorización de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

➢ El acceso a sitios de música, juegos u otros sitios de entretenimiento on- line.

➢ El acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos aquellos que hacen parte de la ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.

➢ El acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía, salvo en los casos que estén debidamente autorizados en cumplimiento de las funciones, caso particular de investigaciones en procesos disciplinarios o administrativos; en tal caso se deben gestionar los mecanismos de acceso seguro en canales protegidos y configurados por personal autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

➢ Acceder a sitios web de carácter discriminatorio, racista o material potencialmente ofensivo para las personas, incluyendo, bromas de mal gusto, prejuicios, menosprecio o acoso.

➢Acceder a sitios de "hacking" o sitios reconocidos como inseguros para la seguridad de la información, los cuales puedan poner en riesgo la integridad, disponibilidad y confidencialidad de la información de INDUSTRIAS MORARBE S.A.S., salvo en los casos que se requiera para el cumplimiento de las funciones, en cuyo caso se deben gestionar los mecanismos de acceso seguro en canales protegidos y configurados por personal autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

7.9.1.3. Seguridad en la nube

INDUSTRIAS MORARBE S.A.S., en su propósito de cumplir con los lineamientos de apoyo a las actividades de mayor importancia, provee algunos de sus servicios de TI a través de computación en la nube. Con el fin de garantizar la seguridad de la información de los activos y servicios alojados en la nube, INDUSTRIAS MORARBE S.A.S., deberá tener en cuenta y aplicar en los procesos de contratación del servicio, los procedimientos establecidos por la empresa para la gestión de los riesgos de seguridad de información, y en ningún momento se deberá incluir activos de información ni servicios en la nube a los cuales el resultado del análisis de riesgos no arroje un nivel aceptable para la seguridad de la información.

Lineamientos generales

➢ En los casos que se requiera el almacenamiento de información institucional sensible, pública reservada o pública clasificada, se debe garantizar su acceso restringido mediante contraseña segura.

➢Todos los usuarios de servicios de computación en la nube de INDUSTRIAS MORARBE S.A.S., deben mantener especial cuidado con la información institucional y en todo momento aplicar y cumplir los controles de seguridad que se definan en el presente manual para el uso seguro de la información.

7.10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

7.10.1. Requisitos de seguridad de los sistemas de información

Lineamientos generales

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, se asegurará que en los procesos de adquisición de nuevos sistemas de información o de mejora a las aplicaciones de software existentes, se incluyan los requisitos suficientes para garantizar la seguridad de la información de acuerdo a las normas y estándares de desarrollo de software y a las disposiciones del presente manual.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, será responsable de ejecutar las pruebas necesarias junto con los desarrolladores y/o proveedores externos, que garanticen que las aplicaciones de software adquiridas o mejoradas cumplan con los requisitos de seguridad de la información exigidos.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, deberá asegurarse que todas las aplicaciones de software desarrolladas o adquiridas cuenten con los respectivos acuerdos de licenciamiento, condiciones de uso y derechos de propiedad intelectual.

➢ La actualización de la información contenida en los portales Web e Intranet de INDUSTRIAS MORARBE S.A.S., debe hacerse de acuerdo a lo establecido en la "Guía para la actualización de los portales web e intranet Institucionales"

➢ En caso de que algún componente o servicio del portal Web e Intranet se encuentre en mantenimiento o no disponible por fallas técnicas, se debe publicar una imagen o texto que informe al usuario sobre dicho evento.

➢ La redacción de cada uno de los contenidos de los portales Web e Intranet de INDUSTRIAS MORARBE S.A.S., está a cargo de los gestores de contenido asignados por cada dependencia y deberá producirse conforme a lo establecido en la "Guía para la actualización de los portales web e intranet Institucionales"

➢ Los cambios solicitados que requieran modificación de la estructura básica de los portales Web e Intranet o creación de otras nuevas, serán ejecutados exclusivamente por la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

➢ Se debe garantizar la autenticación secreta de los usuarios a los sistemas de información y aplicaciones institucionales, implementando controles que garanticen el acceso seguro y la confidencialidad de las operaciones.

➢ Se deben implementar métodos y/o protocolos de comunicación segura para la transmisión de datos de las aplicaciones y sistemas de información institucionales.

➢Se deben implementar las medidas necesarias para que los aplicativos y sistemas de información cuenten con herramientas que garanticen la integridad de la información, el no repudio y la prueba de entrega y recibo de las comunicaciones y documentos.

7.10.2. Seguridad en los procesos de desarrollo y soporte

7.10.2.1. Desarrollo seguro

Para el desarrollo de software al interior de INDUSTRIAS MORARBE S.A.S., se debe realizar un proceso de planificación de los desarrollos en donde se determine la respectiva metodología a utilizar, las etapas de desarrollo, la estructura de componentes a elaborar, los respectivos responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad, teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de INDUSTRIAS MORARBE S.A.S. Las etapas de desarrollo deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del software.

Lineamientos generales

➢ Los requerimientos de nuevos desarrollos o ajustes a las aplicaciones existentes serán realizadas por los responsables de las dependencias propietarias de estas a través de la mesa de ayuda y de acuerdo con el procedimiento formalmente establecido.

➢ La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad, se documentan entre la dependencia solicitante y la Dirección de Tecnologías

de la Información y las Comunicaciones DTIC. Los requerimientos del software se deben validar durante el proceso de aceptación del desarrollo de software.

➢ Para el desarrollo y puesta en producción del software se debe contar con ambientes separados de desarrollo, pruebas y producción, determinando roles y responsabilidades claramente establecidas a fin de evitar modificaciones no autorizadas del código fuente del software.

➢ Los cambios requeridos sobre el software de INDUSTRIAS MORARBE S.A.S., se controlan a través del procedimiento de "Gestión de Cambios", el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos de los cambios es necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su adecuada gestión.

➢ En los procesos de desarrollo, INDUSTRIAS MORARBE S.A.S. se asegura de establecer las condiciones necesarias para la transferencia de los derechos de propiedad intelectual de códigos fuente.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC se debe asegurar que los desarrollos de software en la empresa, se realicen utilizando herramientas de programación licenciadas.

➢ Los desarrollos de software en la empresa deben contar con los manuales técnicos y de usuario además de la respectiva documentación de acuerdo a la metodología utilizada.

➢ Cuando se contraten desarrollos con proveedores externos, se debe garantizar la definición y cumplimiento de los acuerdos de licenciamiento, propiedad de los códigos fuente y los derechos de propiedad intelectual, de acuerdo con la normatividad legal vigente.

➢ Durante el desarrollo de software se deberán realizar y documentar las pruebas de funcionalidad de la seguridad necesarias que incluyan la verificación de que no existe contenido malicioso ni presencia de vulnerabilidades conocidas.

➢Para la realización de pruebas, los datos utilizados no deben contener información real de los ambientes de producción, se deben preparar conjuntos de datos de prueba especiales que impidan la pérdida de confidencialidad de la información institucional.

7.11. RELACIONES CON LOS PROVEEDORES

7.11.1. Política de seguridad de la información para las relaciones con los Proveedores

Para los servicios contratados con proveedores en los cuales se requiera del intercambio de información institucional, se deben establecer acuerdos de confidencialidad y de intercambio de información en los que se definan claramente los requerimientos de seguridad de la información, incluida la obligación de cumplir con lo establecido en el presente manual y sus respectivas cláusulas civiles y penales en caso de incumplimientos.

El responsable del activo de información debe definir la finalidad de la autorización de acceso a la información que se otorgue al proveedor, y documentar la autorización del acceso a los datos de acuerdo con el fin previsto.

Siempre que se otorgue acceso a la información de INDUSTRIAS MORARBE S.A.S. a terceros, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de la Empresa y las cláusulas requeridas para proteger la información a la cual se otorgará el acceso.

Lineamientos generales

➢ INDUSTRIAS MORARBE S.A.S., establecerá con los proveedores, Acuerdos de Niveles de Servicio (ANS) para cada servicio contratado con sus respectivas penalizaciones en caso de incumplimiento, y realizará el seguimiento periódico de los mismos.
➢ Antes de conceder acceso a la información institucional de INDUSTRIAS MORARBE S.A.S., se debe dar a conocer el presente manual a los proveedores a los cuales se otorgará el acceso.
➢ Antes de conceder permisos de acceso a la información a los proveedores, el responsable del activo debe analizar la justificación de la necesidad y el tipo de acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso y los controles mínimos de seguridad a tener en cuenta frente al tratamiento de la información.
➢En ningún caso se otorgará acceso a los sistemas de información o áreas seguras de INDUSTRIAS MORARBE S.A.S., hasta no haber formalizado la relación contractual y firmado el acuerdo de confidencialidad con los Proveedores.

7.11.2. Gestión de la prestación de servicios de proveedores

Lineamientos generales

➢ INDUSTRIAS MORARBE S.A.S., será responsable de hacer el seguimiento periódico, supervisar y velar por el cumplimiento de las obligaciones contractuales y la calidad de los productos y servicios, así como el cumplimiento de los acuerdos de niveles de servicio establecidos con sus Proveedores.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, será la encargada de aprobar los cambios que deban realizar sus Proveedores durante la prestación de los servicios, garantizando los principios de seguridad de la información y teniendo en cuenta la criticidad del servicio afectado.

➢Los Proveedores de productos o servicios de INDUSTRIAS MORARBE S.A.S., deben abstenerse de realizar cambios que afecten la prestación de los servicios contratados con la empresa o generen riesgo para la seguridad de la información institucional, sin previo aviso y autorización de la Dirección de Tecnologías de la Información y las Comunicaciones DTIC.

7.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

7.12.1. Gestión de incidentes y mejoras en la seguridad de la información

Lineamientos generales

➢ INDUSTRIAS MORARBE S.A.S. establece los responsables para el tratamiento de los incidentes relacionados con la seguridad de la información en concordancia con las competencias, responsabilidades y los activos de información a su cargo.

➢ Todos(as) los(as) funcionarios(as), empleados(as) y contratistas de la empresa deberán reportar de manera oportuna a la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, a través de correo electrónico, teléfono o mesa de ayuda, las debilidades de seguridad en los sistemas de información o servicios tecnológicos, así como los incidentes de seguridad de información que detecten o que sean de su conocimiento.

➢ El responsable de seguridad informática junto con el responsable del (de los) activos afectados durante un incidente de seguridad, serán los encargados del seguimiento, documentación y análisis de los incidentes reportados, así como de su comunicación al jefe inmediato y a los propietarios de la información que pueda llegar a ser comprometida.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, será la responsable de establecer el procedimiento para la gestión y respuesta de incidentes de seguridad de la información, en el cual se deben considerar y determinar los criterios

para clasificar un evento de seguridad como un incidente, así como los pasos a seguir para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

➢ Todo evento que se clasifique como un incidente de seguridad debe ser documentado y tratado de forma inmediata y de acuerdo con los procedimientos formalmente implementados por la empresa.

➢La gestión de los incidentes de seguridad se debe registrar en una base de conocimientos y lecciones aprendidas, con el fin de que pueda ser consultada y sirva de apoyo oportuno para la prevención de futuros incidentes.

7.13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

7.13.1. Continuidad de seguridad de la información

Lineamientos generales

➢El Gerente General, Los Administradores, Los jefes de cada dependencia de la empresa, serán los responsables de identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la Empresa, evaluarán los riesgos para determinar el impacto de dichas interrupciones, identificaran los controles preventivos, y recomendarán ajustes a los planes de contingencia necesarios para garantizar la continuidad de las actividades de INDUSTRIAS MORARBE S.A.S.

➢La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC, Formulará los planes, controles y procedimientos necesarios, para asegurar la continuidad de los sistemas de información, aplicaciones y en general los servicios de TI que soportan las operaciones en las cuales se de tratamiento a la información institucional de INDUSTRIAS MORARBE S.A.S.

➢ En las instalaciones, plataformas o sistemas donde se procese o almacene información institucional crítica, se deben implementar medidas de redundancia suficientes para asegurar la disponibilidad de la información.

7.14. CUMPLIMIENTO

7.14.1. Cumplimiento de requisitos legales y contractuales

Lineamientos generales

➢INDUSTRIAS MORARBE S.A.S., con la participación de la Oficina Asesora de Jurídica y la Dirección de Tecnologías de la Información y las Comunicaciones DTIC, identificará, documentará, actualizará cuando sea necesario, y dará cumplimiento a la normatividad y requisitos legales relacionados con la seguridad de la información, que estén directamente relacionados con el ejercicio de sus funciones.

7.14.1.1.Política de Derechos de Propiedad Intelectual, Antipiratería y Antifraude

INDUSTRIAS MORARBE S.A.S. está comprometida con la seguridad de la información, el cumplimiento de la normatividad legal vigente relacionada con derechos de autor y de propiedad intelectual sobre las obras creadas por los(as) funcionarios(as), contratistas y terceros en cumplimiento con sus obligaciones constitucionales y legales a su cargo, las cuales sonde propiedad de la Empresa; así mismo con la prevención de actos fraudulentos y de piratería, por lo cual establece lineamientos de carácter obligatorio que con su aplicación y cumplimiento por parte de funcionario(as), empleados(as) y contratistas de la empresa, contribuirán a prevenir la materialización de riesgos por acciones voluntarias o involuntarias que conllevarían a cometer acciones que violen los derechos de autor y de propiedad intelectual, el fraude y la piratería, afectando la seguridad de la información y/o la imagen institucional como también se podría incurrir en posibles perjuicios para las personas, o para INDUSTRIAS MORARBE S.A.S., lo que conllevaría a sanciones legales, económicas o penales.

Lineamientos generales

➢La empresa implementará los controles necesarios que contribuyan al cumplimiento de la normatividad legal vigente relacionada con los derechos de autor y de propiedad intelectual.

➢ INDUSTRIAS MORARBE S.A.S. deberá adquirir el software de carácter licenciado a nombre de la empresa, mantenerlo y almacenarlo en sitio seguro con un registro y/o inventario de las respetivas licencias para efectos de auditoría y control.

➢ El desarrollo de software adquirido por INDUSTRIAS MORARBE S.A.S. a terceras partes o realizado por contratistas y/o funcionarios(as) y empleados(as) de la empresa, será de uso exclusivo de la empresa y debe ser registrado a nombre de INDUSTRIAS

MORARBE S.A.S. ante las entidades competentes, con el fin de proteger los derechos de autor y/o de propiedad intelectual.

➢ Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite el autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

➢ Cuando el personal de soporte técnico de la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC encuentre programas instalados sin autorización en los equipos de la empresa, procederá con la desinstalación inmediata de los mismos.

➢ Las licencias de uso de software estarán bajo custodia de la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas, dispositivos, etc.), que acompañen a las versiones originales de software.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones - DTIC es la única dependencia autorizada para realizar copia de seguridad del software original de INDUSTRIAS MORARBE S.A.S.; cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización puede conllevar a las sanciones administrativas y legales pertinentes.

➢ El software adquirido o desarrollado por INDUSTRIAS MORARBE S.A.S., no puede ser copiado o suministrado a terceros sin la debida autorización de la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC y/o, sin que se suscriba algún tipo de contrato o convenio por parte de INDUSTRIAS MORARBE S.A.S. y el tercero.

➢ Se prohíbe el uso e instalación de juegos y/o software que aun siendo libre o gratuito no esté autorizado por la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC para su uso.

➢ No está permitido almacenar archivos de música, videos o cualquier otro elemento que requiera para su uso de una licencia relacionada con derechos de autor o de propiedad intelectual, patentes o similares.

➢ Los(as) funcionarios(as), empleados (as) contratistas o terceros responsables de la publicación de la información en los sitios Web e Intranet de la empresa, deberán atender el cumplimiento a las normas vigentes en materia de propiedad intelectual y demás políticas establecidas en la empresa, y bajo ninguna circunstancia deben publicar información sensible, reservada o confidencial que se encuentre en poder de INDUSTRIAS MORARBE S.A.S.

➢ La empresa efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual registro de auditoria.

➢ La Dirección de Tecnologías de la Información y las Comunicaciones DTIC podrá autorizar el uso de material o software declarado como de uso libre, el producido por ella misma o el producido por el titular o propietario externo cuando medie autorización de este, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente; para esto la Dirección de Tecnologías de la Información y las Comunicaciones - DTIC se asegurará que el software cumpla con los requisitos mínimos de seguridad y licenciamiento para su uso.

➢ Todo desarrollo de software deberá contener estándares mínimos de seguridad en el código fuente, también contará con métodos de encriptación que no permita ser visible fácilmente por medio de navegadores.

➢Todo desarrollo de software interno o propiedad de la PB deberá tener manuales técnicos y de usuarios al igual que un repositorio del código y los ambientes de desarrollo, pruebas y producción.

7.14.2. Revisiones de seguridad de la información

Lineamientos generales

➢La Dirección de Tecnologías de la Información y las Comunicaciones DTIC, verificará permanentemente el cumplimiento de los controles, procedimientos y directrices establecidos en el Sistema de Gestión de Seguridad de la Información – SGSI de INDUSTRIAS MORARBE S.A.S., y velará por el cumplimiento de las políticas establecidas en el presente manual.

7.15. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La política de protección de datos personales en virtud de lo consagrado en la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013 y el Decreto 1074 de 2015 aplicado a todo dato personal que hayan sido suministrado o que se suministre a INDUSTRIAS MORARBE S.A.S., aplica y da cumplimiento a la normatividad vigente en materia de protección de datos de carácter personal.

Lineamientos generales

➢El responsable del tratamiento de datos personales es INDUSTRIAS MORARBE S.A.S.

- Los(as) funcionarios(as) y contratistas de INDUSTRIAS MORARBE S.A.S., deben, observar, acatar y cumplir las órdenes e instrucciones de carácter legal que aplica la empresa respecto al manejo de los datos de carácter personal cuya divulgación o indebido uso pueda generar un perjuicio a los usuarios, en cumplimiento de los derechos contenidos en el artículo 15 de la Constitución Política de Colombia, Ley 1266 de 2008, Ley 1273 de 2009, Ley 1581 de 2012, Decreto Reglamentario 1377 de 2013, Decreto 1074 de 2015 y demás disposiciones complementarias.

7.15.1. Alcance de la Política de Protección de Datos Personales

La política de protección de datos personales, se aplicará a todas las bases de datos y/o archivos que contengan datos personales que sean objeto de tratamiento por parte de INDUSTRIAS MORARBE S.A.S., incluso aquella información que haya sido obtenida o recolectada con anterioridad a la Ley 1581 de 2012 y cualquier otro dato que sea susceptible de ser tratado por INDUSTRIAS MORARBE S.A.S.

7.15.2. Tratamiento de los datos personales por parte de INDUSTRIAS MORARBE S.A.S.

INDUSTRIAS MORARBE S.A.S., en el desarrollo de su misión, actúa como responsable y/o encargado del tratamiento de datos personales que se encuentren en sus bases de datos. En consecuencia, podrá solicitar, consultar, compartir, informar, reportar, procesar, modificar, actualizar, aclarar, compilar, sustraer, ofrecer, enviar, intercambiar, adquirir, retirar, divulgar, obtener, transferir, transmitir, almacenar, utilizar, recolectar, usar, circular, suprimir, en general y en adelante, dar tratamiento, a datos personales de las personas que requieren servicios propios de INDUSTRIAS MORARBE S.A.S., funcionarios(as),empleados (as) contratistas y proveedores.

7.15.3. Efectos de la Autorización

Para todos los efectos, se entiende que la autorización por parte de los titulares a favor de INDUSTRIAS MORARBE S.A.S., para el suministro y/o tratamiento de sus datos personales, realizada a través de sus sitios web o por medio de cualquier canal adicional, físico, telefónico, electrónico, o personal, implica el entendimiento y la aceptación plena de todo el contenido de la presente política y de manera voluntaria, el

titular y/o sus representantes, según sea el caso, le concede(n) a INDUSTRIAS MORARBE S.A.S., su autorización para que utilice dicha información personal conforme a las estipulaciones mencionadas.

7.15.4. Autorización

El usuario declara haber recibido explicación o haber o consultado la presente política, obligándose a leerla, conocerla y consultarla en desarrollo del derecho que le asiste como titular de datos personales, sin perjuicio de haber recibido de parte de INDUSTRIAS MORARBE S.A.S., una clara, cierta y adecuada ilustración respecto de la misma, la cual además se ha puesto a su disposición en la página web de INDUSTRIAS MORARBE S.A.S., www.morarbe.com.co; en consecuencia, el usuario manifiesta que acepta en su integridad la presente política, y autoriza a INDUSTRIAS MORARBE S.A.S., para que obtenga y le de tratamiento a sus datos personales de acuerdo con los siguientes parámetros de uso:

Si el usuario no está de acuerdo con la presente política, no podrá suministrar información alguna que deba registrarse en una de las bases de datos de INDUSTRIAS MORARBE S.A.S., por tanto, dicho usuario, deberá abstenerse de hacer uso de los servicios que ofrece la Empresa que haga necesario el suministro de información por parte suya.

INDUSTRIAS MORARBE S.A.S., mantiene parámetros de seguridad y buen uso de los datos personales apropiados y acordes con la normativa que le rige como empresa pública, en consecuencia, les dará a los mismos los usos adecuados para mantener la confidencialidad requerida de acuerdo con lo establecido en esta política y en la legislación vigente.

Los datos personales tratados por INDUSTRIAS MORARBE S.A.S., podrán ser transferidos o transmitidos a Entidades que contribuyan directa o indirectamente para llevar a cabo los usos y finalidades autorizadas por los usuarios para el desarrollo de las funciones propias de la Empresa, y prestar los servicios que puedan cumplir con la misión; en todo caso, dicha información se conservará bajo estricta confidencialidad y será sometida a un tratamiento riguroso, respetando los derechos y las garantías del ciudadano, de conformidad con lo previsto en la ley.

INDUSTRIAS MORARBE S.A.S., podrá utilizar proveedores de servicios y/o procesadores de datos que trabajen en su nombre, incluyendo, contratistas, delegados, outsourcing, tercerización o aliados, con el objeto de desarrollar servicios de alojamientode sistemas, de mantenimiento, servicios de análisis, servicios de mensajería por email, servicios de entrega, entre otros. En consecuencia, el usuario entiende y acepta que mediante la presente autorización faculta a estos terceros, para acceder a su información personal, en la medida en que así lo requieran para la prestación de sus servicios. Sin perjuicio de lo anterior, se precisa que tanto los(as) funcionarios(as) y contratistas de la empresa como las Entidades competentes protegen en todos los casos la confidencialidad de la Información personal a su cargo.

INDUSTRIAS MORARBE S.A.S., podrá recolectar información que se encuentre en el dominio público para crear o complementar sus bases de datos. A dicha información sele dará el mismo tratamiento señalado en la presente política, con las salvedades contenidas en la ley.

7.15.5. Finalidades de la autorización

A los datos personales que le sean suministrados a INDUSTRIAS MORARBE S.A.S., se les dará un tratamiento conforme a una o algunas de las siguientes finalidades:

➢ Compartir con las Entidades competentes la información, para el desarrollo de sus funciones o para complementar o enriquecer la prestación de los servicios de INDUSTRIAS MORARBE S.A.S.

➢Dar tratamiento en medios físicos, digitales o por cualquier medio, asegurando el correcto registro y la utilización de las páginas web de INDUSTRIAS MORARBE S.A.S.

➢ Registrar y administrar dentro de sus bases de datos la información adquirida en virtud de la relación existente entre el usuario y INDUSTRIAS MORARBE S.A.S., de acuerdo a la naturaleza jurídica de dicha relación (laboral, civil, comercial, etc).

➢Prevenir y detectar el fraude, así como otras actividades ilegales.

7.15.6. Información personal recolectada

La información personal que lINDUSTRIAS MORARBE S.A.S.., puede recolectar y someterá tratamiento es la siguiente:

• Nombre completo del titular de la información.

- • Identificación.
- Fecha de nacimiento.
- Domicilio.
- • Dirección para notificación.
- • Teléfonos de contacto.
- • Correo electrónico.
- • Identidad de género.
- • Actividad económica
- • Profesión
- • Nivel de estudios
- • Estrato

7.15.7. Deberes de INDUSTRIAS MORARBE S.A.S. cuando actúe como responsable del tratamiento

Sin perjuicio de lo contenido en la ley, son deberes de INDUSTRIAS MORARBE S.A.S.,en calidad de responsable del tratamiento, los siguientes:

➢ Garantizar al ciudadano, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
➢ Solicitar y/o conservar la respectiva autorización otorgada por el titular.
➢ Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
➢ Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
➢ Garantizar que la información a la que se le de tratamiento, sea veraz, completa, exacta, actualizada, comprobable y comprensible. Rectificar si es del caso.
➢ Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
➢ Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
➢ Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
➢ Informar a solicitud del titular sobre el uso dado a sus datos.
➢Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información del titular.

7.15.8. Derechos del Titular de la información personal

El titular de la información personal suministrada a INDUSTRIAS MORARBE S.A.S., tendrá los siguientes derechos:

➢ Conocer, actualizar y rectificar su información personal gratuitamente.
➢ Solicitar prueba de la existencia de la autorización otorgada a INDUSTRIAS MORARBE S.A.S.
➢ Ser informado respecto al uso que se le ha dado a su información personal.
➢ Revocar la autorización y solicitar la supresión de los datos cuando no se haga un uso conforme a los usos y finalidades autorizados.
➢ Presentar consultas y reclamos referentes a la información personal.
➢Acceder de forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

7.15.9. Seguridad de la información y reserva de la información personal

➢ La información personal no será destinada a uso o finalidades distintas a las establecidas en la presente política, razón por la cual INDUSTRIAS MORARBE S.A.S., procurará proteger la privacidad de la información personal y conservarla bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como el respeto de los derechos del titular, según lo estipulado en la ley.
➢ La INDUSTRIAS MORARBE S.A.S., se encuentra eximida de responsabilidad, frente a las obligaciones adquiridas a través del presente aviso de privacidad, cuando por cualquier circunstancia una autoridad competente solicite que sea revelada la información personal, para actuaciones judiciales o administrativas vinculadas a cualquier tipo de obligación, proceso, investigación, persecución, o actualización de datos o acción de interés público.
➢La presente política permanecerá mientras el dato se encuentre en las bases de datos de INDUSTRIAS MORARBE S.A.S., y no sea de dominio público.

7.15.10.Tratamiento de datos personales de menores de edad

➢ En aplicación de lo establecido en la ley, INDUSTRIAS MORARBE S.A.S., procederá a efectuar el tratamiento de la Información personal; de niños, niñas y adolescentes,

respetando el interés superior de los mismos y asegurando, en todos los casos, el respeto de sus derechos fundamentales y garantías mínimas.

➢ En todos los eventos en los que se requiera dar tratamiento a la información personal de menores de edad, INDUSTRIAS MORARBE S.A.S., obtendrá la autorización de sus representantes legales, que para este efecto son el padre y/o madre o tutor.

7.15.11.Consulta, rectificación y reclamos

➢ **Consulta:** Las consultas y solicitudes deben ser dirigidas por el titular a través de cualquier medio y a cualquiera de los contactos que se señalan más adelante, y serán atendidas en los términos establecidos por la ley y la respuesta podrá ser entregada por cualquier medio físico o electrónico.

➢ **Rectificaciones y Reclamos:** Cuando el titular de la información o sus causahabientes consideren que su información debe ser corregida, actualizada o suprimida, o cuando adviertan un presunto incumplimiento por parte de INDUSTRIAS MORARBE S.A.S., de sus deberes en materia de protección de datos personales contenidos en la legislación aplicable y en la presente política de privacidad, podrán presentar un reclamo de la siguiente manera:

➢ Presentar solicitud escrita frente al requerimiento específico.

➢INDUSTRIAS MORARBE S.A.S.., resolverá el reclamo en los términos establecidos por la ley, por cualquier medio físico o electrónico y en la dirección de notificación que haya incluido en el respectivo reclamo.

8. NORMATIVIDAD APLICABLE

- Ley 23 de 1982, Congreso de la República. Aplicable Toda la norma
- Ley 1266 de 2008, Congreso de la República. Aplicable Toda la norma
- Ley 1273 de 2009, Congreso de la República. Aplicable Toda la norma
- Ley 1581 de 2012, Congreso de la República. Aplicable Toda la norma
- Ley 1712 de 2014, Congreso de la República. Aplicable Toda la norma
- Decreto 2573 de 2014, Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Aplicable Toda la norma
- Decreto 1074 de 2015, Ministerio de Tecnologías de laInformación y las Comunicaciones de Colombia. Aplicable Capítulo 25, 26

- Decreto 1078 de 2015, Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Aplicable Título 9, Capítulo 1
- Decreto 1008 de 2018 Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. Aplicable Toda la norma
- Norma técnica colombiana NTC-ISO 31000 de 2011. Information Technology Security Techniques. Aplicable Toda la norma
- Norma técnica colombiana NTC-ISO- IEC 27001 de 2013, Information Technology Security Techniques. Aplicable Toda la norma
- Documento CONPES Política Nacional de Seguridad Digital 3854 de 2016. Consejo Nacional de Política Económica y social - CONPES aplicable Toda la norma

9. ANEXOS

- Política general de seguridad de la información
- Política controles en la red de datos y transferencia de Información
- Política de backups
- Política de dispositivos móviles
- Política de teletrabajo
- Política de derechos de propiedad intelectual, antipiratería y antifraude
- Política de escritorio y pantalla limpia
- Política de Trabajo en casa

Registro de aprobación
Elaboró : JULIANA CANO DE BEDOUT. Cargo: Jefe ÁREA JURIDICA
Revisó: LORENA MARIA GÓMEZ. Cargo REVISORIA FISCAL
Aprobó: JORGE IVAN MORALES. Cargo: GERENTE

JORGE IVAN MORALES
Representante Legal