Versión	Fecha	Descripción del cambio
1	14/12/2023	Generación política de seguridad

1. INTRODUCCION

PRESENTACION DE LA COMPAÑIA

Independence Drilling S.A. es una empresa colombiana líder en la prestación de bienes y servicios petroleros de Colombia, con 44 años de experiencia realizando perforación y mantenimiento de pozos de petróleo y gas.

Más de 1.400 personas hacen parte de nuestro equipo y trabaja con pasión y empeño de la mano de clientes, proveedores, comunidad y demás grupos de interés, para construir valor y confianza en el territorio, comprometidos con la búsqueda de la excelencia, el respeto por la gente y la protección del medio ambiente.

IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACION

La importancia de la seguridad de la información radica en salvaguardar los activos críticos y sensibles de una organización, incluyendo datos, sistemas y procesos, contra amenazas internas y externas. La integridad, confidencialidad y disponibilidad de la información son fundamentales para la continuidad del negocio y la construcción de la confianza con clientes, socios y empleados. La pérdida, robo o compromiso de datos puede tener consecuencias significativas, desde daños financieros y reputacionales hasta violaciones regulatorias. En un entorno digital cada vez más interconectado, la seguridad de la información no solo es esencial para proteger la propiedad intelectual y la privacidad, sino también para garantizar la resiliencia de las operaciones comerciales en un mundo donde las amenazas cibernéticas son una realidad constante.

2. OBJETO:

Establecer los lineamientos que garanticen la protección de información de LA COMPAÑÍA que son objeto de tratamiento, a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la organización alineados con el contexto de direccionamiento estratégico y de gestión del riesgo, con el fin de dar cumplimiento a las normas, leyes, políticas y procedimientos de atención de derechos de los titulares, teniendo en cuenta los criterios de integridad, no repudio, disponibilidad, legalidad, confidencialidad, recolección, almacenamiento, uso y circulación de la información.

OBJETIVOS ESPECÍFICOS

- Definir los lineamientos y controles de acceso de seguridad de la información para la gestión de datos personales

- Brindar la debida protección a los intereses y necesidades de los titulares de la Información personal tratada en LA COMPAÑÍA.

- Generar compromiso de todos los trabajadores con los cuales la organización tenga interacción respecto al correcto manejo y protección de la información que es gestionada y resguardada en LA COMPAÑÍA.

- Identificar e implementar los controles tecnológicos necesarios para fortalecer la función de la seguridad de la información.

- Implementar buenas prácticas del Sistema de Gestión de Seguridad de la Información.

- Proteger la información que se encuentre dentro de los activos tecnológicos de LA COMPAÑÍA.

- Asegurar la identificación y gestión de los riesgos a los cuales se exponen los activos de información de LA COMPAÑÍA.

- Dar cumplimiento a las exigencias de la normatividad vigente en materia de Protección de Datos Personales.

- Cumplir con los principios de seguridad de la información: Disponibilidad, integridad y confidencialidad.

- Concientizar a los trabajadores de LA COMPAÑÍA sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información.

- Regular el tratamiento de la seguridad de la información personal en sus etapas de recolección, almacenamiento, administración, transferencia, transmisión, actualización, supresión y protección de los datos que se reciban.

- Implementar los controles de seguridad de la información personal para el Recurso Humano antes de la vinculación y una vez finalizado el contrato laboral.

- Asegurar el control de acceso a la información personal, tanto en las instalaciones físicas como a nivel tecnológico.

- Definir los accesos a la información personal de las bases de datos con información personal sensible.

- Asegurar los procesos que permitan contar con copias de respaldo a la información personal.

- Implementar las acciones pertinentes para la protección de la información personal mediante el acceso remoto.

- Definir los responsables y autoridades de tratamiento de datos de las bases que cuentan con información personal sensible

- Implementar los controles de seguridad de información personal que se realizan a través de terceros ajenos a la organización.

- Implementar medidas de seguridad para garantizar el uso o extracción de la información de manera remota.

3. AMBITO DE APLICACIÓN:

De acuerdo con la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", los Decretos 1377 de 2013 y 886 de 2014 (hoy incorporados en el Decreto único 1074 de 2015), la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013. LA COMPAÑÍA INDEPENDENCE DRILLING S.A., (en adelante "LA COMPAÑÍA"), adopta mediante el presente documento las políticas para garantizar el derecho constitucional a la seguridad de la información, permitiendo conocer, actualizar, rectificar, suprimir y revocar la autorización de la información registrada en las bases de datos y/o archivos de la organización. Esta política es aplicable para toda la información personal almacenada en de clientes, prospectos, proveedores, empleados o de cualquier persona que suministre información a LA COMPAÑÍA.

Establecer políticas sobre la información es una prioridad para LA COMPAÑÍA y por tanto es responsabilidad de todos velar que no realicen actividades que contradigan la esencia y el espíritu de cada una. LA COMPAÑÍA ha elaborado la

presente política, cuya aplicación es de carácter obligatorio para todas las personas naturales o jurídicas que hagan uso de los datos registrados en las bases de datos de estas, con el fin de proporcionar lineamientos para el cumplimiento de las obligaciones legales para la protección de datos personales. Se realizará actualizaciones de la política en cualquier momento por motivos legislativos, regulatorios o jurisprudenciales, políticas internas o circunstancias que lo ameriten. Se deberá informar oportunamente mediante comunicado a todas las partes involucradas.

MARCO LEGAL

Las políticas de seguridad informática que se definen en este documento se basan en las buenas prácticas y lineamientos establecidos en las siguientes leyes y normas:

- Ley Estatutaria 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- DECRETO 1377 DE 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de organizaciones públicas y privadas". Artículo 20. Libertad de Información. "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- LEY 1266 DE 2008, Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información

4. ALCANCE

Esta política aplica para toda la información personal registrada y definida en la MATRIZ ANEXA SEGURIDAD DE INFORMACIÓN y almacenada en las bases de datos y repositorios de LA COMPAÑÍA definidas en esta matriz, en los cuales se definen los roles de administración y uso de la información personal, y demás bases de datos personales que LA COMPAÑÍA construya e identifique. Cubre todos los aspectos administrativos, legales y de control que deben ser cumplidos por todos los trabajadores, para conseguir un nivel adecuado de seguridad de la información, reducir y mitigar los riesgos relacionados con fraude, filtraciones, hurto y uso inadecuado de la misma definidos en la MATRIZ SEGURIDAD DE LA INFORMACIÓN. Se tendrá en cuenta una fecha periódica anual para la actualización y publicación de cambios de la política según corresponda.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Para LA COMPAÑÍA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.
De acuerdo con lo anterior, esta política aplica para todos los trabajadores, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema de Gestión de Seguridad de la Información, (en adelante "SGSI") están determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de LA COMPAÑÍA.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus clientes, socios y trabajadores.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

LA COMPAÑÍA establece los siguientes principios de seguridad para soportar y aplicar buenas prácticas del SGSI:

- Las responsabilidades frente a la seguridad de la información son definidas, compartidas, publicadas y aceptadas por cada uno de los trabajadores.
- Adoptará y aplicará controles, acciones y buenas prácticas para proteger la información almacenada, procesada, publicada o resguardada por los diferentes procesos de LA COMPAÑÍA, con el fin de minimizar impactos financieros, operativos, administrativos o legales.

- Asegurará el cumplimiento de la política de tratamiento de datos personales y las políticas legales, regulatorias, contractuales relacionadas a la seguridad de la información establecidas por LA COMPAÑÍA, con el fin de garantizar la recolección, almacenamiento, uso, circulación o supresión de datos que se utilicen para el desarrollo de su actividad.
- Seguimiento en cada uno de los sistemas contratados por la compañía para verificar que cumplan con los controles de seguridad y controles de acceso para evitar posibles ataques y fugas de la información almacenada en las bases de datos de LA COMPAÑÍA.
- LA COMPAÑÍA es responsable de generar, establecer, actualizar, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos.
- El incumplimiento a la política de Seguridad de la Información traerá consigo, las consecuencias previstas en la presente.

5. EMISOR:

MACROPROCESO	PROCESO
Tecnología	Aseguramiento

6. VIGENCIA

Aplica a partir de su publicación en diciembre 2023.

7. POLÍTICA

POLÍTICA DE SEGURIDAD DE INFORMACIÓN DE LA COMPAÑÍA

LA COMPAÑÍA cuenta con bases de datos personales que han sido recolectadas a través de diferentes fuentes manejadas por esta y son reportadas de conformidad con la normatividad vigente.

Los datos personales almacenados en las bases de datos que conserva LA COMPAÑÍA son objeto de tratamiento, recolección, almacenamiento, procesamiento, uso, análisis, transmisión o transferencia, atendiendo de forma estricta los deberes de seguridad y confidencialidad regulados por la Ley 1581 de 2012 y el Decreto 1074 de 2015.

LA COMPAÑÍA se compromete a administrar los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de los activos en cumplimiento a los requisitos aplicables.

A continuación, se establecen las políticas de seguridad que soportan el SGSI de LA COMPAÑÍA:

7.1 Política de Tratamiento de Datos Personales

LA COMPAÑÍA establece los lineamientos para la administración y tratamiento de datos personales conforme a las regulaciones contenidas en la Ley 1581 de 2012, como responsable del tratamiento de datos personales, garantizará la seguridad, integridad, confidencialidad de los datos sensibles o personales que se hayan recogido y tratado en operaciones tales como la recolección, almacenamiento, uso, circulación o supresión en desarrollo de su actividad, de acuerdo con las normas vigentes y las políticas definidas para este efecto. Estos datos se deben utilizar únicamente para los fines autorizados por el titular. En caso de encargar a un tercero, el tratamiento de datos personales, LA COMPAÑÍA exigirá al tercero la implementación de los lineamientos necesarios para la protección de los datos personales y por lo menos el cumplimiento de la presente política.

Así mismo, buscará proteger la privacidad de la información personal de sus trabajadores, estableciendo los controles necesarios para preservar aquella información que LA COMPAÑÍA conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias y no sea publicada, revelada o entregada a trabajadores sin autorización.

Conozca la política de tratamiento de los datos personales de LA COMPAÑÍA en la página https://www.independence.com.co/tratamiento-de-datos/.

7.1.1 Lineamientos para el Tratamiento de Datos Personales

Responsabilidades de los Trabajadores que manejan bases de datos personales

- Las áreas responsables encargados de los datos personales deben contar con la autorización firmada para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de LA COMPAÑÍA.

- Conservar la copia o evidencia de la respectiva autorización otorgada por el titular.
- La información sensible, es decir aquella que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, será objeto de tratamiento por aquellas personas autorizadas y conforme lo dispone la regulación vigente y la presente política para el tratamiento de datos personales de LA COMPAÑÍA.
- Los responsables de los datos personales deben controlar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos, para esto se debe revisar y mantener actualizada periódicamente la matriz establecida para la asignación de personal autorizado a información confidencial. ANEXO-MATRIZ SEGURIDAD DE INFORMACIÓN
- Suscribir los acuerdos de confidencialidad con los encargados del tratamiento de dichos datos personales.
- Acoger las directrices técnicas y lineamientos establecidos para el intercambio de datos con los encargados del tratamiento de dichos datos personales y para el envío (mensaje de texto, correos electrónicos, etc), con el fin de prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Comunicar las novedades y actualizaciones realizadas a los datos que se hayan utilizado para validar la correcta aplicación de las medidas y directrices estipuladas.
- Los trabajadores deben guardar la discreción correspondiente o la reserva absoluta con respecto a la información de LA COMPAÑÍA y/o de las bases de datos que trata.

7.2 Política de Seguridad de la Información del Recurso Humano

LA COMPAÑÍA establece acciones para asegurar que los trabajadores entiendan sus responsabilidades, como usuarios y sus roles asignados para reducir el riesgo de fraude, hurto, filtración o uso inadecuado de la información y de las instalaciones. Se debe asegurar que los trabajadores, adopten sus responsabilidades en relación con esta política y actúen de manera consistente frente a las mismas.

7.2.1 Lineamientos de seguridad para los recursos humanos

Responsabilidades antes de la contratación

- Los candidatos, aspirantes y trabajadores deben emitir autorización a LA COMPAÑÍA para el tratamiento de sus datos personales de acuerdo con la ley 1581 de 2012, por el cual se establecen disposiciones generales de Habeas Data y se regula el manejo de información contenida en base de datos personales, lo que se reflejará en las cláusulas de los contratos.

Responsabilidades durante el vínculo contractual

- Como parte de la relación laboral, los trabajadores que manejen bases de datos personales deben suscribir un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de LA COMPAÑÍA.
- Todos los trabajadores que tengan acceso a datos personales deben proteger la información a la cual acceden para evitar su perdida, alteración indebida o destrucción.
- Todos los trabajadores están en la obligación de informar posibles incidencias relacionadas a la seguridad de la información en cuanto a datos personales.

Responsabilidades terminación de la relación laboral o cambio de cargo

- El trabajador debe entregar todos los activos de información físicos y/o electrónicos que le fueron asignados, de acuerdo con el procedimientos de terminación de la relación laboral o cambio de cargo y con el paz y salvo entregado por Gestión humana.
- Cuando se realiza la desvinculación de un trabajador que tenga información digital y física el equipo de Gestión Humana y/o Jefe inmediato debe informar a través de la mesa de ayuda para proceder con la copia de seguridad e inactivación del usuario en los diferentes sistemas de información.
- Cuando un usuario realiza cambio de cargo, se debe revisar los accesos y permisos para renovarlos, actualizarlos o mantenerlos, estos cambios deben ser informados por el equipo de Gestión Humana semanalmente a mesa de ayuda.

7.3 Política de Gestión y Uso de Activos de Información

LA COMPAÑÍA como propietaria de la información digital y física, así como de la información generada, procesada, almacenada y transmitida por sus plataformas tecnológicas, otorga responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

Los administradores de estos activos son los trabajadores autorizados y son los responsables de la información de los procesos a su cargo, archivos digitales y físicos y recursos tecnológicos.

7.3.1 Lineamientos de Gestión y Uso de Activos de Información

Responsabilidades de la Gerencia Corporativa de TI

- Aplicar buenas prácticas y lineamientos establecidos dentro de esta política para el adecuado uso de los recursos tecnológicos en LA COMPAÑÍA.
- LA COMPAÑÍA debe contar con unas herramientas de seguridad (Ej. firewall, sistemas de prevención, antivirus y detección de intrusos para la conexión a internet). La administración, control y monitoreo de estos servicios está bajo la responsabilidad de la Gerencia Corporativa de TI o quien haga sus veces.
- Seguimiento de las pruebas de vulnerabilidad realizadas por los Terceros contratados para los diferentes recursos tecnológicos, con el fin de detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. El tercero debe revisar y analizar las vulnerabilidades y tomar medidas correctivas para garantizar la mitigación de riesgos.
- Recibir recursos tecnológicos de trabajo para su reasignación o disposición final, y generar copias de seguridad de la información.
- Administrar, mantener y actualizar el inventario de los activos de información.
- Establecer los requerimientos mínimos de seguridad que deben cumplir los sistemas de información a desarrollar, actualizar o adquirir.
- Periódicamente, se debe efectuar la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de

LA COMPAÑÍA y en el caso que lo realice un trabajador se considerará como falta grave.

- Garantizar la disponibilidad de información almacenada en los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de estos.
- Realizar borrado seguro en los equipos de cómputo y demás dispositivos, una vez se realiza su devolución al almacén para dar de baja al activo.
- Informar y documentar la descontinuación de el/los sistemas de información que deban ser retirados por obsolescencia o fallas que afecten directamente los procesos de LA COMPAÑÍA.
- Cumplir con lo dispuesto en el Anexo 4 del manual del usuario del registro nacional de bases de datos – RNBD proferido por la Superintendencia de Industria y Comercio.
- Se debe realizar backup total de todos los sistemas de información contratados por la compañía, de acuerdo con lo establecido por contrato con cada proveedor y su periodicidad diaria, semanal y mensual según corresponda.

Responsabilidades de los trabajadores

- Actuar como propietarios de la información física y electrónica de la organización, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Generar, actualizar y mantener un inventario de los activos de información que están bajo la dependencia de su área o proceso, acogiendo las indicaciones de las guías de clasificación de la información.
- Monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Los recursos tecnológicos de LA COMPAÑÍA deben ser utilizados de forma ética, con el único fin de llevar a cabo las labores asignadas y en cumplimiento de las leyes y reglamentos vigentes, para evitar daños o pérdidas sobre la operación; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Todos los recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- Toda la información que provenga de archivos externos a LA COMPAÑÍA tiene que analizarse con el antivirus configurado por la Gerencia Corporativa de TI.

- No está permitido la instalación ni uso de software diferente al adquirido y autorizado por LA COMPAÑÍA sin el consentimiento de sus superiores y visto bueno de la Gerencia Corporativa de TI.
- Los trabajadores no pueden realizar copias de seguridad de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada, deben solicitarlo a la Gerencia Corporativa de TI con autorización del jefe inmediato; La copia de archivos de LA COMPAÑÍA, así como el robo, daño intencional o utilización para fines distintos a las labores propias asignadas, se sancionarán de acuerdo con las normas y legislación vigentes.
- No está permitido la conexión de equipos de cómputo y de comunicación ajenos a la red de LA COMPAÑÍA.
- Los documentos que se impriman en las impresoras de LA COMPAÑÍA deben ser de uso específico para las funciones asignadas a su cargo.
- Los trabajadores que realizan impresiones de documentos con clasificación pública reservada, privada o semiprivada, deben asegurar que no esté a disposición de otras personas y no deben dejar la impresora desatendida, preservando la confidencialidad de los datos.
- Evitar la divulgación o destrucción de información sin previa autorización o uso indebido de la información y alteraciones intencionales o no justificadas

7.4 Política de Gestión y Control de Accesos

LA COMPAÑÍA define los lineamientos para asegurar un acceso controlado a la información y plataformas informáticas, considerándolas como importantes para el SGSI. El control de acceso a la Información se realiza aplicando privilegios necesarios para la realización de las actividades asignadas.

7.4.1 Lineamientos de la Gestión y Control de Accesos

Responsabilidades de la Gerencia Corporativa de TI

- Definir en conjunto con las áreas funcionales los roles y permisos de acceso a los diferentes sistemas y repositorios de información de LA COMPAÑÍA, y establecer controles de seguridad y seguimientos de medición periódica, con el fin de prevenir riesgos que afecten la confidencialidad, disponibilidad e integridad de la información. Así mismo verificar y monitorear que cada activo de información de LA COMPAÑÍA se asigne a un "Propietario", y cuente con los requisitos de seguridad como políticas de protección, perfiles de acceso y respuesta ante incidentes.

- La Gerencia Corporativa de TI solo presta servicios de soporte técnico a equipos propios o de su tenencia para el desarrollo del objeto social de LA COMPAÑÍA.
- Gestionar en conjunto con las áreas funcionales los incidentes de seguridad de la información que se presenten, así como la investigación, determinación de causa, posibles responsables y recomendaciones de mejora para los sistemas afectados.
- Informar por medio de comunicados formales los eventos que estén en contra de la seguridad de la información.
- Cumplir con lo dispuesto en el manual del usuario del registro nacional de bases de datos – RNBD proferido por la Superintendencia de Industria y Comercio.
- Los equipos de infraestructura y sistemas de información realizarán dos veces al año (Cada 6 meses) la verificación, actualización y/o depuración de cierres masivos de tickets si no han tenido respuesta oportuna del usuario final o que por su complejidad se hayan convertido en evolutivos.
- Los equipos de infraestructura y sistemas de información realizarán dos veces al año (Cada 6 meses) la verificación, actualización y/o depuración de usuarios que no estén activos en la organización con el fin de validar todos los accesos que correspondan por sistemas de información y/o bloqueo de accesos.
- Es responsabilidad de la gerencia de TI tener el control de acceso ambiental o Físico al Datacenter, asignar accesos, y proteger los activos de información que se tengan almacenados.
- Toda persona externa al área que requiera el ingreso al Datacenter debe hacerlo con el acompañamiento de personal de la Gerencia de TI

Responsabilidades de los trabajadores

- Definir, autorizar, clasificar, restringir y delimitar los criterios y niveles de acceso a la información de acuerdo con los roles y responsabilidades de los trabajadores, que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- Revisar periódicamente y aplicar controles de seguridad a la consistencia de la clasificación de la información, para verificar el cumplimiento de los requerimientos establecidos por LA COMPAÑÍA.
- Los trabajadores que tengan bajo su responsabilidad la custodia de la información física deben mantener el control de acceso a esta información. Deben bloquear sus equipos de cómputo cada vez que se retiren de su puesto de trabajo, con el fin de evitar la filtración de información

- Los cambios de permisos de acceso a servicios de TI para los trabajadores deben ser solicitado a la Gerencia Corporativa de TI, mediante el envío de una comunicación oficial a través de la mesa de servicio, debe estar autorizado por el jefe inmediato o el responsable asignado.
- Determinar los tiempos de retención de la información en conjunto con las áreas que se encarguen de su protección y almacenamiento de acuerdo con los lineamientos y políticas de LA COMPAÑÍA.

7.4.2 Lineamientos de Uso de Internet

Responsabilidades de la Gerencia Corporativa de TI

- El acceso y uso de redes sociales está autorizado solo para los trabajadores que cuenten con aprobación de la Gerencia Corporativa de TI, previa autorización del jefe inmediato y se deben usar exclusivamente para las tareas asignadas.
- Los recursos tecnológicos usados para acceder a internet son propiedad de LA COMPAÑÍA, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso la información, respetando en todo momento el derecho a la privacidad y a la seguridad de los datos personales consagrados en la Ley 1581 de 2012.

Responsabilidades de los trabajadores

- LA COMPAÑÍA permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los trabajadores, evitando errores, pérdidas y modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.
- El uso de correo electrónico asignado por LA COMPAÑÍA debe ser usado exclusivamente para las tareas propias del trabajador, no debe utilizarse para otro fin.
- Los trabajadores no están autorizados a enviar cadenas de correo, correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red y correos con contenido que atente la integridad y dignidad de las personas y el bueno nombre de LA COMPAÑÍA.
- Todos los mensajes son sujetos a análisis frente a amenazas y ataques informáticos dirigidos y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de LA COMPAÑÍA.

- Información que se publique o divulgue por cualquier medio de internet, de cualquier trabajador o contratista de LA COMPAÑÍA que sea creado a nombre personal, se considera por fuera del alcance de las políticas de la seguridad de la información y por lo tanto su disponibilidad, integridad, confiabilidad y daños y perjuicios que pueda llegar a causar, son completamente responsabilidad de la persona que las haya realizado.
- No se debe utilizar el nombre de LA COMPAÑÍA en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la organización.

7.4.3 Lineamientos de Uso y Protección de Claves de Acceso

- LA COMPAÑÍA debe concientizar y controlar a través de buenas prácticas de seguridad el uso y protección de contraseñas; ya que son el medio de validación de identidad de los usuarios para el ingreso a las instalaciones y recursos tecnológicos. Desde la gerencia de TI se emitirán E-cards en un periodo trimestral, informando sobre la importancia del manejo de la seguridad de información y las diferentes herramientas disponibles para el uso correcto

Las contraseñas deben cumplir con los siguientes requisitos:

- Debe tener mínimo ocho (8) caracteres alfanuméricos.
- Debe contener caracteres en mayúscula.
- Debe contener caracteres en minúscula.
- Base de 10 dígitos (0 a 9).
- Contener al menos un carácter especial (Ejemplo i, %, &, *, +).
- No debe contener información personal, ni productos a resaltar de LA COMPAÑÍA.
- No asociar fechas especiales.
- Nunca utilizar sus contraseñas personales en el entorno laboral.
- El usuario debe cambiar obligatoriamente la contraseña, la primera vez que ingrese al sistema.
- La contraseña debe cambiarse obligatoriamente cada 3 meses, o cuando lo establezca la Gerencia Corporativa de TI.
- No usar caracteres iguales consecutivos.
- No debe contener solo números o solo alfabéticos.
- Las contraseñas no deben estar visibles ni registradas en papel, o almacenadas en sistemas electrónicos personales.
- No deben compartirse con los demás usuarios.

- Las contraseñas de ninguna manera pueden ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
- Se evita el revelar contraseñas en cuestionarios, reportes o formularios.
- Se evita el activar o hacer uso de la utilidad de recordar clave de las aplicaciones.

Responsabilidades de la Gerencia Corporativa de TI

- Si se detecta o sospecha que las actividades de una cuenta de usuario pueden comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración de la Gerencia Corporativa de TI.
- Las contraseñas "Predefinidas" de los sistemas de información deben ser desactivadas o cambiadas después de la instalación del producto.
- La creación del usuario se realiza de acuerdo con nombres y apellidos para todos los sistemas de información indicando: primeras iniciales de nombres y el primer apellido: Ejemplo: JUAN MANUEL DAZA usuario: JMDAZA.
- Los administradores de los recursos tecnológicos pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y número de intentos efectuados para determinar posibles accesos indebidos o no autorizados.

Responsabilidades de los trabajadores

- Las contraseñas son personales, ningún usuario debe acceder a la red o recursos de tecnología utilizando una cuenta de otro usuario.
- Los trabajadores son responsables del uso de las claves de acceso que se le asignen para la utilización de los recursos de tecnología.
- No deben incluir contraseñas en ningún proceso de registro automatizado.
- Deben asegurar el cierre de sesión de los sistemas de información una vez finalicen o pausen sus funciones.
- Los usuarios y claves de los administradores de los recursos tecnológicos de Gerencia Corporativa de TI son de uso personal e intransferible.
- No se debe intentar modificar los parámetros de la seguridad de los sistemas de la red de LA COMPAÑÍA.

7.4.4 Lineamientos Conexiones Remotas

LA COMPAÑÍA establece los lineamientos para los trabajadores que requieran y se les autorice el acceso a recursos tecnológicos a través de conexión remota por medio de herramientas VPN para el desarrollo de sus actividades la cual debe ser aprobada, registrada y auditada, por la Gerencia Corporativa de Tecnología. Al usar la tecnológica VPN - Virtual Private Network (Red privada virtual), se busca prevenir la interceptación de posibles atacantes en la conexión. Este tipo de conexión es segura por la aplicación de una capa de cifrado y autenticación en la ruta de la comunicación (denominado túnel de comunicación).

Responsabilidades de la Gerencia Corporativa de TI

- Las actividades de acceso remoto (uso de VPN - Virtual Private Network) a los recursos tecnológicos de LA COMPAÑÍA, se autorizan de acuerdo con las necesidades específicas del área solicitante. Son esporádicas, política de directorio activo
- Auditar y monitorear el estado de las conexiones remotas del personal autorizado, con el fin de evitar el uso inadecuado de la información de la organización.

Responsabilidades de los trabajadores

- Los usuarios que requieren conectarse a los recursos tecnológicos por conexión remota deben realizarla a través de conexión VPN segura, configurada por la Gerencia Corporativa de TI con el usuario y contraseña asignada, de acuerdo con la definición de segmentación de la red de cada sistema publicado a través de red interna o externa.
- Mantener en total reserva las credenciales que les han sido otorgadas para su seguridad.
- Mantener la confidencialidad y protección de la información a la que tienen acceso fuera de la organización.
- Usar el antivirus instalado por LA COMPAÑÍA, para brindar una mayor protección a los archivos e información que están gestionando.
- Se prohíbe, sin excepción alguna, la conexión remota desde redes públicas o equipo de cómputo públicos.

7.5 Política de Seguridad de los Equipos

LA COMPAÑÍA establece los siguientes lineamientos para asegurar la protección de la información en los equipos. Esta debe ser aplicada por todos los trabajadores.

- **Control de Acceso Físico:**
  - Aseguramos que el acceso a las instalaciones del CPD esté restringido a personal autorizado a través del sistema de acceso biométrico y contraseña fuertes para garantizar la autenticación adecuada.

- **Vigilancia y Monitoreo:**
  - Sistema de cámaras de seguridad para monitorear, controlar y registrar actividades en áreas clave con el apoyo del área y personal de seguridad capacitado.

- **Ambiente Controlado:**
  - Se mantiene una temperatura y humedad controladas dentro del CPD mediante equipo de Aire Acondicionado para asegurar el funcionamiento óptimo de los equipos.
  - Contamos con sistema de detección de incendios y supresión de incendios adecuados.

- **Protección contra Intrusiones:**
  - Utilizar sistemas de detección de intrusos para alertar sobre intentos no autorizados de acceso, cámaras de seguridad o medios disuasivos implementado en las instalaciones de la compañía.
  - Reforzar la seguridad física de las instalaciones, como cercas perimetrales y cerraduras de alta seguridad a través de control Biométrico.

- **Respaldo de Energía:**
  - Contamos con sistemas de respaldo de energía, UPS y baterías asociadas para garantizar la continuidad del servicio en caso de cortes de energía.

- **Políticas y Procedimientos:**
  - Establecer políticas y procedimientos claros para el acceso físico y las medidas de seguridad, y asegurarse de que el personal esté debidamente capacitado.

- **Gestión de Visitantes:**
  - Planilla como sistema de registro para visitantes que incluye la identificación y la autorización previa por parte de los lideres del área de TI.
  - Se asegura que los visitantes, proveedores y terceros estén acompañados en todo momento mientras estén en el CPD.

- **Seguridad en el Transporte de Datos:**
  - Implementamos medidas de seguridad para proteger el transporte físico de equipos y datos sensibles digitalmente entre las instalaciones y los Datacenter.

- **Actualización Regular de Sistemas de Seguridad:**
  - Se mantiene actualizados los sistemas de seguridad física regularmente para aprovechar las últimas tecnologías y técnicas de protección.

- **Colaboración con Proveedores de Datacenters:**
  - Colaboramos estrechamente con los proveedores de servicios de datacenter, como Cirion e IFX, para garantizar que cumplan con los estándares de seguridad y adoptar prácticas complementarias dentro de sus instalaciones e implementaciones de infraestructura On-premise.

Estas medidas combinadas proporcionan un enfoque integral para salvaguardar la infraestructura de TI de LA COMPAÑÍA, minimizando los riesgos asociados con amenazas físicas y garantizando la integridad y disponibilidad de los servicios de TI.

7.5.1 Lineamiento de la seguridad en los equipos empresariales

Responsabilidades de la Gerencia Corporativa de TI

- Debe realizar mantenimientos preventivos y correctivos de los recursos tecnológicos de LA COMPAÑÍA.
- Mantener y asegurar los contratos de soporte y mantenimiento en los equipos.
- Generar y asignar estándares de configuración segura para los equipos de los trabajadores de LA COMPAÑÍA.
- Velar porque los equipos que se encuentran sujetos a traslados físicos fuera de LA COMPAÑÍA posean pólizas de seguro.
- La instalación, reparación o retiro de cualquier componente de los recursos tecnológicos de LA COMPAÑÍA, solo puede ser realizado por los trabajadores de la Gerencia Corporativa de TI, o personal de terceras partes autorizado por dicha Gerencia.

Responsabilidades de los trabajadores

- Los trabajadores deben bloquear la sesión de trabajo de su equipo al alejarse, no deben descuidarlos o desbloqueados en sitios públicos.

- Los movimientos y asignaciones de recursos tecnológicos deben informarse a la Gerencia Corporativa de TI, es la única área autorizada de realizar dichos cambios.
- Es responsabilidad del trabajador informar a la Gerencia Corporativa de TI a través de la mesa de servicio, las fallas o problemas presentados en los recursos tecnológicos de propiedad de LA COMPAÑÍA, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

7.6. Política para la Relación e Intercambio de Información con Terceros

LA COMPAÑÍA establece mecanismos de control en sus relaciones con proveedores con el fin de proteger la confidencialidad, integridad y disponibilidad de la información. Aplica a todos los proveedores, contratistas y terceros que tengan relación con LA COMPAÑÍA. Así mismo, garantiza y establece controles para la protección de la información que requiera ser transferida o intercambiada con terceros, se debe establecer Acuerdos de Confidencialidad, Acuerdo de encargo de tratamiento de datos personales y/o transmisión de datos personales, según aplique a cada caso, con las terceras partes con quienes se realice intercambio de información, así mismo, se debe verificar la devolución y/o destrucción de la información, la cual debe ser certificada por el Representante Legal de la persona jurídica, una vez termina la relación contractual con el tercero.

7.6.1 Lineamientos para la Relación e Intercambio de Información con Terceros

Responsabilidades de la Gerencia Corporativa de TI

- Para toda adquisición de recursos tecnológicos realizados por LA COMPAÑÍA, La Gerencia Corporativa de TI, es responsable de definir los requisitos de seguridad, los cuales deben quedar documentados y aprobados por las partes en el contrato o acuerdo.
- Deben establecer las condiciones de conexión adecuada para los equipos de cómputo de los terceros en la red de datos de LA COMPAÑÍA.
- Debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información de LA COMPAÑÍA.
- Autorizar el establecimiento del vínculo de transmisión y transferencia de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

- Todos los contratos de TI que manejen información de la compañía deben mantener la clausula de protección de datos, como parte de los anexos

Responsabilidades de los trabajadores

- Los trabajadores responsables de la realización y/o firma de contratos o convenios con terceras partes en acompañamiento de la Gerencia Corporativa de TI, definen los acuerdos de confidencialidad e intercambio de información, incluyendo los compromisos adquiridos y las penalidades civiles o penales por incumplimiento de dichos acuerdos, Se debe incluir la prohibición de divulgar o destruir la información entregada por LA COMPAÑÍA.
- Los posibles riesgos asociados con el acceso y condiciones de seguridad a los recursos tecnológicos de LA COMPAÑÍA deben ser acordados y documentados, con el fin de asegurar la protección de dichos accesos.
- Asegurar y monitorear que los términos y condiciones de seguridad de la información en los acuerdos realizados entre LA COMPAÑÍA y proveedores se cumplan, así como los incidentes y problemas de seguridad que se generen se deben gestionar oportunamente.
- Asegurar que los datos personales de los usuarios que sean requeridos por terceros sólo puedan ser entregados a personas autorizadas, con previo consentimiento de los titulares de estos, exceptuando en los casos que disponga la ley o por solicitud directa de un ente de control.
- Garantizar que el intercambio de información con terceros quede registrado para auditorias, donde debe almacenar la información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- No está permitido el intercambio de información sensible deberá darse mediante las autorizaciones emitidas por el titular.

Responsabilidades de Terceros

- Los terceros deben tener acceso limitado y con autorización a información reservada y confidencial de LA COMPAÑÍA. Si fuese necesario el suministro de esta información, se debe cumplir con medidas de seguridad que garantice la no divulgación y/o modificación de dicha información.
- Los terceros no pueden tener acceso a áreas, carpetas o zonas donde se encuentre información sensible de la organización. Sí fuera necesario su ingreso, se debe obtener la autorización de la gerencia

encargada de la Gerencia Corporativa de TI, el cual debe monitorear los accesos durante el tiempo que este permanezca en dicha área.

- Cuando se definan cambios en los acuerdos con los terceros; se debe actualizar y notificar los cambios a todas las partes involucradas. Deben ser aprobados por el responsable de la base de datos personales, en los términos previstos en la autorización emitida por el titular, y en la Gerencia Corporativa de TI antes de implementarlos.

7.7 GENERALES

- LA COMPAÑÍA debe aplicar y comunicar los requisitos de esta política a todos los trabajadores en las diferentes dependencias.
- En cualquier momento y sin previo aviso, LA COMPAÑÍA puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales de propiedad de LA COMPAÑÍA, al igual que las unidades de red institucionales, computadores, servidores u otros medios de almacenamiento propios. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
- Los trabajadores tienen prohibido almacenar información personal que no esté relacionada con sus funciones. LA COMPAÑÍA no se hace responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.
- Los trabajadores no deben compartir, publicar o dejar a la vista, datos sensibles (Contraseñas, direcciones IP, entre otros).
- Los trabajadores vinculados con LA COMPAÑÍA deben conservar su escritorio libre de información reservada, semiprivada o privada que pueda ser alcanzada, borrada o usada por terceros o personal que no tenga autorización para su uso o conocimiento.

7.8 SANCIONES

El incumplimiento de la presente política conlleva graves consecuencias las cuales serán siempre tomadas previo análisis de la situación, escuchando en debida forma a todas las partes. Las sanciones aplicables siempre estarán enmarcadas dentro de los principios de legalidad, oportunidad, debido proceso,

inocencia, Derecho a la Defensa, y proporcionalidad siguiendo lo definido en la Constitución Política, la ley y lo dispuesto en el Reglamento Interno de Trabajo. Frente a los trabajadores de LA COMPAÑÍA, se tendrá como falta grave el incumplimiento de la presente política, el de los procesos, formatos, instructivos, matrices o instrucciones, de cualquiera otra disposición y cualquier otra herramienta que haga parte de esta.

8. GESTION DE INCIDENTES

La gestión de incidentes de seguridad de la información mediante la creación de tickets en la Mesa de Ayuda de LA COMPAÑIA es esencial para una respuesta eficaz y organizada:

- **Creación del Ticket:**
  - Cuando se detecte un incidente de seguridad, cualquier miembro del personal debe reportarlo inmediatamente a través de la plataforma de la mesa de ayuda.
- **Información Detallada:**
  - Se debe proporcionar información detallada sobre el incidente, incluyendo la naturaleza del incidente, la hora de detección, las personas o sistemas afectados y cualquier evidencia relevante.
- **Priorización del Incidente:**
  - Implementar un sistema de priorización para clasificar la gravedad del incidente y asignar recursos en consecuencia.
- **Notificación Automática:**
  - Se evaluará y se notificará de ser necesario de acuerdo a la criticidad del incidente para alertar al equipo de respuesta a incidentes (CSIRT) y a otros responsables clave seguidamente se cree el ticket
- **Análisis de Causa Raíz:**
  - Realizar un análisis exhaustivo de la causa raíz del incidente para comprender cómo ocurrió y evitar recurrencias.
- **Etapas de Resolución:**
  - Establecer etapas claras para la resolución del incidente, desde la contención inicial hasta la recuperación y la lección aprendida.
- **Comunicación Proactiva:**
  - Mantener a todas las partes interesadas informadas sobre el progreso de la respuesta de la gestión del incidente de acuerdo con la necesidad.

- **Documentación Detallada:**
  - Registrar de manera detallada todas las acciones tomadas durante la gestión del incidente, lo que facilitará la revisión y la mejora continua.
- **Cierre del Ticket:**
  - Una vez que se haya resuelto completamente el incidente, cerrar el ticket y proporcionar una evaluación post-incidente para futuras mejoras.
- **Revisión Post-Incidente:**
  - Llevar a cabo una revisión post-incidente para evaluar la eficacia de la respuesta, identificar áreas de mejora y actualizar los procedimientos según sea necesario.

Implementar un enfoque estructurado y sistemático para la gestión de incidentes a través de la creación de tickets en la Mesa de Ayuda contribuye a una respuesta más rápida, eficiente y coordinada ante amenazas de seguridad de la información.

9. COPIAS DE SEGURIDAD Y RECUPERACION

Para los equipos de cómputo de los grupos de Directores, Gerentes y Jefes de LA COMPAÑÍA, se realiza Backup de la información contenida en los discos del equipo y son llevados al almacenamiento en la nube, para los equipos de otros funcionarios se realizará este proceso de acuerdo con solicitudes particulares de la organización, para su posterior recuperación u solicitudes particulares por roles de la compañía que requiere de dicha información. Este mismo procedimiento se realiza para el respaldo de las cuentas de correo corporativo MS Office 365.

Los Backups, respaldos y recuperación de la información por parte de los proveedores y sus datacenters a nivel de servidores se realiza de la siguiente manera, los cuales nos reportan la actividad y estado de la toma del Backup mediante correo electrónico al departamento de TI para su respectivo control:

La siguiente política establece las pautas para la realización de respaldos de datos en los datacenters de nuestros proveedores de servicio de alojamiento de servidores, con el objetivo de garantizar la disponibilidad, integridad y recuperación eficiente de la información crítica.

- **Frecuencia de Respaldos:**
  - Se realizarán respaldos diarios, con un enfoque especial en la información que experimenta cambios frecuentes.

- Adicionalmente, se llevarán a cabo respaldos semanales que abarquen todos los datos relevantes acumulados durante la semana.
- Mensualmente, se ejecutarán respaldos completos de todos los datos esenciales para asegurar una captura integral de la información.

- **Procedimientos de Respaldos:**
  - Todos los respaldos se llevarán a cabo de manera automática y programada, utilizando herramientas de respaldo confiables y probadas.
  - Los respaldos diarios se centrarán en los datos modificados desde el último respaldo, garantizando eficiencia y minimizando el impacto en los recursos del sistema.
  - Los respaldos semanales y mensuales comprenderán una revisión exhaustiva de la totalidad de los datos críticos.
- **Periodo de Retención:**
  - Los respaldos diarios se retendrán durante al menos siete días para facilitar la recuperación rápida de datos recientes.
  - Los respaldos semanales se conservarán por un periodo mínimo de cuatro semanas.
  - Los respaldos mensuales se mantendrán durante un periodo mínimo de doce meses para asegurar la conformidad con los requisitos regulatorios y permitir la recuperación de datos a largo plazo.
- **Pruebas y Validación:**
  - Se realizará prueba anual de restauración en caso de ser requerida por la organización para verificar la integridad de los respaldos y garantizar la efectividad del proceso de recuperación para el sistema CORE de LA COMPAÑÍA.
  - Cualquier anomalía o fallo detectado durante las pruebas será abordado y corregido.

- **Registro y Auditoría:**
    - Se realizará auditoría anual para evaluar el cumplimiento de la política y aplicar mejoras continuas según sea necesario para todos los proveedores con los cuales tenga relacionamiento el área de Tecnologías de LA COMPAÑIA.

10. CUMPLIMIENTO Y AUDITORIA

El cumplimiento y la auditoría de la presente política de seguridad de la información son aspectos críticos para asegurar que los controles y procedimientos establecidos se mantengan efectivos y se ajusten a los estándares y regulaciones pertinentes realizados por la entidad BDO Colombia, a continuación, se enuncia las actividades generales:

- Establecimiento de métricas y objetivos
- Monitoreo continuo
- Revisiones periódicas
- Auditorías internas y externas
- Seguimiento de incidentes
- Documentación y registros
- Mejora continua
- Conformidad con Regulaciones
- Comunicación y Concientización

11. REVISION Y ACTUALIZACION

Se revisará y actualizará la presente política de seguridad de la información de forma anual para asegurar su relevancia y efectividad frente a los cambios en el entorno empresarial, las tecnologías y las amenazas cibernéticas que puedan afectar LA COMPAÑÍA.

- **Programación de Revisiones Periódicas:**
    - Establecemos un calendario anual regular para revisar la política de seguridad de la información acorde a la naturaleza de LA COMPAÑÍA.

- **Involucramiento de Stakeholders:**
    - Involucrar a los stakeholders clave en el proceso de revisión, incluyendo a los responsables de seguridad de la información, personal de TI, representantes legales y otros líderes relevantes.

- **Evaluación del Contexto Empresarial:**
  - Revisión del contexto empresarial para identificar cambios en la infraestructura, regulaciones, tecnologías y amenazas. Evalúa cómo estos cambios pueden afectar la efectividad de la política actual.

- **Análisis de Incidentes y Lecciones Aprendidas:**
  - Analizar cualquier incidente de seguridad ocurrido desde la última revisión. Examinar las lecciones aprendidas y determina si se deben realizar ajustes en la política para prevenir incidentes similares en el futuro.

- **Cumplimiento Normativo:**
  - Verificar la conformidad de la política con las normativas y regulaciones aplicables. Asegúrate de que la política esté actualizada para abordar cualquier cambio en los requisitos legales.

- **Retroalimentación del Personal:**
  - Solicitar retroalimentación del personal que interactúa directamente con la política. Pueden ofrecer perspectivas valiosas sobre la aplicabilidad y eficacia de los controles establecidos.

- **Benchmarks y Mejores Prácticas:**
  - Comparar la política con estándares de la industria, benchmarks y mejores prácticas. Y buscar aplicar buenas prácticas en LA COMPAÑÍA para el aseguramiento de la información.

- **Tecnología Emergente:**
  - Considerar la adopción de nuevas tecnologías y evalúa si la política actual debe adaptarse para abordar la seguridad de la información en el contexto de nuevas herramientas o plataformas.

- **Cambio de Personal y Roles:**
  - Actualizar los roles y responsabilidades dentro de la política para reflejar cambios en el personal y la estructura organizativa.

- **Revisión de Documentación:**
  - Revisar la documentación asociada, como manuales de usuario, procedimientos operativos y formularios. Hay que asegurar de

que toda la documentación esté alineada con la política actualizada.

- **Comunicación y Concientización:**
  - Comunicar cualquier cambio en la política al personal relevante y proporcionar capacitación adicional según sea necesario para garantizar la comprensión y cumplimiento continuos.

- **Documentación de Cambios:**
  - Documentar todos los cambios realizados en la política, proporcionando una pista de auditoría clara y un historial de revisiones.

Al seguir este enfoque estructurado, la revisión y actualización de la política de seguridad de la información se convertirá en un proceso integral y proactivo, asegurando que LA COMPAÑÍA se mantenga adaptada y resistente en el siempre cambiante panorama de la seguridad cibernética.

12. DOCUMENTOS APLICABLES

Anexo 1. Matriz Seguridad
Anexo 2. Diseño e implementación de estrategia seguridad de la información

13. GLOSARIO DE TERMINOS

Término	Descripción
Activo	De acuerdo con la norma [ISO/IEC 27000]: Cualquier información, elemento o sistema relacionado con el tratamiento de esta que tenga valor para la organización. Se pueden clasificar de la siguiente manera: - Información: elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en LA COMPAÑÍA. Ejemplo: archivo de Excel "listado de empleados.docx" - Software: Es todo sistema, aplicación o conjunto de procedimientos que se utilizan para la gestión de la información propia de LA COMPAÑÍA. Ejemplo: SAP. - Personal: Son todos los trabajadores de LA COMPAÑÍA, subcontratados, clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información. Ejemplo: Pedro Pérez.
Amenaza	[ISO/IEC 13335-1:2004] Circunstancia, evento o persona que tiene el potencial de causar daño a un sistema y organización.
Autenticación	Proceso de identificar a los usuarios y garantizar que los mismos sean quienes dicen ser.
Autorización	Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
Base de datos	Conjunto Organizado de datos personales que sea objeto de tratamiento.
Cifrado	Conversión de datos de un formato legible a un formato codificado.
Confiabilidad	Asegura que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
Confidencialidad	[NTC 5411-1:2006]. Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CSIRT	Entidad externa gestionada por el MINTIC, Centro de respuesta para incidentes de seguridad en tecnologías de la información. Permite realizar acompañamiento y asesoría cuando se presente un incidente cibernético en cada una de las fases de la gestión de incidentes
Disponibilidad	[NTC 5411-1:2006]. Propiedad de que la información sea accesible y utilizable por solicitud de una EMPRESA autorizada.
Trabajadores	Todo usuario, directivo, empleado, proveedor, practicante y terceros que laboren o tengan vinculo contractual o jurídico con LA COMPAÑÍA y tengan acceso a la información
Habeas data	Recurso legal a disposición de todo individuo que permite acceder a un banco de información o registro de datos que incluye referencias informativas sobre sí mismo.
Integridad	Propiedad de la información que se encarga de salvaguardar la exactitud y validez de datos y mantener el estado completo de los activos de información, proporcionando información confiable y precisa en todo momento.
No repudio	Capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.
Política de seguridad	Normas y directrices que permiten garantizar confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.
Procedimiento	Acciones que se realizan con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo. Se distinguen dos clases de procedimientos: obligatorios y recomendados. Estos últimos representan "buenas prácticas", que son aconsejables, pero no requeridas.
Recursos tecnológicos	Son todos los elementos que utilizan la tecnología para llevar a cabo un propósito, archivos digitales, sistemas de información, servicios, bases de datos y equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros)

Requisito	Necesidad establecida, generalmente explicita u obligatoria.
Riesgo	Posibilidad de que una amenaza se produzca, dando lugar a una afectación. Probabilidad de que ocurra el ataque por parte de la amenaza.
Seguridad de la información	Conjunto de medidas técnicas operativas, organizativas, administrativas y legales que permite a la organización resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de esta.
SGSI	Sistema de gestión de la seguridad de la información. [ISO/IEC 27001: 20005] Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de una compañía, con el fin de establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad.
Titular	Persona natural cuyos datos personales sean objeto de tratamiento de datos.
Transferencia de información	Se da cuando el responsable directo del tratamiento de datos personales envía o entrega la información o los datos personales a otra persona o entidad pública o privada que a su vez es responsable del tratamiento de los datos.
Tratamiento	Conjunto de operaciones sobre datos personales tales como la recolección, almacenamiento, uso, circulación o supresión.
Vulnerabilidad	ISO/IEC 13335-1:2004. Debilidad de un activo o grupo de activos que afecta las propiedades de confidencialidad, integridad y disponibilidad de los datos.