TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el contexto actual, la información se ha convertido en uno de los activos más valiosos para cualquier organización. **[NOMBRE DE LA EMPRESA]** reconoce la importancia crítica de la información que gestiona y es plenamente consciente de las amenazas a las que está expuesta, así como de las implicaciones contractuales y legales derivadas de no implementar las medidas necesarias para su protección.

Por lo tanto, la empresa debe tener una visión integral de los riesgos que pueden comprometer la seguridad o la privacidad de la información que maneja. Lo anterior, con el propósito de establecer controles efectivos que minimicen dichos riesgos y aseguren la integridad, disponibilidad y confidencialidad de la información propia, así como la información confiada por las partes interesadas.

El presente documento tiene como fin establecer los lineamientos que orientarán los procesos, procedimientos y actuaciones para garantizar la seguridad de la información, mediante la formulación de una “política y lineamientos de seguridad de la información” general y de políticas específicas relacionadas, estableciendo un marco estructurado para la protección de la información a lo largo de su ciclo de vida.

2. OBJETIVO GENERAL

Establecer las políticas de seguridad de la información, dentro de la implementación de un Sistema Integrado de Seguridad de la Información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información de **[NOMBRE DE LA EMPRESA]**

Por lo que este manual proporciona directrices claras y específicas para proteger la información a lo largo de su ciclo de vida, asegurando que se implementen controles adecuados para mitigar riesgos y cumplir con las obligaciones legales y contractuales.

2.1. OBJETIVOS ESTRATEGICOS

En concordancia con los requisitos de la Norma **ISO/IEC 27001:2022** y las directrices de la **ISO/IEC 27002:2022**, **[NOMBRE DE LA EMPRESA]** establece los siguientes objetivos estratégicos para el Sistema de Gestión de Seguridad de la Información (SGSI):

1. **Garantizar la confidencialidad, integridad y disponibilidad de la información**, asegurando que el acceso, uso, modificación y disponibilidad de los activos de información se gestione de manera controlada y autorizada.
2. **Cumplir con los requisitos legales, regulatorios, contractuales y normativos aplicables**, en especial lo dispuesto por la normativa colombiana de protección de datos personales y la normativa internacional en seguridad de la información.
3. **Gestionar los riesgos de seguridad de la información**, mediante procesos de identificación, análisis, evaluación y tratamiento que reduzcan vulnerabilidades y prevengan incidentes.
4. **Fortalecer la cultura de seguridad en todos los niveles de la organización**, a través de procesos de sensibilización, capacitación continua y promoción de conductas seguras en el uso de la información y los sistemas tecnológicos.
5. **Asegurar la continuidad del negocio y la resiliencia organizacional**, implementando planes de respuesta ante incidentes y mecanismos de recuperación que reduzcan el impacto de interrupciones en la operación.
6. **Promover la mejora continua del SGSI**, mediante la evaluación periódica del desempeño, la revisión de políticas y controles, y la incorporación de lecciones aprendidas de auditorías e incidentes.
7. **Optimizar el uso de recursos tecnológicos y humanos**, alineando la seguridad de la información con los objetivos estratégicos del negocio y asegurando un equilibrio entre protección, eficiencia y productividad.

3. ALCANCE

Estas políticas y lineamientos son de cumplimiento obligatorio para todos los miembros de **[NOMBRE DE LA EMPRESA]**, así como por terceros que interactúen con la empresa en la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información. Son aplicables a toda la información creada, procesada, almacenada y utilizada en el desarrollo de las actividades operacionales de la empresa. Este manual

abarca todas las fases del ciclo de vida de la información, asegurando su protección integral.

4. VIGENCIA, REVISIÓN Y ACTUALIZACIÓN

La vigencia del presente documento de Políticas y Lineamientos de Seguridad de la Información aplica a partir de su aprobación por la Presidencia y su publicación en el Sistema Integrado de Gestión de la empresa **[NOMBRE DE LA EMPRESA]**

La revisión del contenido del manual deberá realizarse periódicamente, como mínimo una vez cada dos años o cuando se presenten cambios organizacionales, en el entorno operativo de los procesos, o en el entorno tecnológico, así como, cambios en el marco normativo o regulatorio en materia de tecnologías de la información, comunicación, confidencialidad y manejo de la información.

El responsable del área de tecnología, será el responsable de la revisión y actualización del manual de políticas de seguridad y privacidad de la información. Todas las revisiones y actualizaciones deberán ser documentadas y aprobadas por la alta dirección para asegurar el cumplimiento continuo con la norma ISO 27001.

5. REFERENCIAS NORMATIVAS

A continuación, se relacionan leyes y demás regulaciones aplicables en materia de seguridad de la información y que se efectúan como referencias normativas para la creación del presente manual, entre otras:

- **Ley 23 de 1982**: Sobre derechos de autor.
- **Ley 527 de 1999**: Define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales.
- **Ley 603 de 2000**: Modifica el artículo 47 de la Ley 222 de 1995, relacionada con el cumplimiento de normas sobre derechos de autor.
- **Ley 1266 de 2008**: Disposiciones generales del hábeas data y regulación del manejo de información contenida en bases de datos personales.
- **Ley 1273 de 2009**: Código Penal Colombiano, artículos relacionados con la violación de derechos de autor y mecanismos de protección.
- **Ley 1581 de 2012**: Disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014**: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Ley 1928 de 2018**: Aprueba el “Convenio sobre la Ciberdelincuencia”.
- **Decreto Reglamentario 1377 de 2013:** Disposiciones generales para la protección de datos personales.
- **Decreto 1081 de 2015:** Protección y tratamiento de datos personales.

6. GLOSARIO

Se adoptan los términos y definiciones de la familia de normas técnica ISO 27000 vigentes, y de los estándares que se apliquen, descritos a continuación:

- **Acceder**: Acción de autenticarse dentro de un sistema de información o red de datos, logrando el uso de algún recurso o servicio disponible.
- **Acceso**: Posibilidad de ingresar o registrarse en un sistema de información.
- **Activo**: Cualquier cosa que tiene valor para la organización, incluyendo información, software, hardware, servicios, personas y reputación.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Anonimizar**: Proceso mediante el cual la información de identificación personal se modifica de manera irreversible para que no se pueda identificar, directa o indirectamente, a la persona asociada a dicha información, ya sea por sus propios medios o en colaboración con terceros.
- **Autenticación**: Proceso de verificar la identidad de un usuario, proceso o dispositivo, a menudo como condición previa para permitir el acceso a recursos en un sistema de información.
- **Autorización**: Proceso de conceder o denegar permisos a un usuario, proceso o dispositivo para acceder a recursos específicos en un sistema de información.
- **Back up**: Copia de seguridad o respaldo de datos, realizada para prevenir la pérdida de información en caso de fallos del sistema o incidentes de seguridad.
- **Confidencialidad**: Propiedad de la información que asegura que solo las personas autorizadas tienen acceso a ella y se mantiene de forma reservada o secreta.
- **Control de Usuario**: Procedimiento de control para la validación de los privilegios de acceso y uso de los usuarios.
- **Credenciales**: Información, normalmente compuesta por un nombre de usuario y una contraseña, que permite el acceso a una red de información a través de equipos de cómputo, un sistema informático o servicio.
- **Disponibilidad**: Propiedad de la información que asegura que está accesible y utilizable cuando se requiere.
- **Información Corporativa**: Toda aquella información que se produce, recibe, administra, envía y almacena, y que sirve para el desarrollo de las actividades en todos los procesos de negocio.
- **Infraestructura:** sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización Incidente de seguridad de la información
- **Integridad**: Propiedad de la información que asegura que es precisa y completa, y que no ha sido alterada de manera no autorizada.
- **Internet**: Red de redes que permite la interconexión descentralizada de computadoras a través de un conjunto de protocolos denominados para la conectividad.
- **Intransferible**: Por su naturaleza confidencial, no permite ser entregado en su conjunto para ser usado por personas diferentes al propietario.
- **Mejora continua.** Actividad recurrente para mejorar el desempeño
- **Monitoreo:** Determinar el estado de un sistema, un proceso o una actividad. Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.
- **Partes Interesadas**: Terceros que pueden representar un interés en el contexto de la organización, como proveedores y entes de control.
- **Permisos**: Niveles de acceso y posibilidades de actuar, enmarcados en roles que se asignan al usuario dentro de un sistema informático.

- **Propietario de cuenta**: Persona o usuario a quienes les ha sido asignada una cuenta de acceso dentro de una red corporativa o un sistema de información.
- **Red**: Estructura que permite la transmisión de información entre equipos de cómputo dentro de las organizaciones.
- **Restaurar**: Acción de disponer para su uso una información contenida en un back up, copia de seguridad o respaldo.
- **Retención**: Período de tiempo definido para la conservación de una colección de datos en un almacenamiento definido.
- **Roles**: Conjunto de permisos estándar generalizados que se asocian a un usuario en particular.
- **Seguridad de la Información**: Prácticas de seguridad enfocadas a la protección de la información mediante el uso de herramientas tecnológicas de hardware, software, procesos y procedimientos dentro de las organizaciones.
- **Seguridad Informática**: Implementación de herramientas de seguridad, normalmente perimétricas, para mantener el control de la infraestructura tecnológica empresarial y proteger la información.
- **Sistema de Información**: Software disponible para el procesamiento de información empresarial.
- **Software**: Conjunto de instrucciones de código que materializan un producto informático para desarrollar tareas previamente programadas.
- **Usuario**: Persona con privilegios dentro de la infraestructura tecnológica empresarial para el acceso a la información y el uso de servicios disponibles.

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El presente documento representa la posición de la administración de **[NOMBRE DE LA EMPRESA]** con respecto a la protección de los activos de información (colaboradores, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la empresa y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

[NOMBRE DE LA EMPRESA] para asegurar la dirección estratégica de la empresa, establece la compatibilidad de la política de seguridad de la información con el fin de:

- Minimizar el riesgo de los procesos misionales de la empresa.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de eficiencia y eficacia administrativa.
- Mantener la confianza de los colaboradores, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores, terceros, y clientes de **[NOMBRE DE LA EMPRESA]**
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a la empresa **[NOMBRE DE LA EMPRESA],** sus colaboradores, contratistas, terceros y en general a las partes interesadas.

Nivel de cumplimiento

- Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación, se establecen las 12 políticas de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de **[NOMBRE DE LA EMPRESA]**

1. **[NOMBRE DE LA EMPRESA]** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios que le aplican por su naturaleza.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los colaboradores de **[NOMBRE DE LA EMPRESA],** contratistas y terceros.

3. **[NOMBRE DE LA EMPRESA],** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

4. **[NOMBRE DE LA EMPRESA],** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de medidas de control, de acuerdo con la clasificación de la información de su propiedad o en custodia.

5. **[NOMBRE DE LA EMPRESA],** protegerá su información de las amenazas originadas por parte del personal.

6. **[NOMBRE DE LA EMPRESA],** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. **[NOMBRE DE LA EMPRESA],** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. **[NOMBRE DE LA EMPRESA],** implementará control de acceso a la información, sistemas y recursos de red.

9. **[NOMBRE DE LA EMPRESA],** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. **[NOMBRE DE LA EMPRESA],** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. **[NOMBRE DE LA EMPRESA],** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

12. **[NOMBRE DE LA EMPRESA],** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad, Ciberseguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la empresa **[NOMBRE DE LA EMPRESA],** incluyendo lo establecido en el marco legal colombiano en cuanto a Seguridad y Privacidad de la Información se refiere.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD, CIBERSEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8.1. POLÍTICA DE ORGANIZACIÓN INTERNA

La empresa **[NOMBRE DE LA EMPRESA],** establece los siguientes lineamientos a seguir en cuanto a la organización de la seguridad de la información:

- **Estructura Organizacional:** Se debe establecer una estructura organizacional que permita definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI). La estructura debe incluir roles específicos para la gestión de la seguridad de la información y asegurar que todos los niveles de la organización estén involucrados.
- **Funciones y Responsabilidades:** Todos los involucrados por el alcance de la presente política deben tener funciones y responsabilidades claras frente al SGSI y los activos de la información bajo su responsabilidad. Esto incluye la designación de un responsable de seguridad de la información y la definición de roles específicos para la gestión de riesgos y la respuesta a incidentes.
- **Segregación de Funciones:** Se debe mantener la segregación de funciones entre los roles para evitar conflictos de intereses en temas de seguridad de la información. Se debe incluir la separación de tareas críticas para asegurar que ninguna persona tenga control total sobre todos los aspectos de cualquier función crítica.

    - **Controles de seguimiento y monitorización:** Establecer controles de supervisión de las actividades para asegurar que se realizan correctamente.
    - **Controles de auditorías:** Implementar controles mediante registros que revelen los datos necesarios en las auditorías periódicas para evaluar posibles violaciones de seguridad. Aumentar la frecuencia de las auditorías en temas sensibles para transmitir la continuidad en la vigilancia de la seguridad de la información.
    - **Registros automatizados:** Registrar automáticamente los cambios, accesos o tareas sensibles relacionadas con la seguridad de la información,

como la asignación de permisos, contraseñas o modificaciones en aplicaciones de desarrollo.

- **Contacto con Autoridades y Grupos de Interés:** Cuando sea conveniente, se podrá autorizar el intercambio de información sobre amenazas informáticas y se podrá establecer contacto con autoridades y grupos de interés relevantes para asegurar el cumplimiento de las normativas y la colaboración en caso de incidentes de seguridad.
  En caso de presentarse incidentes de seguridad de la información, es necesario mantener informados a los organismos de control del Estado.

  - Ante la Superintendencia de Industria y Comercio cuando el incidente tiene relación con protección de datos personales.
  - Ante la Fiscalía general de la Nación cuando el incidente de seguridad de la información constituye delito informático.
  - Ante el centro de respuesta de incidentes la Policía Nacional (CSIRT PONAL) cuando se requiera apoyo en el tratamiento de evidencias forenses de delitos informáticos.

- **Gestión de Proyectos:** Los proyectos que se ejecuten deben estar alineados con la Política de Seguridad de la Información. Durante el ciclo de vida de los proyectos, se deben establecer objetivos claros y gestionar los riesgos de seguridad de la información de manera proactiva.

  - **Objetivos de seguridad:** Determinar los objetivos para preservar la confidencialidad, integridad y disponibilidad de la información relacionada o afectada por el proyecto.
  - **Celebración de contratos:** Los contratos, convenios que se suscriban entre **[NOMBRE DE LA EMPRESA] y** terceros / contratistas deben incluir la gestión de riesgos de seguridad de información, ciberseguridad y protección de datos.
  - **Evaluación de riesgos:** En caso de que aplique los contratos y/o proyectos de tecnología de información deberán ser sujetos de evaluación de riesgos de seguridad de la información en la fase de diseño o planificación del proyecto para identificar y ponderar los riesgos asociados a la seguridad de la información. 1. Identificar posibles requerimientos de seguridad de la información que deberían ser evaluados como requisitos del proyecto. 2. Identificar riesgos asociados a derechos de propiedad intelectual y licencias de uso de tecnologías de código abierto, framework de desarrollo, módulos de terceros y requisitos de licenciamiento de uso software propietario. 3. Identificar riesgos de seguridad de la información asociados a la protección de datos personales que podrían estar incluidos en el proyecto. 4. Identificar riesgos de ciberseguridad asociados a tecnologías no probadas o en etapas iniciales de desarrollo.
  - **Acuerdos de confidencialidad:** Los proyectos deben considerar la suscripción de acuerdos de confidencialidad y no divulgación sobre la información a la que puedan tener acceso los contratistas y/o terceros responsables de la ejecución del proyecto.

- **Controles de seguridad:** Establecer los controles necesarios para mitigar los riesgos identificados.
- **Proceso de seguridad de la información:** Documentar un proceso para integrar la seguridad de la información en cualquier proyecto, basado en las lecciones aprendidas.

- **Teletrabajo:** Se dispondrán de herramientas y controles necesarios para proteger la confidencialidad, integridad y disponibilidad de la información en los procesos llevados a cabo mediante conexiones remotas. Se debe establecer un procedimiento para la autorización y control del teletrabajo, asegurando que la información accedida remotamente solo se use para fines laborales y, en lo posible, evitar guardarla en los equipos personales.

  En **[NOMBRE DE LA EMPRESA]**, existen dos modalidades para el teletrabajo: el aprovisionamiento de equipos por parte de la empresa y la autorización de uso de equipos personales. En los proyectos que lo requieren por razones de seguridad de la información, la empresa proporcionará el equipo de trabajo necesario.

  El empleado que acceda al teletrabajo se compromete a:

  - Acceder a los diferentes entornos y activos informáticos de **[NOMBRE DE LA EMPRESA]**, respetando la normativa vigente en materia de derechos de autor y protección de datos personales.
  - Utilizar la información a la que tenga acceso única y exclusivamente para cumplir con sus funciones.
  - Cumplir con las medidas de seguridad adoptadas por **[NOMBRE DE LA EMPRESA]** para asegurar la confidencialidad, disponibilidad e integridad de los activos de información institucionales.
  - No ceder en ningún caso a terceras personas la información a la que tenga acceso, ni siquiera para su conservación.

  Para garantizar la conexión segura a los activos de información de **[NOMBRE DE LA EMPRESA]**, el empleado que acceda al teletrabajo se compromete a:

  - Realizar las conexiones remotas a las redes de **[NOMBRE DE LA EMPRESA]** mediante conexión VPN.
  - Utilizar software contra código malicioso en la estación de trabajo usada para el teletrabajo.
  - Contar con un navegador de internet actualizado.
  - Contar con software de ofimática licenciado y actualizado.

  En el caso de que el empleado utilice su propio equipo para el teletrabajo, se aplicarán las siguientes condiciones adicionales:

  - El dispositivo personal debe tener instalado software con licencia para protección contra software malicioso.
  - El dueño del dispositivo personal es responsable de mantener actualizado el sistema operativo y el software de su equipo, aplicando las actualizaciones

de seguridad recomendadas por los fabricantes del sistema operativo y las aplicaciones instaladas.
- Todo dispositivo personal autorizado para manejar información de **[NOMBRE DE LA EMPRESA]** debe cumplir con las normativas vigentes sobre el uso de software legal. El usuario es completamente responsable de asegurarse de que todo el software en su dispositivo esté debidamente licenciado.
- No se permite almacenar información confidencial en equipos de cómputo que sean propiedad de los empleados.

- **Uso de Dispositivos Personales (BYOD):** El uso de dispositivos personales por colaboradores, contratistas o terceros para actividades laborales debe ser verificado por el área de tecnología.

  - Cualquier dispositivo personal autorizado para conectarse a las redes de datos de **[NOMBRE DE LA EMPRESA]** debe tener instalado software con licencia para protección contra software malicioso.
  - El dueño del dispositivo personal es responsable de mantener actualizado el sistema operativo y el software de su equipo, aplicando las actualizaciones de seguridad recomendadas por los fabricantes del sistema operativo y las aplicaciones instaladas.
  - Las conexiones remotas a las redes de **[NOMBRE DE LA EMPRESA]** desde dispositivos personales deben realizarse mediante conexiones VPN.
  - Todo dispositivo personal autorizado para manejar información de **[NOMBRE DE LA EMPRESA]** debe cumplir con las normativas vigentes sobre el uso de software legal. El usuario es completamente responsable de asegurarse de que todo el software en su dispositivo esté debidamente licenciado.
  - No se permite almacenar información confidencial en equipos de cómputo que sean propiedad de los empleados.

8.2. POLÍTICA DE SEGURIDAD DEL TALENTO HUMANO

La empresa **[NOMBRE DE LA EMPRESA]**, dentro de la gestión del talento humano tendrá en cuenta:

8.2.1. Antes del ingreso:

- El área de talento humano de **[NOMBRE DE LA EMPRESA],** debe contar con un procedimiento para la incorporación de personal, en el cual se verifique la información suministrada por el aspirante y sus antecedentes.

  - Comprobar la veracidad del currículum vitae del postulante.
  - Comprobar el nivel académico y experiencias profesionales declaradas.
  - Comprobar de forma independiente la identidad.
  - Comprobaciones de antecedentes penales etc.
  - Comprobar si existen referencias tanto en el ámbito profesional como en el personal.

  - Comprobar si tiene la capacitación necesaria para desempeñar sus funciones.
  - Verificar en lo posible el perfil del candidato en relación con su confiabilidad si va a desempeñar una tarea sensible para la organización en materia de Seguridad de la Información

- Se debe proteger la confidencialidad, integridad y disponibilidad de la información suministrada por los candidatos, así como, la información de hojas de vida y expedientes laborales de los colaboradores.
- El colaborador de **[NOMBRE DE LA EMPRESA],** debe firmar la autorización de manejo de datos personales de acuerdo a lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
- Se deben incorporar cláusulas de confidencialidad en los contratos que se elaboren en **[NOMBRE DE LA EMPRESA],** para la contratación de personal, así como los de prestación de servicios.

8.2.2. Durante su permanencia en el empleo:

- El Área de tecnología diseñará y ejecutará un plan de concientización de seguridad de la información, de manera permanente, que permita a los incluidos en el alcance de la presente política disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano. El plan de concientización debe incluir la importancia del conocimiento y el cumplimiento de las obligaciones aplicables, responsabilidad de las acciones, buenas prácticas para el aseguramiento de la información y demás procedimientos que se consideren necesarios.
- Es responsabilidad del colaborador informar cualquier incidente o evento que afecte la seguridad de la información al área de tecnología.
- El colaborador se compromete con mantener el escritorio y la pantalla libre de información, con el fin de prevenir el acceso no autorizado, pérdida o daño a la misma, teniendo en cuenta los siguientes lineamientos:

  - Mantener el escritorio limpio, ordenado y, sobre todo, al desatenderlo, no dejar a la mano documentos o medios de almacenamiento extraíbles con información reservada.
  - El escritorio o pantalla del equipo de cómputo deben estar libres de documentos, solo accesos directos a aplicaciones, y en cualquier momento que se deje desatendido el usuario lo debe bloquear usando las teclas *Windows + L*.
  - No desatender los documentos que se envían a imprimir o digitalizar.
  - Al finalizar la jornada los documentos y medios de almacenamiento extraíbles deben quedar resguardados bajo llave.

- El área de talento humano de **[NOMBRE DE LA EMPRESA],** debe contar con un proceso disciplinario formal y comunicado a los empleados para los incumplimientos de la seguridad de la información.
- Demás Políticas de ciberseguridad que comprometan la infraestructura tecnológica de **[NOMBRE DE LA EMPRESA].**

8.2.3. Terminación o cambio de responsabilidades:

- Al término de la relación laboral con **[NOMBRE DE LA EMPRESA],** o por cambio de cargo o funciones, se debe dejar constancia de la información manejada.

- Al término de la relación laboral el área de talento humano debe notificar al área de tecnología para que se proceda a desactivar el usuario, el acceso a los aplicativos y los accesos biométricos.
- Cuando se cambie de cargo o funciones el área de talento humano debe notificar al área de tecnología para que se proceda a actualizar la información del usuario, y se agreguen o se eliminen los permisos de acceso a los servicios y sistemas de información.
- Los deberes y responsabilidades del acuerdo de confidencialidad permanecen aún después de la desvinculación.
- Cambiar o actualizar las responsabilidades en los términos y condiciones del empleo ante cambios de empleo dentro de la organización

8.3. POLÍTICA DE GESTIÓN DE ACTIVOS

La empresa **[NOMBRE DE LA EMPRESA],** teniendo en cuenta la política de seguridad de la información establece directrices para el manejo de los activos de información:

8.3.1. Inventario y propiedad de activos:

- Los activos de información deben ser Identificados, inventariados y clasificados, este inventario y clasificación será revisado y actualizado periódicamente.
- Cada activo de información debe tener un responsable o propietario, el cual será responsable de su uso y protección mientras estén en su custodia ya sea física o electrónicamente. Así mismo, son responsables de informar a los jefes inmediatos de cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración y/o divulgación no autorizados.
- Se contará con un procedimiento de clasificación de la información y se establecerán mecanismos de protección de acuerdo a esta clasificación, incentivando la integridad y confidencialidad de la misma.
- Se establecerá un procedimiento para el uso dispositivos de almacenamiento extraíbles.
- La empresa **[NOMBRE DE LA EMPRESA],** actuará como responsable del tratamiento de los datos personales y los usará solo para las finalidades para las que está facultado, según establece su política de tratamiento de datos personales, los activos de información con datos personales deben cumplir con la Ley 1581 de 2014.

8.3.2. Uso aceptable de los activos de información:

- La información que se genera, procesa, almacena, transfiere o transmite a través de los procesos estratégicos, misionales, de apoyo y de evaluación y mejora en **[NOMBRE DE LA EMPRESA] es** propiedad exclusiva de la empresa.
- Las actividades realizadas con esta información deben estar alineadas con las funciones asignadas a cada empleado.
- El acceso a la información debe realizarse utilizando las credenciales designadas a cada usuario.
- Solo los usuarios autorizados tienen permiso para modificar la información bajo su responsabilidad.
- Todos los empleados y partes interesadas que prestan servicios para **[NOMBRE DE LA EMPRESA]** deben garantizar la integridad, confidencialidad y disponibilidad

de los activos de información a los que tienen acceso, asegurándose de que la información se utilice únicamente para las tareas asignadas.
- Al finalizar la jornada laboral, los usuarios deben apagar los equipos de cómputo que les han sido asignados.

8.3.3. Uso seguro del servicio de internet:

- El acceso a Internet dentro de las instalaciones de **[NOMBRE DE LA EMPRESA]**, debe ser utilizado para la ejecución de tareas asignadas y/o relacionadas con la actividad contratada.
- El servicio de Internet puede ser asignado a quienes desempeñen funciones dentro de **[NOMBRE DE LA EMPRESA]**, ya sea personal interno o partes interesadas responsables de la prestación de servicios. La autorización para que los visitantes utilicen el servicio de Internet debe ser solicitada por los responsables de los procesos o dependencias que reciben la visita (se brindará la red de acceso de internet para visitantes).
- Los servicios de acceso a Internet asignados a cada usuario dependerán de su rol y funciones dentro de la empresa, y deberán estar formal y expresamente autorizados (navegación, descarga o transferencia de archivos, acceso a redes sociales, servicios de noticias, video en línea, etc.).
- El acceso a redes sociales, video en línea, audio u otros servicios no directamente relacionados con la función misional de la empresa solo está permitido a las áreas o procesos cuya misión lo requiera. La empresa se reserva el derecho de suspender estos servicios según las situaciones de riesgo identificadas o reportadas.
- Todos los usuarios del servicio de Internet deben informar al responsable del proceso sobre cualquier contenido no autorizado o sospechoso detectado durante la conexión.
- **[NOMBRE DE LA EMPRESA]** puede supervisar el uso del servicio de Internet para asegurar que se utiliza conforme a las funciones asignadas. En los procesos de verificación del uso adecuado del servicio de Internet, se respetarán los derechos de intimidad y privacidad de los usuarios.
- El acceso a sitios web y la información publicada en Internet puede ser suspendido si se identifican acciones que impliquen:

    - Riesgos para la seguridad de la información, ciberseguridad y protección de datos personales.
    - Ejecución de acciones ilícitas según la normativa legal vigente.
    - Uso del servicio de Internet para actividades personales.
    - Descargar, gestionar o cargar ilegalmente contenidos protegidos por derechos de autor a través de los equipos de la empresa (música, videos, obras literarias, pictóricas, imágenes).
    - Publicación de información que afecte negativamente la imagen de la empresa o sus empleados.
    - Publicar información basada en opiniones, criterios, pronunciamientos y/o posiciones personales presentándola como si fuera compartida y autorizada por toda la empresa.
    - Realizar o fomentar propaganda de productos comerciales o propaganda política.

- Distribuir correos electrónicos y mensajes de spam a través de los equipos de la empresa e Internet. Distribuir mensajes e imágenes acosadoras, violentas, discriminatorias o de odio mediante los equipos de la empresa.
- Publicar información despectiva sobre la empresa, sus propietarios u otros empleados.
- Acceso a servicios de videojuegos, apuestas o entretenimiento en línea.
- Acceso a material pornográfico o a sitios web de contenido para adultos relacionados con desnudos, erotismo o pornografía.
- Acceso a sitios web que fomenten la discriminación por razones raciales, políticas, ideológicas, de género o de cualquier otra índole que contravengan la constitución política de Colombia o los derechos humanos.
- Uso comercial del servicio de Internet de la empresa.
- Espionaje o captura no autorizada del tráfico de datos de las redes de la empresa.
- Ingreso a páginas relacionadas con violencia, pornografía, drogas, alcohol, web proxys, hacking o cualquier sitio web que pueda comprometer la seguridad de la información.
- Intercambiar información de la empresa con terceros sin previa autorización del responsable del proceso.
- Realizar capturas de datos de acceso, contraseñas o cualquier información que circule por la red de la empresa.
- Descifrar cualquier tipo de información de la empresa, como el correo electrónico, en los equipos de la empresa.
- Instalar software inapropiado que pueda ser perjudicial para los equipos y la red en el lugar de trabajo.
- Ejecutar transacciones que consuman recursos informáticos en detrimento de la funcionalidad de los recursos tecnológicos de la empresa.

Para garantizar un uso seguro del servicio de Internet, todos los usuarios deben:

- Verificar que las URL de los sitios web sean seguras y comiencen con https://.
- No seguir enlaces sospechosos en correos electrónicos o sitios web desconocidos.
- Evitar que los navegadores guarden información sensible como contraseñas y datos de tarjetas de crédito.
- Mantener el antivirus del computador habilitado durante la navegación por Internet.
- No instalar software, módulos o librerías anunciados por las páginas web visitadas.
- Si necesita conectarse a una red pública, utilizar una red privada virtual (VPN) para proteger tus datos.

8.3.4. Uso seguro del servicio de correo corporativo:

Los usuarios del servicio de correo electrónico de **[NOMBRE DE LA EMPRESA]** deben seguir estos lineamientos:

- Utilizar la cuenta de correo electrónico corporativo como una herramienta tecnológica exclusiva para el desarrollo de sus funciones laborales.
- Los usuarios autorizados serán responsables de todas las actividades realizadas mediante el uso de sus credenciales de acceso a los buzones de correo corporativo.

- Cumplir con las políticas, reglamentaciones, protocolos, estándares, guías y lineamientos establecidos por la empresa, así como con la normativa legal vigente en aspectos como seguridad de la información, ciberseguridad, privacidad, protección de datos, derechos de propiedad intelectual, confidencialidad y demás normas aplicables al servicio de correo electrónico corporativo.
- Hacer un uso responsable de la cuenta de correo electrónico corporativo y de las herramientas asociadas para las comunicaciones generadas dentro de sus funciones laborales.
- Leer, mantener y responder oportunamente los mensajes recibidos en el buzón de correo corporativo, incluyendo aquellos dirigidos a la carpeta de correos no deseados.
- Mantener la confidencialidad de sus credenciales de acceso (nombre de usuario y contraseña).
- Cambiar la contraseña inicial y cuando se realice un restablecimiento de contraseña, siguiendo los procedimientos establecidos que incluye factor de doble autenticación.
- Los usuarios autorizados son responsables del contenido de sus mensajes de correo electrónico y sus posibles consecuencias. El área de tecnología no controla, censura ni modifica el contenido de los mensajes de los usuarios.
- Utilizar el servicio de correo electrónico exclusivamente para enviar, recibir y reenviar mensajes como comunicación oficial dentro de las actividades laborales, y no para otros fines.
- Usar la dirección de correo electrónico corporativo como contacto oficial.
- Registrarse para participar o iniciar sesión con la cuenta de correo electrónico corporativo en plataformas o servicios corporativos con propósito laboral.
- Informar al área de tecnología sobre fallas de seguridad, piratería informática u otros incidentes detectados en el servicio de correo electrónico corporativo, así como sobre correos electrónicos sospechosos.
- Reportar al área de tecnología cualquier uso no autorizado o si sospechan que su cuenta de correo electrónico corporativo o contraseña están comprometidas.
- En caso de pérdida o robo del dispositivo, el usuario deberá informar inmediatamente al área de Tecnología.

Uso del correo corporativo en otros dispositivos

El acceso al correo corporativo deberá realizarse desde los equipos corporativos suministrados o aprobados por la organización. No obstante, cuando por razones laborales sea necesario acceder desde otros dispositivos electrónicos (como teléfonos móviles, tablets u otros equipos), se deberán cumplir las siguientes condiciones:

- El acceso deberá realizarse únicamente a través de aplicaciones o configuraciones autorizadas por el área de Tecnología.
- No se deberán almacenar ni guardar las contraseñas de acceso al correo corporativo en navegadores o aplicaciones del dispositivo.
- El usuario deberá cerrar la sesión de correo al finalizar su uso, y evitar dejar cuentas abiertas en dispositivos compartidos o de uso personal.
- El usuario será responsable de garantizar la protección de la información corporativa almacenada o visualizada en el dispositivo.
- En caso de pérdida, robo o uso no autorizado del dispositivo con acceso al correo corporativo, el usuario deberá informar de manera inmediata al área de Tecnología.

- El área de Tecnología podrá restringir, revocar o eliminar el acceso al correo corporativo en dispositivos que no cumplan con las condiciones de seguridad establecidas.

Se considera uso no adecuado del correo electrónico institucional de **[NOMBRE DE LA EMPRESA]** las siguientes acciones:

- Enviar, reenviar y recibir correos electrónicos para fines no laborales.
- Utilizar cuentas de correo electrónico personales para emitir comunicaciones oficiales en nombre de la empresa.
- Enviar mensajes o materiales que sean ilícitos, acosen, difamen, insulten o amenacen, o que sean dañinos, vulgares, obscenos o de naturaleza objetable o ilegal.
- Enviar correos electrónicos desde la cuenta de otras personas sin su autorización.
- Enviar mensajes anónimos o que utilicen seudónimos, títulos, cargos o funciones no oficiales.
- Enviar información que infrinja derechos de autor, propiedad intelectual u otras normativas legales aplicables.
- Enviar información confidencial y/o personal de otras personas sin autorización.
- Dejar la sesión de correo electrónico abierta y accesible para personas no autorizadas.
- Enviar deliberadamente mensajes de spam, basura, virus, malware, cartas en cadena o cualquier software malicioso que pueda dañar los sistemas de información de la empresa o de terceros.
- Enviar cadenas de mensajes, comunicaciones, cartas, publicidad o repeticiones excesivas de un mismo mensaje (spamming).
- Registrar o iniciar sesión en sitios web o aplicaciones inseguras o sospechosas.
- Utilizar el correo electrónico institucional para registrarse en redes sociales, plataformas de entretenimiento y otros servicios que no tengan un propósito laboral.
- Crear cuentas de correo electrónico para usuarios no autorizados.
- Solicitar, migrar, eliminar o suspender cuentas de correo electrónico sin la debida justificación y autorización.
- Restablecer contraseñas o iniciar sesión en cuentas de correo electrónico de otros usuarios sin su consentimiento.

8.3.5. Devolución de activos:

- Al finalizar el periodo de utilización, contrato o acuerdo, todos los empleados, contratistas y partes interesadas que posean activos de la organización deben solicitar la firma del paz y salvo de entrega del cargo. Este documento certificará la devolución de todos los activos físicos y electrónicos, así como la finalización de las demás actividades asignadas según la competencia de cada área.
- Realizar la transferencia y el borrado seguro de información en los casos pertinentes.
- Verificación de que todos los activos han sido devueltos en buen estado.

8.3.6. Clasificación de la información:

Los activos de información de **[NOMBRE DE LA EMPRESA]** se clasifican conforme a las siguientes normas legales:

- Ley 1266 de 2008: Disposiciones generales del hábeas data y regulación del manejo de información en bases de datos personales, especialmente financiera, crediticia, comercial, de servicios y de terceros países.
- Ley 1581 de 2012: Disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Ley 1564 de 2012: Código General del Proceso.

Tipo de Información	Valor de Confidencialidad	Fuente Normativa
Información confidencial	Datos que deben mantenerse en secreto y solo ser accesibles a personas autorizadas. Incluye información comercial, contratos, datos de empleados, etc.	Ley 1266 de 2008
Información sensible	Datos que, si se divulgan, pueden causar daño a individuos u organizaciones. Incluye datos personales, financieros, de salud, etc.	Ley 1581 de 2012
Información crítica u organizacional	Datos cuya pérdida o divulgación puede tener un impacto severo en la organización, como secretos comerciales o información estratégica.	Ley 1712 de 2014
Información pública	Datos que pueden ser accesibles por cualquier persona sin restricciones. Incluye información publicada en sitios web oficiales, informes públicos, etc.	Ley 1712 de 2014 en Colombia.

Los resultados de esta clasificación se utilizarán como criterio para asignar el acceso a la información dentro de la empresa y para definir los controles necesarios para proteger la confidencialidad, integridad y disponibilidad de los diferentes activos de información.

La identificación de vulnerabilidades y amenazas es fundamental para salvaguardar la integridad de la información, prevenir incidentes de seguridad, cumplir con regulaciones legales y optimizar el uso de recursos en la gestión de riesgos.

Para el proceso de valoración de cada activo de información identificado, se debe evaluar la criticidad de cada uno de estos, detallando las necesidades específicas en términos de **Confidencialidad, Integridad y Disponibilidad (C.I.D.).**

- **Confidencialidad:** El propósito es identificar los activos que contienen información confidencial y determinar las medidas necesarias para mantener su seguridad. Para ello, se evaluó el nivel requerido para cada activo de información, asegurando que los datos sensibles se protejan adecuadamente contra accesos no autorizados.

- **Integridad:** Se debe valorar el activo identificando el grado de exactitud y completitud que se debe mantener en la información, asegurando que los datos no sean alterados de manera indebida. La evaluación de mecanismos para proteger los datos contra modificaciones no autorizadas y la implementación de controles para verificar la precisión de la información.
- **Disponibilidad:** Se debe valorar determinando el nivel de accesibilidad necesario para los activos de información, aseverando que los datos estén disponibles para los usuarios autorizados cuando los necesiten. Lo anterior, implicó evaluar la infraestructura y los procedimientos necesarios para garantizar que los servicios y datos críticos estén siempre operativos.
- **El Nivel crítico** de cada activo se debe calcular combinando los criterios de Confidencialidad, Integridad y Disponibilidad, proporcionando una medida holística de su importancia y los riesgos asociados, con el fin de priorizar los esfuerzos de mitigación de riesgos.

Los resultados de la clasificación de los activos de información podrán utilizarse como criterio de asignación de acceso a la información, así como para definir los controles para proteger la confidencialidad, integridad y disponibilidad de los diferentes activos de información. La clasificación del activo debe revisarse periódicamente y mantenerse actualizada.

8.3.7. Etiquetado de la información:

- La información debe ser etiquetada de acuerdo al esquema de clasificación que hayamos definido en el apartado anterior.
- Los activos de los sistemas que contienen información clasificada como sensible o crítica deberían llevar una etiqueta adecuada de clasificación.
- El etiquetado de la información clasificada es un requisito clave para acuerdos que impliquen compartir información.

8.3.8. Manejo de los activos y manipulación de soportes:

- Se deben considerar las restricciones de acceso derivadas del nivel de clasificación de los activos.
- Seguir las especificaciones del fabricante para el almacenamiento de los activos.
- No se debe mantener en medios almacenamiento extraíbles información calificada como reservada o clasificada.
- Se debe llevar un control y autorización de traslado de activos físicos.
- Renovar dispositivos periódicamente para evitar la degradación de datos.
- Proteger la información almacenada con copias de seguridad en soportes independientes.
- Evitar la transferencia de información hacia medios extraíbles.

Para garantizar la eliminación segura de información reservada o confidencial, se deben considerar las siguientes alternativas:

1. Sobre escritura: En caso de que el dispositivo no acepte sobreescritura, se debe reinicializar a la configuración de fábrica.

2. Purga: Realiza la desmagnetización del medio, eliminando los datos almacenados mediante la exposición a un campo magnético fuerte.
3. Destrucción física: Evitar cualquier posibilidad de recuperación de datos. Proveer métodos como trituración, incineración, pulverización o desintegración.

8.4. POLÍTICA CONTROL DE ACCESO

Los servicios y los sistemas de información de la empresa **[NOMBRE DE LA EMPRESA],** deberán contar con un sistema de control de acceso a los mismos, este se enfoca en asegurar el acceso de los usuarios y prevenir el acceso no autorizado, incluyendo medidas como la protección mediante contraseñas. El control de acceso debe entenderse tanto lógica como físicamente.

El acceso a los activos de información en **[NOMBRE DE LA EMPRESA]** se otorga siguiendo las recomendaciones de estándares de seguridad reconocidos, como ISO 27001. Estos estándares se basan en los siguientes principios:

- **Necesidad de uso**: Cada cuenta de usuario solo tendrá acceso a la información necesaria para realizar las tareas asignadas. Esto asegura que los usuarios no tengan acceso a información que no necesitan para sus funciones.
- **Principio de mínimo privilegio**: Los privilegios de acceso se otorgan bajo el principio de mínimo privilegio, lo que significa que todo acceso está restringido a menos que sea explícitamente autorizado.
- **Controles de acceso físico**: Se deben implementar controles de acceso físico para proteger los activos de información almacenados en medios físicos.
- **Controles de acceso lógico en medios electrónicos**: Los activos de información almacenados en medios electrónicos deben estar protegidos mediante controles de acceso lógico.
- **Cumplimiento de clasificación y roles**: Los controles de acceso lógico deben estar alineados con el nivel de clasificación del activo de información y los roles y funciones del personal autorizado para acceder a ellos.
- **Solicitud de cambios o retiro de controles**: Solo los responsables de los activos de información pueden solicitar cambios o el retiro de los controles de seguridad de acceso físico o lógico de los activos bajo su responsabilidad.

Adicional, se detallan otros controles de acceso que obedecen a las siguientes directrices:

- Los usuarios deberán ser únicos y no podrán ser compartidos. Así mismo, los privilegios de los usuarios serán inicialmente asignados mediante el principio de mínimo privilegio.
- Se prohibirá el uso de usuarios genéricos. En su defecto, se utilizarán cuentas de usuario asociadas a la identidad nominal de la persona asociada.
- Control de acceso basado en roles: deberán establecerse perfiles o roles de acceso por aplicación y/o sistemas para poder asignar los mismos a los diferentes usuarios.
- Necesidad de saber: solo se permitirá el acceso a un recurso cuando exista una necesidad legítima para el desarrollo de la actividad.
- Privilegios mínimos: los permisos otorgados a los usuarios deberán ser los mínimos.
- Segregación de funciones: deberá asegurarse una correcta segregación de funciones para desarrollar y asignar derechos de acceso.

8.4.1. Registro y cancelación de cuentas de usuario:

- La solicitud para la asignación de cuentas de usuario para acceder a los activos de información de **[NOMBRE DE LA EMPRESA]** debe ser realizada por el líder del área correspondiente o la persona delegada para dicha actividad.
- Cada cuenta de usuario se asigna a una única persona, con los derechos de acceso correspondientes a sus funciones.
- Las cuentas de usuario para acceder a los activos de información, servicios tecnológicos y sistemas informáticos de la empresa son personales e intransferibles.
- La asignación de cuentas de usuario compartidas, gestionadas por varias personas, solo se permite por razones específicas relacionadas con el cumplimiento de funciones y debe ser autorizada por el superior inmediato.
- Al finalizar la relación laboral o contractual, se procederá a la desvinculación de la cuenta de usuario asignada. Además, se ajustarán los derechos de acceso de las cuentas de otros usuarios según sea necesario.
- Se debe mantener un registro actualizado de todas las cuentas de usuario, incluyendo aquellas con derechos de acceso privilegiado y sus respectivos responsables.
- **[NOMBRE DE LA EMPRESA]** se adhiere a los lineamientos de seguridad de autenticación de usuarios de los servicios informáticos suministrados por terceros, sobre los cuales la empresa no tiene control ni privilegios de administrador.
- Se deben eliminar los accesos de usuarios que han abandonado la organización.
- Se debe modificar los accesos de usuarios que han cambiado de función o puesto de trabajo si procede.

8.4.2. Derecho de acceso privilegiado:

- Los privilegios de acceso como administrador a los activos de información deben ser otorgados únicamente al personal esencial.
- Solo se debe asignar privilegios de administrador a aquellos empleados que posean las competencias necesarias para realizar tareas administrativas.
- Las cuentas con privilegios de administrador deben ser utilizadas exclusivamente para labores administrativas y no para tareas cotidianas.
- La asignación de privilegios de administrador debe seguir el principio de mínimo privilegio, otorgando solo los permisos necesarios para realizar las tareas asignadas
- Los roles o permisos de administrador deben ser revocados cuando haya cambios en las funciones del empleado o al finalizar su relación laboral. Si es necesario mantener la cuenta activa por un periodo adicional se requiere la autorización del jefe inmediato para el cambio de contraseña del usuario.
- El uso inapropiado de privilegios de administrador será tratado como un incidente de seguridad de la información y gestionado según el procedimiento correspondiente.

8.4.3. Gestión de información de autenticación secreta de usuarios:

- Las contraseñas y claves de acceso para las cuentas de usuario son personales e intransferibles.
- Las contraseñas deben cumplir con la Política de Contraseña Segura de la empresa.

- El uso de técnicas o herramientas para obtener información de autenticación sin autorización se considera un incidente de seguridad de la información.
- Las contraseñas de cualquier cuenta de usuario que se vea afectada, comprometida o conocida por terceros no autorizados deben ser cambiadas lo antes posible.
- La información de autenticación para cuentas de usuario asignadas a servicios informáticos (como conexiones a bases de datos, servidores web, servicios de monitorización, etc.) debe ser conocida solo por el personal encargado de administrar esos servicios.
- La seguridad de la información de autenticación para cuentas de uso compartido debe gestionarse mediante software especializado para la gestión de contraseñas compartidas.
- Las contraseñas, claves o preguntas de seguridad asignadas a cuentas de usuario proporcionadas por terceros deben cambiarse la primera vez que se utilicen.
- Los responsables de la administración de cuentas de usuario asignadas por terceros deben establecer controles de protección de la información de autenticación, incluyendo contraseñas seguras, configuración de autenticación de dos factores, cambio periódico de contraseñas y prevención de la reutilización de contraseñas.

8.4.4. Revisión de derechos de acceso de usuarios:

- La asignación de derechos de acceso a la información debe ser controlada y tener un registro de la misma.
- El administrador del activo de información debe asignar únicamente los derechos aprobados por el líder del área correspondiente.
- El acceso a los activos de información se otorga siguiendo las recomendaciones de estándares de seguridad reconocidos, como ISO 27001. Esto significa que cada cuenta de usuario solo tendrá acceso a la información necesaria para realizar sus tareas asignadas.
- Los privilegios de acceso se otorgan bajo el principio de mínimo privilegio, restringiendo todo acceso a menos que sea explícitamente autorizado.
- Los derechos de acceso para personas que trabajen temporalmente en la empresa deben ser otorgados únicamente por el periodo de su servicio.
- Se debe evitar el uso no autorizado de identificaciones de usuario genéricas de administración, de acuerdo con las capacidades de configuración del sistema.
- Los administradores de los activos de información deben mantener un registro de todas las solicitudes de asignación, modificación y eliminación de derechos de acceso.

8.4.5. Responsabilidades de los usuarios: Seguridad de las contraseñas.

- Las contraseñas de acceso a las cuentas de usuario, incluidas las cuentas con privilegios de administrador, se regirá por una política de contraseñas robustas que garantice una complejidad adecuada en su composición. La periodicidad de actualización de estas credenciales estará sujeta a los mecanismos de seguridad implementados; en sistemas donde se aplique la autenticación multifactor (MFA), los ciclos de rotación podrán extenderse conforme a los estándares de riesgo de la organización, asegurando siempre una renovación mínima anual.

- Las contraseñas no deben contener información que pueda vincularse con el nombre de la cuenta, datos personales del usuario, o información institucional. Esto incluye datos fácilmente identificables como fechas de nacimiento, hobbies, nombres de familiares, datos académicos o laborales, y cualquier otra información publicada.
- Evitar el registro de las contraseñas en el código fuente de programas o en la configuración de servicios informáticos.
- Evitar el registro de las contraseñas en los servicios de almacenamiento de contraseñas de los navegadores de internet.
- Las contraseñas no deben ser transmitidas en texto claro a través de servicios de correo electrónico, mensajería instantánea, ni deben ser dejadas expuestas o visibles en formatos impresos, archivos de software o dispositivos extraíbles, a menos que puedan ser almacenadas de forma segura.
- Cualquier contraseña que haya sido comprometida o se sospeche que ha sido comprometida debe ser reemplazada de inmediato.

8.4.6. Control de acceso a sistemas de información, aplicaciones y código fuente:

- Las diferentes versiones del software deben ser almacenadas, controladas y protegidas utilizando herramientas que prevengan cambios no autorizados.
- Las bibliotecas y componentes de terceros utilizados en el desarrollo de software deben estar actualizados, contar con soporte y ser sometidos a pruebas de análisis de vulnerabilidades antes de su implementación en entornos de producción.
- Las bibliotecas y componentes de terceros deben ser obtenidos de fuentes verificadas y confiables.
- Las bibliotecas y componentes de terceros utilizados en los desarrollos de software deben contar con las licencias necesarias para su uso en el sistema de información final.
- El procedimiento de inicio de sesión no debe mostrar los identificadores del sistema o de la aplicación hasta que el inicio de sesión haya sido exitoso.
- Los sistemas deben mostrar advertencias y evitar proporcionar mensajes de ayuda que puedan dar pistas a usuarios no autorizados.
- El área de tecnología debe registrar los intentos fallidos de inicio de sesión y notificar a los líderes de área correspondiente sobre esta información.
- Las sesiones inactivas deben cerrarse después de un cierto tiempo de inactividad.
- En el caso que aplique se puede considerar la limitación de las horas del día para el acceso a las aplicaciones.

8.5. POLÍTICA DE SEGURIDAD PARA EL USO DE RECURSOS CRIPTOGRÁFICOS

La empresa **[NOMBRE DE LA EMPRESA],** utilizará herramientas de criptografía con el fin de garantizar la confidencialidad e integridad de la información, para lo cual el Área de tecnología establecerá, implementará y comunicará las herramientas criptográficas que se

deben usar y aplicar a la información en su almacenamiento y trasferencia, igualmente para el manejo de las claves criptográficas.

- Las claves criptográficas deben ser generadas de manera segura, utilizando métodos y herramientas que aseguren su fortaleza y aleatoriedad.
- La distribución de las claves criptográficas debe realizarse de manera segura, asegurando que solo las personas autorizadas tengan acceso a ellas.
- Las claves criptográficas deben ser renovadas periódicamente para mantener su seguridad. Las claves que ya no se utilicen deben ser destruidas de manera segura para evitar su recuperación.
- El tráfico de redes inalámbricas debe estar protegido mediante cifrado WPA2. El tráfico de redes inalámbricas a invitados puede ser libre.
- El acceso a servidores debe realizarse utilizando protocolos que garanticen el cifrado de los datos, como SSH, SFTP/FTPS y HTTPS.
- El tráfico de los sitios web de la empresa debe estar protegido mediante certificados seguros emitidos por entidades de certificación reconocidas. Los certificados deben cumplir con estándares internacionales como TLS v1.3 o superior.
- Los certificados y firmas digitales utilizados para documentos y servicios de información deben ser generados por entidades de certificación avaladas.
- Las claves criptográficas utilizadas para cifrar la información deben cumplir con la política de contraseña segura de la empresa.
- En caso de aplicar cifrado de datos, se debe utilizar un estándar igual o superior a AES-256 (Advanced Encryption Standard).
- Los servicios web de uso exclusivo dentro de la red local o extendida (no accesibles desde internet), así como las conexiones VPN o de escritorio remoto, deben estar protegidos con certificados digitales emitidos por la entidad certificadora interna. Estos certificados deben tener una vigencia máxima de tres años y utilizar algoritmos sin vulnerabilidades, como mínimo SHA-256, con una longitud de llave de 2048 bits.
- Cuando las claves públicas sean emitidas por un proveedor externo, debe existir un Acuerdo de Nivel de Servicio (SLA) que defina claramente las responsabilidades del proveedor.

8.6. POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

La empresa **[NOMBRE DE LA EMPRESA],** ha establecido lineamientos para establecer áreas seguras y medidas para el cuidado de los equipos, con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información.

8.6.1. Áreas Seguras:

Los espacios físicos donde se ubiquen los sistemas de información, equipos de tecnologías de la información, documentos físicos, etc. deben estar protegidos adecuadamente, y según sea el caso, mediante controles tales como:

- Controles de acceso perimetrales
- Sistemas de vigilancia
- Señalización de área restringida
- Registro de ingreso

- Sistemas de extinción de incendio
- Sensores y monitoreo de variables ambientales

A continuación, se especifican las políticas con el fin de minimizar el riego de incidentes de seguridad (accesos no autorizados, robo, sabotaje, etc.) y accidentes ambientales (incendio, fallos en el fluido eléctrico, altas temperaturas, etc.):

Entrada y accesos físicos:

- Los puntos de acceso a las instalaciones físicas de **[NOMBRE DE LA EMPRESA]** deben estar protegidos para evitar accesos no autorizados.
- El acceso a las áreas de procesamiento o almacenamiento de información debe estar limitado exclusivamente al personal debidamente autorizado.
- Se deben mantener registros del acceso físico a las áreas donde se almacena o procesa información.

Nota: La entrada y acceso físico también es controlada por la administración del edificio a través de software de gestión de acceso por QR, arcos detectores de metales, personal de seguridad, cámaras, escáneres de imagen térmica y caninos de detección de explosivos o drogas. El control es muy estricto al tener embajadas y ser el centro de operaciones de la Bolsa de Valores de Colombia.

Detección y control de amenazas ambientales:

Las áreas de procesamiento y almacenamiento de información en **[NOMBRE DE LA EMPRESA]** deben estar protegidas contra diversas amenazas físicas y ambientales, incluyendo desastres naturales como incendios, inundaciones, terremotos, explosiones, disturbios civiles, contaminación por agentes tóxicos y otras amenazas, ya sean intencionales o no. Se deben considerar los siguientes controles de detección de amenazas ambientales:

- **Incendios**: Implementar sistemas de detección de incendios, alarmas y mecanismos de control de fuego para prevenir y mitigar los daños causados por incendios.
- **Sobretensión eléctrica**: Utilizar sistemas de puesta a tierra y dispositivos de protección contra sobrevoltaje para evitar fluctuaciones en el suministro eléctrico que puedan dañar estaciones de trabajo, servidores, equipos de comunicaciones y otros activos informáticos.
- **Explosivos y armas:** Realizar inspecciones de paquetes y vehículos para detectar la presencia de armas o explosivos que puedan ingresar a las instalaciones donde se almacena o procesa información.
- **Inundaciones.** Sistemas de detección temprana de inundaciones bajo los pisos de los centros de procesamiento de datos y disponer de motobombas para actuar en caso de inundación.

Nota: La administración del edificio tiene sus propios controles de detección de amenazas ambientales. Específicamente, sistemas de detección de incendios, alarmas, cámaras, inspecciones de acceso a explosivos y armas, y la disposición de motobombas es aprovisionada y controlada por la administración del edificio.

Trabajo en áreas seguras y Data Center:

- Prohibir la realización de trabajos sin la supervisión de personal autorizado.
- Inspeccionar las zonas al finalizar las visitas para asegurar que no haya quedado nada fuera de lugar.
- Prohibir el uso de móviles y cámaras, a menos que se cuente con una autorización expresa.
- Asegurar que los puntos de acceso a los centros de procesamiento de información y áreas seguras estén protegidos para evitar accesos no autorizados.
- Los trabajos en las áreas de procesamiento de datos deben ser supervisados y controlados en todo momento.
- Mantener cerradas las áreas de almacenamiento y procesamiento de información para prevenir el acceso de personal no autorizado.

Seguridad del cableado:

- El cableado de comunicaciones dentro de las instalaciones de **[NOMBRE DE LA EMPRESA]** debe estar protegido para prevenir cualquier manipulación no autorizada.
- El cableado de comunicaciones debe estar separado de las redes eléctricas para evitar interferencias.
- Tanto la red de cableado eléctrico como la de comunicaciones deben someterse a mantenimiento regular.
- Los puntos de acceso del cableado a los equipos o a las salas deben asegurarse según corresponda y los cables deben estar protegidos.
- El cableado de comunicaciones y las redes eléctricas deben estar claramente identificados para facilitar las tareas de mantenimiento y reparación.
- El acceso a los cuartos de equipos y a las cajas de conexión eléctrica y de comunicaciones debe estar restringido únicamente al personal autorizado.

Elementos de soporte:

- Implementar sistemas de alimentación ininterrumpida para mantener operativos los equipos críticos durante cortes de energía.
- Implementar sistemas de almacenamiento de agua de emergencia para asegurar el suministro durante cortes.
- Realizar mantenimientos periódicos para verificar el estado de los sistemas.
- Realizar simulacros y pruebas periódicas de los planes de contingencia para asegurar su efectividad.

Nota: El edificio es responsable de garantizar, mantener y proveer el suministro de energía, agua y cuenta con un plan de contingencia para enfrentar cualquier eventualidad relacionada con fallos en el suministro.

Áreas de entrega y de carga:

Dado que los puntos de carga suelen ser puntos sensibles para la seguridad física, se deben considerar los siguientes aspectos de control en la evaluación de riesgos:

- Establecer horarios específicos de apertura y cierre para la recepción y despacho de carga.
- Implementar controles para la apertura y cierre de puertas externas e internas.
- Supervisar y controlar el acceso del personal involucrado en la recepción y despacho de carga.
- Realizar inventarios detallados de los materiales entregados y despachados.
- Inspeccionar las mercancías entregadas para detectar materiales peligrosos.
- Mantener separadas las entregas entrantes y salientes para evitar confusiones y mejorar la seguridad.
- Informar de cualquier incidente a los responsables de seguridad de manera inmediata.

Nota: La carga se recibe, revisa y despacha por el parqueadero del edificio. La recepción, inspección y despacho de carga es controlada por la administración del edificio y se tienen horarios específicos para la realización de estas actividades.

8.6.2. Ubicación y protección de equipos:

Los equipos de cómputo, escáner, impresoras, etc. se ubicarán de forma tal que se pueda disminuir el riesgo de amenazas ambientales y de accesos no autorizado, igualmente los usuarios deben bloquear los equipos cuando los dejen desatendidos, lo mismo que el escritorio libre de documentos y medios de almacenamiento con información importante cuando no estén en él, y para reforzar esta medida el área de tecnología programará el bloqueo de los equipos a los cinco (5) minutos de inactividad.

- Las estaciones de trabajo deben ser utilizadas exclusivamente para las labores y funciones designadas. Está prohibido su uso para fines personales.
- Cada usuario debe tener una cuenta de usuario y contraseña única, que no debe ser compartida con nadie.
- Las estaciones de trabajo que cuenten con acceso a activos de información no pueden ser utilizadas por otra persona cuando no estén en uso.
- El uso de periféricos (micrófonos, cámaras, lectores de huellas, escáneres, impresoras, etc.) y medios de almacenamiento debe limitarse según las funciones asignadas.
- Los puertos USB para dispositivos de almacenamiento deben permanecer bloqueados en estaciones de trabajo con información reservada y clasificada.
- Está prohibido instalar, desinstalar o realizar cambios en el hardware o software de las estaciones de trabajo sin autorización.
- Las estaciones de trabajo deben contar con herramientas de protección contra software malicioso instaladas y actualizadas permanentemente.
- El software de protección contra códigos maliciosos y el software de detección y respuesta de incidentes (XDR) deben estar siempre activos y actualizados.
- Cualquier dispositivo conectado a una estación de trabajo debe ser verificado con software antivirus antes de procesar cualquier tipo de información.
- Los usuarios no deben tener privilegios de administración sobre sus equipos.

- Para asegurar la actualización del software (antivirus, parches de seguridad, sistema operativo, etc.), los usuarios deben apagar sus máquinas al finalizar la jornada laboral.
- Las estaciones de trabajo deben estar ubicadas en lugares que minimicen el riesgo de daño por amenazas físicas como fuego, agua, polvo, agentes químicos, vandalismo y acceso no autorizado.
- Está prohibido consumir alimentos o bebidas cerca de las estaciones de trabajo para prevenir daños por derrame de líquidos o contaminación.

8.6.3. Equipos y activos fuera de las instalaciones:

- Todo retiro de equipos de cómputo de las instalaciones debe ser registrado en un formato de entrada y salida.
- Los equipos autorizados para trabajar fuera de las instalaciones no deben ser dejados desatendidos o sin vigilancia en ningún momento.
- Los equipos y medios de almacenamiento autorizados para uso fuera de las instalaciones deben estar protegidos con contraseñas de usuario para el acceso.

8.6.4. Equipos desatendidos por el usuario:

- Los usuarios deben cerrar todas las sesiones de aplicaciones y redes cuando no estén en uso. Esto incluye tanto dispositivos móviles como equipos fijos.
- Los usuarios deben activar el bloqueo de pantalla en sus dispositivos cuando no estén en uso.
- El bloqueo de pantalla debe configurarse para activarse automáticamente después de un período de inactividad definido.
- Los equipos no deben ser dejados desatendidos sin las medidas de seguridad adecuadas.
- En caso de que un equipo deba ser dejado temporalmente, debe estar bloqueado y en un lugar seguro.

8.6.5. Política de escritorios y pantalla limpia:

- La información sensible no debe quedar expuesta o accesible a personal no autorizado. Esto incluye documentos impresos en el escritorio o en las impresoras, así como archivos sensibles en el escritorio del computador.
- Las pantallas no deben mostrar información cuando el equipo no esté en uso.
- La información crítica publicada en tableros o salas de reuniones debe ser borrada o eliminada al finalizar su utilización.
- El papel utilizado para imprimir información clasificada como reservada o crítica no debe ser reciclado; debe ser destruido una vez utilizado.
- Los escritorios deben estar libres de papeles cuando no estén en uso o desatendidos.
- Las impresoras deben configurarse de modo que solo el creador pueda acceder a las copias una vez que se haya ingresado un código en la máquina para evitar el acceso no autorizado.

8.7. POLÍTICA SEGURIDAD DE LAS OPERACIONES

La empresa **[NOMBRE DE LA EMPRESA],** tomará las medidas necesarias para que se garantice la integridad, confidencialidad y disponibilidad de la información. La empresa se compromete a implementar controles de seguridad que prevengan, detecten y respondan a amenazas, protegiendo la información crítica y garantizando la continuidad del negocio en situaciones adversas.

8.7.1. Documentación de procedimientos operativos:

- Todos los procedimientos operativos de IT deben documentarse en un formato claro y estandarizado, abarcando actividades esenciales como la instalación, configuración, arquitectura, administración, y mantenimiento de equipos y sistemas.
- La documentación debe revisarse periódicamente y actualizarse siempre que se produzcan cambios en la infraestructura, configuración o procedimientos operativos.
- Todos los documentos deben adherirse a estándares de redacción específicos y cumplir con las mejores prácticas, incluyendo codificación de seguridad, trazabilidad de cambios y descripciones claras.
- La documentación debe almacenarse en ubicaciones seguras, tanto en formato físico (si se considera necesario) como digital, preferentemente en sistemas de gestión documental con acceso controlado.

8.7.2. Seguridad en la gestión de cambios y capacidad:

- Antes de implementar un cambio, el responsable del área evaluará su impacto en la seguridad, disponibilidad y continuidad del sistema, enfocándose en posibles riesgos que afecten a la operación diaria.
- Cambios significativos que afecten la infraestructura general deben ser autorizados por un supervisor o responsable de IT.
- Todos los cambios deben registrarse e incluir detalles como la descripción del cambio, la fecha de implementación y el responsable del mismo.
- Los proveedores deben informar previamente cualquier modificación que pueda afectar los sistemas de la empresa.
- Una vez aplicado un cambio, el área de tecnología o el responsable asignado monitoreará el sistema brevemente para asegurarse de que no se han introducido problemas de seguridad o rendimiento significativos.
- Realizar análisis periódicos para evaluar las necesidades actuales y futuras de capacidad en función del crecimiento de la empresa.
- Prever la actualización de infraestructura para cubrir los requisitos futuros, considerando factores como almacenamiento, procesamiento, y ancho de banda.

8.7.3. Separación de los ambientes de desarrollo, prueba y operación:

- El área de tecnología establecerá una línea base de seguridad que refleje los requisitos mínimos de protección para los activos de información.
- La línea base de seguridad debe actualizarse como resultado de las actualizaciones de seguridad formuladas por los fabricantes y proveedores.

- Las pruebas de análisis de vulnerabilidades que se realicen en la infraestructura deberán ser revisadas de forma general para ajustar la línea base de seguridad según sea necesario.
- Los cambios o accesos realizados en cualquiera de los entornos deberán ser registrados para asegurar la trazabilidad.
- Los accesos a los entornos de producción y pruebas estarán controlados, asegurando que solo el personal necesario tenga acceso a cada ambiente.
- Los entornos de desarrollo se mantendrán completamente separados de los entornos operativos, asegurando que las pruebas y modificaciones no afecten la estabilidad y seguridad del sistema en producción.
- Todo software en los entornos de producción y pruebas deberá mantenerse en versiones compatibles y estables, preferiblemente soportadas por el fabricante o proveedor.
- El software de código abierto, librerías, módulos o framework de desarrollo debe mantenerse en versiones compatibles, estables y soportadas por los sistemas de información que los utilizan.
- Antes de poner en producción cualquier dispositivo, servicio o componente, se deberá verificar que cumpla con la línea base de seguridad establecida.

8.7.4. Protección contra código malicioso (Antivirus):

- La instalación de software antivirus y de protección contra malware en los equipos de la empresa será responsabilidad exclusiva del área de tecnología o del personal autorizado, garantizando que todos los dispositivos críticos cuenten con protección activa y actualizada.
- Únicamente se permitirá el uso de software aprobado por la organización. Todo software de terceros debe ser previamente evaluado y autorizado para su instalación, evitando así la introducción de aplicaciones no confiables o potencialmente peligrosas.
- Todos los equipos conectados a la red de la empresa, incluidos servidores de archivos y de correo, deben contar con un software antivirus que mantenga sus definiciones de virus actualizadas.
- Antes de utilizar cualquier dispositivo de almacenamiento externo, archivo descargado o documento recibido por correo electrónico, debe realizarse un escaneo de seguridad mediante el software antivirus, reduciendo el riesgo de introducción de malware.
- Si se detecta un posible caso de infección en un equipo, este puede ser desconectado de la red hasta que el área de tecnología confirme la eliminación de la amenaza y restaure su seguridad.
- La protección contra malware no debe desactivarse ni modificarse en su configuración de seguridad sin aprobación del área de tecnología.
- Cualquier alteración de las protecciones establecidas podría comprometer la seguridad de la red y será tratada de acuerdo con las políticas internas de seguridad.

- El personal recibirá pautas generales de buenas prácticas para evitar la instalación de software sospechoso y evitar la descarga de archivos desde fuentes no confiables.

8.7.5. Copias de respaldo:

- El proceso de generación y restauración de copias de respaldo deberá registrarse en un archivo o bitácora simple. Este registro incluirá la fecha, tipo de respaldo y confirmación de éxito o problemas encontrados durante el proceso.
- Las copias de respaldo se almacenarán en ubicaciones seguras para prevenir el acceso no autorizado y proteger la información respaldada de posibles pérdidas o daños.
- El área de tecnología o el responsable definido revisará el correcto funcionamiento de las copias de respaldo mediante pruebas de restauración.
- La información esencial para la operación de la empresa será priorizada en los procesos de respaldo, basándose en su importancia para las actividades estratégicas y operativas.
- El proceso de generación de respaldos y pruebas de restauración se realizará para minimizar interrupciones a las actividades diarias y reducir el tiempo dedicado por el área de tecnología.

8.7.6. Registro de operación y sincronización horaria de los sistemas de información:

- Los activos de información (sistemas y dispositivos) que cuenten con capacidad para registrar eventos de seguridad deben configurarse para generar estos registros de manera continua.
- Los registros generados deben resguardarse contra cualquier acceso no autorizado o alteración, en línea con la política de seguridad y respaldo de la empresa.
- El área de tecnología, en colaboración con los administradores de cada activo de información, definirá un período adecuado de retención para estos registros.
- Los registros de auditoría deben ser almacenados de acuerdo con las políticas de respaldo y continuidad de negocio de la empresa, asegurando que su disponibilidad no se vea comprometida.
- Todos los sistemas de información, dispositivos de comunicaciones, y demás activos tecnológicos con capacidad de generar registros de eventos deberán sincronizar su reloj interno con una fuente de hora oficial y confiable.
- La hora de los sistemas de información, dispositivos de comunicaciones, dispositivos de seguridad, estaciones de trabajo y en general cualquier dispositivo electrónico con capacidad de generar registro de eventos debe estar sincronizada con la hora legal colombiana establecida por el Instituto Nacional de Metrología, reglamentado a través del Decreto 2707 de 1982, Articulo 1 y Articulo 2, por el cual se adopta la hora legal en el territorio nacional.

8.7.7. Instalación de software en sistemas operacionales:

- La instalación de software en estaciones de trabajo y servidores será realizada únicamente por personal del área de tecnología o personal expresamente autorizado.
- Antes de instalar cualquier software, se evaluará la compatibilidad del entorno y se analizará si el sistema cumple con todos los requisitos técnicos necesarios.
- Las decisiones sobre actualizaciones o instalaciones deben considerar el impacto en el entorno operativo y la posibilidad de retroceder a versiones anteriores si fuera necesario.
- Las actualizaciones y parches de seguridad se aplicarán únicamente desde fuentes oficiales y confiables del proveedor, minimizando así el riesgo de comprometer los sistemas.
- Antes de implementar cualquier cambio en servidores, se deberá contar con un respaldo actualizado de la configuración y los datos críticos.
- Solo se permitirá la instalación de software proveniente de fuentes oficiales verificadas.
- Tras la instalación o actualización de software, se realizará un monitoreo de la red para detectar cualquier actividad inusual o disminución en el rendimiento de la transmisión de datos.

8.7.8. Gestión de amenazas y vulnerabilidades técnicas:

- El área de tecnología será responsable de monitorear y recopilar información sobre vulnerabilidades técnicas en los activos de información mediante fuentes confiables y actualizadas.
- Todos los empleados deben informar cualquier vulnerabilidad o riesgo de seguridad identificado en los sistemas al área de tecnología.
- El área de tecnología evaluará regularmente la seguridad de software, bibliotecas y otros componentes utilizados en los sistemas, prestando especial atención a actualizaciones de seguridad y parches disponibles.
- Se llevarán a cabo pruebas periódicas de vulnerabilidad y simulaciones de ataques (pruebas de penetración) en la infraestructura tecnológica para identificar y abordar debilidades en la seguridad.
- Todas las vulnerabilidades detectadas deben ser documentadas y abordadas dentro de un tiempo razonable y el área de tecnología llevará a cabo un seguimiento de las acciones correctivas implementadas.
- Los contratos con proveedores y terceros que presten servicios tecnológicos incluirán cláusulas que especifiquen la obligación de identificar y gestionar vulnerabilidades técnicas en los servicios que ofrecen.
- Se llevará a cabo capacitación para todos los empleados sobre la identificación y reporte de vulnerabilidades, así como sobre buenas prácticas de seguridad para reducir la exposición a amenazas.
- Las políticas de gestión de vulnerabilidades se revisarán y actualizarán anualmente o cuando ocurran cambios significativos en la infraestructura tecnológica o en las amenazas identificadas.

8.8. POLÍTICA SEGURIDAD DE LAS COMUNICACIONES

8.8.1. Seguridad en el uso de servicios en la nube:

- Verificar que los proveedores de nube cuenten con los controles administrativos y técnicos necesarios para cumplir con los requisitos legales y normativos en materia de seguridad de la información y protección de datos personales.
- Los lineamientos sobre responsabilidades en materia de seguridad de la información estarán alineados con las buenas prácticas formuladas por la Cloud Security Alliance.
- En la adquisición de servicios de nube bajo la modalidad SaaS, el proveedor será responsable de implementar los controles de seguridad, mientras que **[NOMBRE DE LA EMPRESA]** solo gestionará el acceso y uso de la aplicación.
- En servicios PaaS, el proveedor será responsable de la seguridad de la plataforma, y **[NOMBRE DE LA EMPRESA]** se encargará de la seguridad de la información y protección de datos de los servicios desplegados en la plataforma.
- Para servicios IaaS, el proveedor garantizará la seguridad de la infraestructura base, mientras que **[NOMBRE DE LA EMPRESA]** será responsable de la seguridad de la información construida sobre dicha infraestructura.
- Los servicios de nube deberán contar con un modelo de gestión de continuidad de operaciones.
- Los servicios de nube deben contar con un modelo de respuesta ante incidentes de seguridad de la información del proveedor de servicios de nube
- Los servicios de nube deben contar un modelo de gestión de identidades y control de privilegios que contemple:

    - Protección del perímetro de la red
    - Autenticación de clientes para garantizar el acceso autorizado
    - Administración de cuentas de usuario, incluyendo la asignación y supervisión de privilegios de acceso
    - Monitoreo continuo de actividad, con registro de eventos y alertas para una supervisión efectiva
    - Los servicios de nube deberán contar con un modelo de respuesta ante incidentes de seguridad de la información.

- Para la seguridad de las aplicaciones en la nube, **[NOMBRE DE LA EMPRESA]** establecerá los siguientes principios:

    - Definición de una línea base de seguridad
    - Implementación de entornos controlados para realizar pruebas y operaciones críticas
    - Uso de máquinas virtuales dedicadas para aislamiento de procesos
    - Administración de la escalabilidad del servicio para ajustar recursos según la demanda
    - Integración de un modelo de despliegue DevOps que favorezca la actualización y mejora continua

- Consolidación de una interfaz unificada para la gestión y supervisión de los servicios en la nube

- En los servicios de nube se deben contemplar aspectos de eliminación segura de la información.

8.8.2. Seguridad en dominios web:

- Los nombres de dominio utilizados por **[NOMBRE DE LA EMPRESA]** son de su propiedad exclusiva.
- Realizar pruebas de vulnerabilidad antes de que el dominio pase a un entorno de producción.
- Implementar controles para proteger la configuración del DNS, evitando modificaciones no autorizadas que puedan afectar el acceso o redireccionar a los usuarios hacia sitios web con contenido malicioso
- Proteger los datos de contacto asociados al dominio, de modo que se mantengan actualizados y autorizados para gestionar el acceso.
- Evitar alteraciones no autorizadas en la configuración del dominio y restringir cambios en los parámetros críticos.
- Asegurarse de que toda la información de contacto vinculada al dominio refleje la identidad institucional de **[NOMBRE DE LA EMPRESA]**
- Establecer mecanismos de control para asegurar la integridad y autenticidad de las comunicaciones entre los servidores.
- La migración o cancelación del dominio se debe realizar con la debida autorización del área de tecnología.
- Los registros AAC (Autorización de la Autoridad de Certificación), los cuales hacen posible que el titular de un nombre de dominio indique las autoridades de certificación que tienen permiso para emitir un certificado.

8.8.3. Seguridad en Redes Privadas Virtuales (VPN):

- Las conexiones remotas mediante redes privadas virtuales (VPN) hacia la red local de **[NOMBRE DE LA EMPRESA] solo** podrán ser autorizadas por el área de tecnología.
- Las contraseñas utilizadas para acceder a las VPN deben cumplir con la política de contraseñas seguras establecida por **[NOMBRE DE LA EMPRESA]**
- Cuando sea necesario la autenticación doble factor en la VPN, este mecanismo deberá habilitarse como medida obligatoria.
- Las solicitudes de acceso a la red local mediante VPN deberán ser gestionadas exclusivamente por personal autorizado, y se debe monitorear y limitar la descarga de datos a través de la VPN para minimizar riesgos de fuga de información.
- Todas las conexiones por VPN deben registrarse en un log que detalle el usuario autorizado, los servicios o servidores a los que se accede, y la fecha de expiración de dicho acceso.
- Las cuentas de usuario configuradas para conexiones VPN no deberán tener privilegios de administración, limitándose a permisos mínimos necesarios.

- Los servidores de VPN deben someterse a evaluaciones periódicas de vulnerabilidad, aplicando parches de seguridad recomendados para mitigar posibles riesgos y mantener la infraestructura segura.
- Todo tráfico a través de la VPN deberá pasar por filtros de seguridad para bloquear el uso de protocolos inseguros que puedan comprometer la red.
- Las VPN deben emplear algoritmos de cifrado fuertes, como mínimo SHA-256 con AES-128/256 o SHA-384 para datos particularmente sensibles.
- Las conexiones VPN deben estar configuradas con un límite máximo de tiempo de sesión, forzando la desconexión y requerir reconexión si el usuario necesita continuar.
- Está prohibido utilizar software gratuito para el establecimiento de conexiones VPN. Solo se permitirá la conexión a la red local de **[NOMBRE DE LA EMPRESA]** mediante el software aprobado por el área de tecnología.
- El área de tecnología determinará la modalidad de conexión VPN permitida, como sitio a sitio (site-to-site) o cliente a servidor (client-to-site), según las necesidades de la organización.

8.8.4. Seguridad en Redes WIFI:

- Las conexiones a las redes WiFi de **[NOMBRE DE LA EMPRESA]** deberán configurarse de manera que se registre la información de acceso de todos los usuarios autorizados.
- Los dispositivos de acceso a redes inalámbricas deberán tener desactivada la difusión del identificador de red (SSID) para evitar la detección de la red por personas no autorizadas.
- Las contraseñas de administración para los dispositivos de red WiFi deberán cumplir con la política de contraseñas seguras de **[NOMBRE DE LA EMPRESA]**
- Toda conexión a la red WiFi de **[NOMBRE DE LA EMPRESA]** deberá configurarse utilizando un protocolo de autenticación seguro, con WPA2 como estándar mínimo.
- Las contraseñas de acceso a las redes WiFi deberán cumplir estrictamente con los lineamientos de la política de contraseñas seguras de la organización.
- La configuración de las redes inalámbricas deberá cifrar todo el tráfico de forma predeterminada, utilizando al menos el protocolo de cifrado AES.
- El firmware de los dispositivos de acceso a redes inalámbricas deberá mantenerse siempre actualizado con los parches de seguridad más recientes recomendados por el fabricante.
- Los accesos a redes WiFi para invitados en las instalaciones de **[NOMBRE DE LA EMPRESA]** deberán configurarse en un segmento de red separado de la red de producción para evitar acceso no autorizado a datos sensibles.
- La opción de configuración remota en los dispositivos de red inalámbrica deberá estar deshabilitada para reforzar la seguridad.
- Las claves de acceso para redes no corporativas deberán rotarse cada 30 días, con el fin de limitar la exposición y prevenir accesos persistentes no autorizados.
- Alternativamente, cuando se habilite un portal cautivo, el acceso deberá redirigirse a una plataforma de registro, autenticación y/o aceptación de condiciones de uso.

- Toda sesión en redes no corporativas deberá contar con mecanismos de desconexión automática, una vez el usuario se retire de la red o se detecte inactividad prolongada.
- Todos los dispositivos de acceso a redes inalámbricas deberán someterse, al menos una vez al año, a pruebas de análisis de vulnerabilidades y ethical hacking para detectar y corregir posibles fallos de seguridad.

8.8.5. Seguridad de bloqueo de accesos no autorizados (Firewall):

- **[NOMBRE DE LA EMPRESA]** utilizará cortafuegos de red para crear un entorno seguro entre Internet y la red privada, como parte de una estrategia de seguridad en capas.
- Todos los cortafuegos instalados deben cumplir con los estándares actuales establecidos por el área de tecnología, y cualquier equipo que no cumpla con estos estándares será desconectado sin previo aviso.
- Las contraseñas de administración de los cortafuegos deben cumplir con la política de contraseñas seguras, no deben ser reutilizadas y deberán expirar periódicamente, bloqueando el acceso si la contraseña no se actualiza.
- El acceso a la consola de administración y a la interfaz web del firewall debe configurarse con un tiempo de expiración máximo de 10 minutos.
- Los cortafuegos deben configurarse para denegar todo tráfico por defecto, permitiendo únicamente el tráfico autorizado explícitamente en esta política.
- Los dispositivos deben deshabilitar protocolos innecesarios (DHCP, SNMP) y sustituir protocolos inseguros (como Telnet y FTP) por sus versiones seguras (como SSH y SFTP).
- Los cortafuegos deben sincronizarse con el servidor NTP de la empresa y configurarse con la zona horaria local de Colombia. Además, se deben habilitar alertas cuando el espacio de almacenamiento para eventos esté próximo a llenarse.
- La opción de copia de seguridad automática debe estar activada en los cortafuegos que cuenten con ella, siguiendo la política de copias de respaldo de la organización.
- Los cortafuegos deberán registrar eventos de administración y auditoría, y se deberá implementar protección contra spoofing y filtros de tráfico para garantizar la integridad de las conexiones.
- Se requiere un proceso de control de cambios antes de modificar cualquier regla del cortafuegos, y cualquier cambio debe ser aprobado formalmente por el área de tecnología de **[NOMBRE DE LA EMPRESA]**
- Los conjuntos de reglas y configuraciones de los cortafuegos deben revisarse de forma periódica para asegurar que cumplen con los niveles de protección necesarios. Solo el personal autorizado del área de tecnología puede acceder y administrar estos conjuntos de reglas y copias de seguridad.

8.8.6. Segregación y filtrado de redes:

- Para controlar el tráfico entre las distintas redes de **[NOMBRE DE LA EMPRESA]**, el área de tecnología aplicará políticas de segmentación y filtrado en redes y subredes mediante cortafuegos, buscando una adecuada protección en toda la infraestructura de comunicaciones.

- Las configuraciones de seguridad se diseñarán siguiendo los principios de Zero Trust, donde no se considera como seguro ningún tráfico, sea interno o externo.
- Deberá evaluarse la segmentación de tráfico para proteger activos específicos, tales como:

    - Redes inalámbricas para invitados o usuarios externos.
    - Servicios en la nube pública.
    - Grupos de usuarios según área de trabajo.

- La segmentación de redes podrá realizarse físicamente o a nivel lógico mediante VLAN y cortafuegos. En casos que lo justifiquen, y de acuerdo con las capacidades tecnológicas, se podrá aplicar microsegmentación para controlar el acceso hasta el nivel de paquetes de datos.
- Las conexiones para terceros, desarrollo, pruebas y entornos de producción deberán ubicarse en segmentos de red separados y protegidos por cortafuegos.
- Para prevenir accesos no autorizados y reducir el riesgo de exposición a sitios potencialmente peligrosos, los cortafuegos de **[NOMBRE DE LA EMPRESA]** deberán configurarse para bloquear sitios con los siguientes contenidos:

    - Contenido para adultos, juegos en línea y material explícito.
    - Sitios que contengan spyware, spam o malware.
    - Servicios de alta demanda de ancho de banda, como descargas de software gratuito, transmisión de video (streaming), redes P2P y descarga de archivos multimedia.

- Además, el acceso a Internet debe contar con controles que prevengan la visita a sitios maliciosos o de dudosa reputación.

8.8.7. Transmisión de información:

- Las condiciones para la transmisión de información deben ser documentadas y aprobadas por ambas partes involucradas en la transferencia.
- En caso de que la información a transferir sea de carácter confidencial, se deberán firmar acuerdos de confidencialidad entre las partes.
- La información reservada deberá ser cifrada durante su transmisión para garantizar su seguridad.
- Todas las transmisiones de información confidencial deberán registrarse adecuadamente.
- La transmisión de información se llevará a cabo a través de canales seguros.

8.9. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La empresa **[NOMBRE DE LA EMPRESA],** implementará requisitos de seguridad de la información a lo largo de todo el ciclo de vida de los sistemas de información (ya sea en proyectos de adquisición o desarrollo de software), y serán incluidos durante el desarrollo y soporte, así como la protección de los datos usados durante las pruebas.

8.9.1. Identificación y documentación de requisitos de seguridad de la información:

- Todos los desarrollos de software y sistemas de información en **[NOMBRE DE LA EMPRESA]**, independientemente de su complejidad y duración, deben identificar y documentar los requisitos de seguridad de la información, ciberseguridad y protección de datos personales.
- Es necesario incluir la identificación de las obligaciones legales y contractuales relacionadas con la seguridad de la información y la protección de datos personales en cada desarrollo.
- Se debe realizar la identificación, valoración, evaluación y tratamiento de los riesgos asociados a la seguridad de la información, ciberseguridad y protección de datos personales que puedan afectar el procesamiento de datos en el sistema de información.
- Todos los desarrollos de software y sistemas de información deben ser diseñados con el principio de "privacidad desde el diseño".
- Deben contemplarse las necesidades de segregación de funciones y los niveles de acceso a la información que manejará el sistema en desarrollo.
- Los sistemas de información deben ser concebidos para ser resilientes ante ataques cibernéticos o interrupciones no intencionadas.
- La protección de la información debe ser considerada durante las fases de procesamiento, almacenamiento y transmisión de los datos.
- Se debe evaluar la necesidad de implementar cifrado para la información tanto en almacenamiento como en tránsito, según corresponda.
- El desarrollo de software debe considerar necesidades de auditoría y registro de eventos relacionados con las actividades realizadas en el sistema de información.

8.9.2. Arquitectura de desarrollo seguro y revisión técnica:

- La arquitectura de los sistemas de información y soluciones de software en **[NOMBRE DE LA EMPRESA]** debe considerar los requisitos de seguridad de la información en todas las capas del sistema, incluyendo, pero sin limitarse a: requisitos de negocio, modelo de datos, requisitos de aplicación y tecnología.
- La arquitectura de los sistemas de información y soluciones de software debe aplicar principios de arquitectura segura, incluyendo, pero no limitándose a:
    - Seguridad en el diseño: La seguridad debe fundamentarse en controles específicos y probados, evitando la "seguridad por oscuridad".
    - Defensa en profundidad: Se debe implementar la seguridad en múltiples capas de defensa.
    - Seguridad por defecto: Los sistemas deben ser diseñados y configurados de manera que la seguridad esté siempre presente.
    - Denegación predeterminada: Los sistemas deben estar diseñados para que los usuarios no tengan habilitadas funciones por defecto, permitiendo solo las necesarias para el desarrollo de sus tareas.
    - Zero Trust: Los sistemas deben considerar que la barrera entre lo confiable y lo no confiable en la red está difuminada.

- Fallo seguro: En caso de una falla, el sistema debe pasar a un estado seguro que proteja los datos y recursos.
- Desconfianza de entradas externas: Todas las entradas al sistema deben ser consideradas inseguras y verificadas antes de su uso.
- Seguridad en la implementación: La implementación del sistema debe asumir que se estará expuesto a un ambiente inseguro y hostil.
- Privilegio mínimo: Solo se deben otorgar los permisos necesarios para la realización de las tareas asignadas.
- Usabilidad y manejabilidad: Los controles de seguridad deben ser transparentes para el usuario y no causar esfuerzos adicionales innecesarios.
- Funcionalidad mínima: El acceso a las funcionalidades del sistema debe realizarse con los mínimos privilegios requeridos.
- Los desarrollos deben diseñarse, construirse y mantenerse utilizando componentes y bibliotecas que no contengan fallas o vulnerabilidades.
- Protección de servicios web: Los servicios web utilizados para compartir o acceder a datos deben implementar certificados digitales en los ambientes de desarrollo, pruebas y producción; los dos primeros con certificados emitidos por una autoridad certificadora interna y producción con un certificado de una autoridad externa.
- Segmentación de red para terceros: Todos los servicios web accedidos por terceros deben estar provisionados en una interfaz independiente en el firewall, con reglas de acceso que autoricen los puertos y protocolos necesarios para su operación.
- Registros de auditoría: Cada aplicación o servicio web debe generar registros de auditoría de las acciones CRUD (Crear, Leer, Actualizar, Eliminar) de los usuarios, registrando la hora de inicio de sesión, dirección IP de origen y el usuario, y permitir la integración y envío de estos logs al SIEM de **[NOMBRE DE LA EMPRESA]**
- Seguridad perimetral: Cualquier aplicación con acceso desde internet debe contar con un servicio de Firewall de Aplicación Web (WAF) configurado en la nube o local, con todos los controles habilitados.

8.9.3. Principios de la ingeniería de sistemas seguros:

- El software desarrollado para los sistemas de información o servicios de **[NOMBRE DE LA EMPRESA]** debe seguir directrices de codificación segura para minimizar la probabilidad de introducir vulnerabilidades en los servicios.
- Los equipos encargados del desarrollo de sistemas de información, componentes o bibliotecas deben aplicar buenas prácticas de codificación segura y adoptar principios como:

    - Seguridad por diseño: La seguridad debe ser considerada desde las fases iniciales del diseño del sistema o componente. Desde las etapas de codificación, se deben implementar controles de validación de entradas, control de acceso, gestión de contraseñas, manejo de errores y excepciones, cifrado de datos, entre otros.

- Denegación por defecto: Por defecto, todos los accesos deben ser negados; el modelo de permisos debe determinar qué accesos a datos o funcionalidades son autorizados.
- Principio de mínimo privilegio: Cada proceso debe ejecutarse con el conjunto más limitado de privilegios necesarios para completar su tarea. El acceso a permisos privilegiados debe ser temporal y restringido solo al tiempo necesario.
- Minimización y ofuscación de código: El código debe ser claro y limpio. Se debe evitar la complejidad innecesaria que dificulte la lectura y mantenimiento del código.
- Evitar atajos: No se deben omitir los controles de seguridad en el código fuente para acelerar el proceso de producción del software.
- Corrección de vulnerabilidades en etapas tempranas: Las vulnerabilidades identificadas durante la codificación deben ser resueltas de inmediato para evitar la propagación de brechas de seguridad en todo el sistema.
- Evitación de componentes con vulnerabilidades conocidas: Aunque el uso de componentes y bibliotecas de código abierto puede ahorrar tiempo, también puede representar un riesgo al ser un punto de entrada para atacantes.
- Auditoría y registro: El software que incorpora registros de auditoría permite la detección de posibles incidentes en su entorno de producción.
- Los desarrollos deben ser diseñados, construidos y mantenidos utilizando componentes, plataformas y bibliotecas que estén libres de fallas o vulnerabilidades.
- Para el desarrollo o mantenimiento de aplicaciones o servicios web, se deben implementar las prácticas recomendadas por OWASP (Open Web Application Security Project).
- Para el desarrollo o mantenimiento de aplicaciones o servicios web, se deben llevar a cabo pruebas de seguridad estáticas (SAST) y dinámicas (DAST).

8.9.4. Ambiente de desarrollo seguro:

- Los entornos de producción del software de los sistemas de información de **[NOMBRE DE LA EMPRESA]** deben ser distintos de los entornos de desarrollo y prueba del software.
- Los proyectos de desarrollo de software deben establecer e implementar reglas claras para el paso a producción de las versiones que hayan superado satisfactoriamente las pruebas de seguridad y aceptación.
- El paso a producción de nuevas versiones del software o sistemas de información debe llevarse a cabo mediante un mecanismo de gestión de cambios formal.
- En los entornos de producción no deben estar disponibles herramientas, compiladores o programas utilitarios que faciliten el desarrollo de software no controlado.

- El acceso a los entornos de producción debe restringirse únicamente al personal autorizado, garantizando así la integridad de los sistemas.
- Los entornos de producción deben adherirse a la política de gestión de vulnerabilidades técnicas de la empresa.
- Los entornos de producción deben cumplir con la política de copias de respaldo establecida por **[NOMBRE DE LA EMPRESA]**

8.9.5. Desarrollo contratado externamente:

- Los proyectos de desarrollo de software contratados externamente deben ser supervisados para garantizar que el proveedor implemente prácticas de desarrollo seguro que estén alineadas con las políticas de **[NOMBRE DE LA EMPRESA] y** las normas de la ISO.
- Todos los contratos de desarrollo de software deben incluir cláusulas que aseguren la cesión de derechos patrimoniales a favor de **[NOMBRE DE LA EMPRESA]**, o la corporación correspondiente, para proteger la propiedad intelectual de los desarrollos.
- Los desarrollos de software deben cumplir con la normativa vigente relacionada con derechos de autor y protección de datos, asegurando la legalidad en el uso de la propiedad intelectual.
- Los contratos de desarrollo de software o sistemas de información deben incluir obligaciones explícitas sobre la aplicación de prácticas de diseño, codificación y construcción seguras, alineadas con los estándares de seguridad de la información establecidos por la organización.
- Todos los desarrollos de software deben someterse a pruebas de seguridad y funcionamiento, las cuales serán supervisadas por un representante designado por **[NOMBRE DE LA EMPRESA]** Se debe asegurar que los datos de prueba utilizados no incluyan información personal real; cualquier dato personal utilizado debe ser anonimizado antes de ser empleado en entornos de prueba.
- Los desarrollos deben ser diseñados, construidos y mantenidos utilizando componentes, plataformas y bibliotecas que no contengan vulnerabilidades conocidas, promoviendo un enfoque proactivo en la gestión de la seguridad.
- Para el desarrollo y mantenimiento de aplicaciones o servicios web, se deben implementar las prácticas recomendadas por OWASP (Open Web Application Security Project).
- Los desarrollos o mantenimientos de aplicaciones y servicios web deben incluir la ejecución de pruebas de seguridad estáticas (SAST) y dinámicas (DAST), asegurando que se identifiquen y aborden vulnerabilidades en todas las fases del ciclo de vida del software.

8.9.6. Uso de Software de Código Abierto:

- El uso de software de código abierto en el desarrollo de sistemas de información y soluciones de software de **[NOMBRE DE LA EMPRESA]** debe realizarse exclusivamente a partir de fuentes obtenidas legalmente, con la debida

autorización del autor, conforme a los términos y condiciones de la licencia vigente.

- Todo software de código abierto, incluyendo herramientas de desarrollo, frameworks, bibliotecas y componentes, debe ser sometido a pruebas de seguridad, análisis de vulnerabilidades y pruebas de hacking ético durante la fase de pruebas de los sistemas de información o soluciones de software, asegurando que no introduzca riesgos a la seguridad.
- El registro de sistemas de información y soluciones de software que utilicen módulos, componentes o bibliotecas de código abierto debe cumplir con los términos de licenciamiento aplicables a cada uno de estos elementos, garantizando así el cumplimiento normativo.
- Los proveedores y terceros que desarrollen software para **[NOMBRE DE LA EMPRESA]** y que utilicen software de código abierto deben informar de manera explícita sobre los módulos, bibliotecas o componentes utilizados, permitiendo una trazabilidad adecuada y asegurando el cumplimiento de los requisitos legales y de seguridad establecidos.

8.9.7. Pruebas de seguridad y aceptación del sistema:

- Se debe implementar un plan de pruebas documentado que incluya requisitos específicos para la seguridad del sistema, tratándolos como una funcionalidad integral del software.
- Todas las pruebas de seguridad deben abarcar también el software desarrollado por terceros, garantizando que se cumplan los mismos estándares de seguridad aplicados al software interno.
- Se deben documentar y revisar los resultados de las pruebas de seguridad, realizando ajustes necesarios en el desarrollo para mitigar riesgos identificados.
- Antes de incorporar nuevas aplicaciones, actualizaciones o versiones de software, se debe llevar a cabo un proceso de aceptación que incluya pruebas funcionales y de seguridad planificadas.
- Los entornos de prueba deben ser distintos de los entornos de operación para minimizar el riesgo de fallos en sistemas reales. Se debe garantizar que los cambios realizados en el entorno de pruebas no afecten a la operación.
- Todas las pruebas de aceptación deben ser documentadas incluyendo los criterios de éxito y las evidencias de las pruebas realizadas.
- En los entornos de prueba, se debe priorizar el uso de datos NO reales para los desarrollos y pruebas de los sistemas.
- En caso de que se requiera utilizar datos reales, se deben aplicar los mismos controles de seguridad que se implementan para la protección de datos reales, incluyendo acuerdos de confidencialidad y medidas de seguridad física y lógica.
- La selección de datos utilizados en entornos de prueba debe ser revisada y aprobada por el Área de tecnología para garantizar que se cumplen los requisitos de seguridad establecidos.

8.10. POLÍTICA SEGURIDAD DE RELACIÓN CON PROVEEDORES

[NOMBRE DE LA EMPRESA], reconoce que los proveedores son parte fundamental en el desarrollo de las actividades propias de la empresa, por esta misma situación implican un riesgo especialmente aquellos que tienen acceso a los activos de información, tales como, sistemas de información, redes de datos de la compañía, etc. por lo tanto debe establecer de modo formal las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones, así:

- Todos los proveedores de servicios y productos de **[NOMBRE DE LA EMPRESA]** deben adherirse a las políticas de seguridad de la información y protección de datos personales establecidas por la empresa.
- Los proveedores deben firmar acuerdos de confidencialidad específicos si es requerido, en el marco de los contratos establecidos.
- Los proveedores deben cumplir con las directrices, políticas y procedimientos de **[NOMBRE DE LA EMPRESA]** en materia de seguridad de la información, asegurando que sus operaciones se alineen con las mejores prácticas.
- Es responsabilidad de los proveedores informar a la unidad de IT sobre los protocolos que tienen para la gestión de incidentes de seguridad de la información, incluyendo la identificación, respuesta y comunicación de incidentes.
- Los proveedores deberán comunicar a la unidad de IT cualquier protocolo o procedimiento que apliquen para gestionar cambios en la prestación de servicios, incluyendo mantenimientos, actualizaciones y cambios de software.
- Los proveedores deben presentar un plan de manejo de emergencia y continuidad de servicios, que detalle las acciones a tomar ante situaciones que puedan interrumpir la prestación de servicios a **[NOMBRE DE LA EMPRESA]**
- Todos los contratos con proveedores deberán incluir cláusulas de confidencialidad y no divulgación que protejan la información a la que tengan acceso durante el cumplimiento de sus obligaciones contractuales.
- Se debe realizar una evaluación de riesgos periódica a los proveedores para garantizar que cumplan con los requisitos de seguridad establecidos, considerando su impacto potencial en la seguridad de la información de la empresa.
- Los proveedores deberán demostrar que sus empleados reciben formación y están conscientes de las políticas de seguridad de la información de **[NOMBRE DE LA EMPRESA]**, promoviendo una cultura de seguridad compartida.

8.11. POLÍTICA GESTIÓN DE INCIDENTES DE SEGURIDAD

La empresa **[NOMBRE DE LA EMPRESA],** debe manejar adecuadamente los incidentes de seguridad de la información, mediante un enfoque estructurado y debe contar con una planeación previa. Las actividades para la gestión de incidentes de seguridad de la información, ciberseguridad y protección de datos personales contemplan:

8.11.1. Tratamiento de incidentes de seguridad de la información, ciberseguridad y protección de datos personales:

- Desarrollar y mantener un procedimiento de respuesta que defina roles y responsabilidades en la gestión de incidentes de seguridad.
- Detección de incidentes de seguridad de la información, ciberseguridad y protección de datos personales.
- Realizar un análisis para determinar las causas de cada incidente.
- Evaluar la naturaleza y el impacto de los incidentes de seguridad identificados para determinar la gravedad y la respuesta adecuada.
- Desplegar acciones correctivas para contener, erradicar y recuperar de los incidentes de seguridad.
- Mantener un registro detallado de cada incidente, incluyendo la naturaleza del incidente, las acciones tomadas y los resultados.
- Realizar análisis post-incidente para identificar mejoras en los procesos de gestión de incidentes y minimizar la probabilidad de recurrencias.
- Manejo de evidencias forenses de los incidentes de seguridad de la información.
- Mantener un plan de capacitación de las personas que se ocupan de los incidentes de la seguridad de la información.

8.11.2. Reporte de eventos y debilidades de seguridad:

- Todos los empleados, servidores y partes interesadas responsables de la prestación de servicios en **[NOMBRE DE LA EMPRESA]** deben reportar al área de tecnología, a través de los canales establecidos, cualquier evento, riesgo o incidente de seguridad de la información, ciberseguridad y protección de datos personales que identifiquen en el desempeño de sus funciones.
- Cualquier debilidad identificada en los sistemas de seguridad de la información debe ser reportada inmediatamente al área de tecnología para su evaluación y tratamiento.

8.11.3. Evaluación y decisión sobre los eventos de seguridad de información:

- Los eventos de seguridad de la información deberán ser evaluados de manera sistemática para decidir sobre la respuesta apropiada, priorizando aquellos que representen un mayor riesgo para la empresa.
- Una vez evaluados, se debe activar el plan de respuesta a incidentes, asegurando que se sigan los procedimientos establecidos para la contención, eliminación y recuperación de los incidentes.
- Se debe evaluar si la organización tiene la capacidad para resolver el incidente por sí misma o necesita ayuda de terceros.

8.11.4. Tratamiento y aprendizaje de las amenazas:

- Después de la gestión de un incidente, se debe realizar una revisión que permita extraer lecciones aprendidas y actualizar las políticas y procedimientos de seguridad de la información en base a estas.
- Compartir información sobre amenazas externas con grupos especializados de respuesta ante incidentes y organismos de seguridad para mejorar las capacidades de tratamiento de amenazas.

- Incluir los resultados del análisis de amenazas en las actividades de identificación de riesgos y en la configuración de dispositivos de prevención y detección de eventos de seguridad.

8.11.5. Recolección de evidencias:

- Seleccionar fuentes para la recopilación de información sobre amenazas de proveedores independientes y grupos especializados en seguridad de la información.
- Recopilar información sobre amenazas informáticas que puedan afectar los activos de información.
- Los controles según la Norma ISO/IEC 27002 para mantener una base de conocimientos sobre los incidentes en la seguridad de la información son:

    - Creación de un registro que considere
    - Volumen de incidentes producidos
    - Tipología de incidentes producidos
    - Coste de la resolución de la incidencia
    - Impacto de la incidencia
    - Solución aplicada

8.12. POLÍTICA GESTIÓN CONTINUIDAD DEL NEGOCIO

La empresa **[NOMBRE DE LA EMPRESA],** es consciente de la dependencia de los sistemas de información y el impacto que puede llegar a tener una interrupción en su disponibilidad, por lo tanto, integra medidas preventivas y planes de contingencia que buscan garantizar la continuidad de las operaciones de los servicios de información, así como la continuidad del sistema integrado de gestión de la seguridad de la información en medio de eventos de contingencia. En consecuencia, ha establecido los siguientes lineamientos:

8.12.1. Planificación de la continuidad de la seguridad de la información:

- Los planes de continuidad del negocio de **[NOMBRE DE LA EMPRESA]** deberán incluir explícitamente los requisitos de la seguridad de la información, garantizando que las medidas de seguridad se mantengan durante situaciones de crisis y desastres.
- Se llevará a cabo un análisis de riesgos para identificar las amenazas que puedan comprometer la seguridad de la información durante una interrupción de los servicios.
- Realizar un análisis de impacto que evalúe cómo las situaciones de emergencia (como la pérdida de energía, fallos en las comunicaciones o colapsos de infraestructura) afectan los requisitos de seguridad de la información.
- El plan incluirá protocolos de emergencia para la gestión de incidentes que comprometan la continuidad de los servicios, asegurando que se mantengan las capacidades de respuesta adecuadas.

8.12.2. Implementación de la continuidad de la seguridad de la información:

- Se debe establecer una estructura de gestión clara que defina las responsabilidades de cada miembro del equipo en la continuidad y recuperación de los sistemas de información.
- Se identificarán los niveles de competencia necesarios para cada función dentro del plan de continuidad, asegurando que los encargados posean la formación y habilidades requeridas para ejecutar sus responsabilidades.
- Se designarán personas específicas para desempeñar funciones clave en la continuidad de la seguridad de la información y la recuperación ante desastres, asegurando que cada función esté cubierta.
- Se documentarán los procedimientos a seguir para gestionar eventos destructivos que puedan afectar la seguridad de la información
- Se asegurará que los procedimientos tengan en cuenta los objetivos y requisitos mínimos de continuidad de la seguridad de la información definidos en el análisis previo

8.12.3. Verificar, revisar y evaluar la continuidad de la seguridad de la información:

- Verificar la aplicabilidad de los controles establecidos en el plan de continuidad, asegurando que estos sigan siendo relevantes y eficaces frente a las amenazas y vulnerabilidades actuales.
- Se debe verificar que todos los activos de información estén incluidos en el plan de continuidad.
- Se debe revisar la implicación del personal en las tareas de recuperación, evaluando que todos los empleados y partes interesadas estén al tanto de sus responsabilidades en caso de un incidente.
- Evaluar la efectividad de las medidas de continuidad y realizar ajustes basados en los resultados obtenidos y en el aprendizaje de incidentes anteriores.

8.12.4. Disponibilidad de las instalaciones de procesamiento de información:

- Se debe identificar aquellos sistemas de información cuya arquitectura no garantice la disponibilidad necesaria para los procesos del negocio sin un sistema de respaldo.
- Se debe analizar la viabilidad de implementar sistemas redundantes para los activos de información críticos.
- Se deben realizar pruebas periódicas para asegurar el correcto funcionamiento de los sistemas redundantes. Estas pruebas deben incluir:
    - Verificación del rendimiento y disponibilidad de los sistemas de respaldo.
    - Ejecución de pruebas de transición para asegurar que la conmutación de un sistema principal a un sistema redundante se realice sin interrupciones en el servicio.
- Establecer procedimientos documentados que detallen los pasos a seguir en caso de una caída del sistema principal.

- Evaluar la efectividad de los sistemas de redundancia y realizar ajustes necesarios en función de los cambios en los procesos del negocio o en la infraestructura tecnológica.

8.13. POLÍTICA DE CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

[NOMBRE DE LA EMPRESA], se compromete a dar cumplimiento a toda la legislación y regulación aplicable a su actividad en materia de seguridad de la información y establecer la responsabilidad de dicho cumplimiento sobre todos sus miembros. En este sentido, se velará por el cumplimiento de toda legislación, normativa o regulación aplicable que sea emitida al respecto.

8.13.1. Identificación legislación aplicable y requisitos contractuales:

El área jurídica y el Área de tecnología identificarán, documentarán y mantendrán actualizados los requisitos legales, reglamentarios o contractuales aplicables, relacionados con seguridad de la información que sean aplicables a la empresa **[NOMBRE DE LA EMPRESA]**

- Se debe realizar una revisión periódica de los cambios en leyes, decretos, circulares internas y externas que sean aplicables a **[NOMBRE DE LA EMPRESA]** en materia de seguridad de la información, ciberseguridad y protección de datos personales.
- Los resultados de la actualización del contexto legal y regulatorio se deben integrar al normograma del Sistema Integrado de Gestión de Calidad y Medio Ambiente de **[NOMBRE DE LA EMPRESA]**, asegurando que todos los procesos estén alineados con las normativas vigentes.
- Ante cualquier cambio en las obligaciones legales en materia de seguridad de la información, se debe asignar al área de tecnología la responsabilidad de identificar dichos cambios.
- Asegurar que todos los empleados y partes interesadas reciban capacitación regular sobre las implicaciones de los cambios legales y regulatorios en sus funciones relacionadas con la seguridad de la información y protección de datos, en caso de ser requerido.
- Se debe mantener una documentación completa y actualizada de todos los cambios legales y regulatorios identificados, así como de las acciones tomadas en respuesta a dichos cambios, asegurando la trazabilidad y el cumplimiento normativo.

8.13.2. Derechos de Propiedad Intelectual:

En cumplimiento de la Ley 23 de 1982, la Ley 603 de 2000 y la Decisión 351 de la Comunidad Andina de Naciones, la empresa **[NOMBRE DE LA EMPRESA],** se compromete a:

- Usar material (documentos, fotografías, videos y software) producidos como parte de su ejercicio misional, o hacer uso de material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

- El Área de tecnología garantizará que el software usado por la empresa se encuentre debidamente licenciado y tomará medidas para no permitir a los usuarios instalar software en las estaciones de trabajo de la empresa.
- Los usuarios se comprometen a no instalar software, en los equipos de la empresa, sin la autorización del Área de tecnología y dar cumplimiento a las leyes de derechos de autor y acuerdos de licenciamiento de software.

8.13.3. Privacidad y protección de información de datos personales:

[NOMBRE DE LA EMPRESA], es depositario de datos personales por lo tanto deberá dar cumplimiento a lo establecido en la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013 y lo consignado en el artículo 15 de nuestra Constitución Política, para lo cual establecerá una política para su manejo y los procedimientos necesarios para su cumplimiento.

8.13.4. Reglamentación de controles criptográficos:

En materia de controles criptográficos, se dará cumplimiento a lo establecido por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según aplique.

8.13.5. Revisiones de seguridad de la información:

[NOMBRE DE LA EMPRESA] llevará a cabo revisiones periódicas del sistema de gestión de la seguridad de la información, ciberseguridad y protección de datos personales con el objetivo de evaluar:

- Determinar si el sistema está alineado con los objetivos establecidos en materia de seguridad de la información y protección de datos.
- Evaluar las oportunidades de mejora identificadas en las áreas de seguridad de la información y ciberseguridad, y asegurar que se apliquen de manera efectiva.
- Revisar la gestión de cambios internos y externos que puedan impactar el sistema de gestión de seguridad de la información y asegurar que se adopten las medidas adecuadas.

Las revisiones del sistema de gestión de la seguridad de la información se realizarán de forma independiente para garantizar la objetividad y la imparcialidad en la evaluación. El resultado de estas revisiones servirá como base para la mejora continua del sistema y para asegurar que se cumplan las normativas vigentes y los estándares de la organización.

9. VIGENCIA DEL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El presente manual rige a partir de la fecha de su publicación y deja sin efectos las demás disposiciones institucionales que le sean contrarias. Toda información no contemplada en el presente manual se reglamentará de acuerdo al Régimen General de Protección de Datos Personales vigente en Colombia.

Las bases de datos en las que se registrarán los datos personales tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en este manual. Una vez se cumpla(n) esa(s) finalidad(es) y siempre que no exista un deber legal o contractual de conservar su información, sus datos podrán ser eliminados de nuestras bases de datos.

Como constancia de lo anterior, esta política y lineamientos de seguridad de la información fue aprobada y firmada por el Representante legal el día DD de MMMM de 202A.

[Nombre del representante legal]

Representante Legal

CONTROL DE CAMBIOS		
Fecha	**Versión**	**Descripción del cambio**
DD-MMM-AAAA	00	Se crea documento alineado con la norma internacional ISO/IEC 27001:2022 e ISO/IEC 27002:2022