1. INTRODUCCIÓN

Para GML SOFTWARE S.A.S., es fundamental proteger la información procesada en la compañía, gestionar los riesgos y aplicar medidas de controles en seguridad que permitan minimizar la materialización de estos frente a las amenazas internas o externas, deliberadas o accidentales, a las que está expuesta la información, asimismo proteger, conservar y asegurar la información para mantener un nivel mínimo de exposición que permitan preservar la integridad, confidencialidad y disponibilidad de esta.

En GML SOFTWARE S.A.S protegemos, custodiamos y preservamos la información relacionada con los procesos de desarrollo de software resultado del uso de metodologías ágiles, así como aquella información relacionada con actividades de consultoría y servicios de staff augmentation para administración de aplicaciones como eje fundamental del negocio y las necesidades de nuestros clientes.

Como recurso vital, la información en nuestra compañía es gestionada por procesos, mediante una adecuada gestión de riesgos de seguridad y privacidad de la información que permiten el adecuado acceso, procesamiento, transferencia, , almacenamiento, presentación, comunicación y divulgación de los activos de información, gestionando su seguridad para dar cumplimiento a los requisitos contractuales, legales, técnicos y reglamentarios que apliquen, así como a las necesidades de las partes interesadas de la compañía.

GML SOFTWARE S.A.S. dispone de tecnologías para el procesamiento, transferencia y almacenamiento de la información, de talento humano que hacen uso de esta, de sitios físicos donde se resguarda información, de transferencia de información entre colaboradores, clientes y partes externas.

Para GML SOFTWARE S.A.S. es importante garantizar el uso eficaz, seguro y racional de la información, por lo que regula su tratamiento atendiendo las disposiciones legales y reglamentarias previstas para el efecto, en especial las contenidas en la norma ISO/IEC 27000 *"Estándar de seguridad de la información; provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información"*, y la norma ISO/IEC 31000 que *"Brinda principios y directrices para la gestión del riesgo"*.

GML SOFTWARE S.A.S., entendiendo el compromiso de preservar la seguridad de la información en el desarrollo de las actividades operativas de la compañía, considera la importancia de reglamentar las principales políticas y directrices en relación con aspectos generales de la gestión y administración de la seguridad de la información mediante la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI, buscando establecer su apropiación, cumplimiento y concienciación.

Al igual que la dinámica evolutiva y cambios organizacionales de GML SOFTWARE S.A.S., la Industria, legislación y normativas vigentes, es pertinente, revisar, actualizar y reglamentar periódicamente las principales políticas y directrices en relación con aspectos generales de la gestión y administración de la seguridad de la información, así como el SGSI de la compañía.

La presente política de seguridad de la información está orientada por los principios, la misión y visión de GML SOFTWARE S.A.S., siendo su objetivo definir los lineamientos y controles que deben ser adoptados e implementados para garantizar que los riesgos de la seguridad de la información sean conocidos, tratados, gestionados y asumidos de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los, procesos, el entorno y las tecnologías de información de GML SOFTWARE S.A.S.

Se trata de una política preventiva y estratégica que permita adelantarse a cualquier situación, evento o incidente que atente contra la integridad, confidencialidad y disponibilidad de la información, en sus diferentes áreas y procesos y en general en la compañía.

Para GML SOFTWARE S.A.S. la promulgación de la presente política de seguridad de la información, se define como un proceso que le permite a percibir un estado de confianza para el desarrollo de las actividades dentro de las áreas y su entorno, mediante la materialización de las estrategias definidas en planes de acción y la adopción de una serie de controles y disposiciones para

reconocer la existencia de riesgos, identificarlos, establecer el plan de tratamiento y determinar el nivel de aceptación que está dispuesto asumir GML SOFTWARE S.A.S.

En virtud de lo anterior se actualiza, se define y se dispone la presente política de seguridad de la información en GML SOFTWARE S.A.S.

2. TÉRMINOS Y DEFINICIONES

Para efectos de dar cumplimiento al presente acuerdo, se tomarán las definiciones estipuladas en los glosarios de las normas ISO 27001 – 22301 – 31000 – 20000, así como también los siguientes términos:

a. **Activo de Información**: Es todo aquello que GML SOFTWARE S.A.S. considera importante o de alta validez en cuanto a la información o elemento relacionado con el tratamiento de esta, personas, infraestructura, sistemas de información, herramientas informáticas, bases de datos, archivos, entre otros.

b. **Análisis de Riesgo:** Uso sistemático de la información para identificar fuentes y tratamiento del riesgo.

c. **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

d. **Dato sensible**: Información que afecta la intimidad de la persona o cuyo uso indebido puede generar su discriminación; tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huellas dactilares, entre otros).

e. **Disponibilidad**: Característica, cualidad o condición de la información que permite encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, garantizando el acceso a la misma y a los sistemas por personas autorizadas en el momento que se defina o así lo requieran.

f. **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

g. **Integridad:** Propiedad que busca mantener los datos libres de modificaciones no autorizadas para mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

h. **Manual de Seguridad de la Información**: Es el documento rector que materializa las políticas de seguridad de la información, estas se encuentran enfocadas al cumplimiento de la normatividad legal vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001.

i. **Plataforma Tecnológica:** Sistema base de integración de infraestructura de tecnología de la información, sistemas de información, sistemas de comunicaciones unificadas, sistemas de telecomunicaciones, redes de datos y herramientas informáticas definidas por GML SOFTWARE S.A.S. para la prestación de servicios tecnológicos.

j. **Riesgo**: Un posible evento que podría causar daño o pérdidas, o afectar la habilidad de alcanzar objetivos, asociado al impacto y probabilidad de ocurrencia.

k. **Servicio Tecnológico**: Es un medio para entregar valor a los usuarios y partes interesadas basándose en el uso de las tecnologías de la información para soportar los procesos de la Compañía.

l. **Sistema de Información**: Conjunto de componentes de hardware y software interrelacionados que permiten registrar, procesar, almacenar, distribuir y consultar información, para apoyar al ambiente productivo y la toma de decisiones estratégicas de GML SOFTWARE S.A.S.

m. **Tratamiento del Riesgo:** Proceso de selección e implementación de acciones de mejorar que permitan mitigar el riesgo.

n. **Usuario**: Persona vinculada a la GML SOFTWARE S.A.S. independiente de su tipo de relación o contrato, a la cual se le concede el acceso para el uso de la plataforma tecnológica de GML SOFTWARE S.A.S.

o. **Partes interesadas**: Persona, grupo, entidad, institución u organización de interés que se relacionan con GML SOFTWARE S.A.S. que se ve afectado por las acciones y decisiones de esta y tiene expectativas sobre cuál debería ser su comportamiento, se trata de todas las partes que pueden afectar a la compañía o verse afectadas por la consecución de las actividades o el negocio de GML SOFTWARE S.A.S.

3. ALCANCE

Esta política tiene alcance y aplicabilidad a los criterios, requisitos y necesidades relacionadas con las partes interesadas definidas en la compañía GML SOFTWARE S.A.S. como empleados, proveedores, clientes, y terceros entre otros y en general a toda persona, organización u compañía cualquiera que sea su vínculo con la organización.

Estas disposiciones también involucran a grupos de interés, partes interesadas, contratistas, consultores y demás colaboradores, que procesan y tratan información de la compañía, incluidas las operaciones de recopilación, análisis, procesamiento, disponibilidad, custodia, conservación y recuperación, al igual los que laboran en las instalaciones de GML SOFTWARE S.A.S, de modalidad teletrabajo autónomo o presencial en sus diferentes modalidades que utilicen tecnologías de información y de comunicaciones propiedad de la compañía. Asimismo, estas disposiciones aplican para todos los equipos tecnológicos propios o arrendados que tiene GML SOFTWARE S.A.S.

4. OBJETIVOS DEL SGSI

GML SOFTWARE S.A.S, como parte de su dirección estratégica, establece en concordancia con sus objetivos estratégicos y su política de seguridad de la información, los siguientes los objetivos de seguridad de la información,

Se establecen los siguientes objetivos rectores que permiten contribuir a cumplir y desarrollar los objetivos de la política de seguridad de la información de GML SOFTWARE S.A.S.

a. Implementar, certificar y mantener un Sistema de Gestión de Seguridad de la Información – SGSI, adoptando el estándar internacional de la norma ISO/IEC 27001.
b. Fomentar para las partes interesadas, usuarios y colaboradores un plan de cultura y concienciación de seguridad de la información en GML SOFTWARE S.A.S. para asegurar su apropiación y cumplimiento del SGSI.
b. Adoptar y gestionar un manual de seguridad de la información el cual incorpore buenas prácticas y normas al cumplimiento de lineamientos y controles definidos para la seguridad de la información.
c. Adoptar y gestionar un manual de control de acceso el cual incorpore buenas prácticas y normas al cumplimiento de lineamientos y controles definidos para la seguridad de la información.
c. Adoptar un plan de gestión de los riesgos de la seguridad de la información que permita identificarlos, evaluarlos, valorarlos y tratarlos de manera que se minimice su impacto en la operación de los procesos de la compañía.
d. Asegurar que la estrategia de recuperación y restauración de los servicios tecnológicos y sistemas de información críticos esté alineada a la estrategia de continuidad de la operación de GML SOFTWARE S.A.S.
e. Asegurar que en los procesos de la compañía se integren los requisitos y controles de seguridad definidos por la norma ISO 27001.
f. Cumplir con los requisitos contractuales, legales y reglamentarios relacionados con la seguridad de la información que apliquen al negocio.

5. NORMATIVA Y REFERENTES

En el desarrollo, interpretación y aplicación de la presente política, se tomarán los siguientes referentes entre otros como base fundamental para la aplicación de esta.

5.1. Normatividad externa

a. Ley 527 de 1999 sobre la firma electrónica.
b. Ley 1273 de 2008 Delitos informáticos y protección el bien jurídico o tutelado que es la información.
c. Ley 1266 de 2008 Habeas data financiera y seguridad en datos personales.
d. Ley 1341 de 2009 Tecnologías de la Información y aplicación de seguridad.
e. Ley 1581 de 2012 Protección de datos personales.
f. Decreto 2364 de 2012 Firma electrónica.
g. Decreto 1377 de 2013 Se reglamenta parcialmente la Ley 1581 de 2012.
h. Decreto 1151 de 2008 Gobierno en línea.
i. Decreto Único Reglamentario 1074 de 2015 del Ministerio de Industria y Comercio

5.2. Marcos de referencia

a. Norma ISO/IEC 27001 “Estándar de seguridad de la información; provee estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información”.
b. Norma ISO/IEC 27002 “Guía de buenas prácticas en controles de seguridad de la información”.
c. Norma ISO/IEC 27005 “Directrices para la gestión del riesgo en seguridad de la información”
d. Norma ISO/IEC 22301 “Fundamentos de un sistema de gestión de continuidad de negocio
e. Norma ISO/IEC 31000 “Brinda principios y directrices para la gestión del riesgo”.
f. Norma ISO/IEC 38501 “Marcos de trabajo para el gobierno y la gestión de tecnología de la información”.

5.3. Roles, responsabilidades y autoridades en la seguridad de la información

La Seguridad es promovida, con la participación de los colaboradores, así como de las personas o entidades externas que tengan un vínculo con la compañía.

A continuación, se relacionan las autoridades y responsabilidades que gestionan, apoyan y velan por el cumplimiento de la normatividad, los controles y las buenas prácticas en Seguridad de la Información en la compañía

5.3.1. Gerencia general y alta dirección

Su responsabilidad se enfoca en ejercer el liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información – SGSI.

a. Asegurar que los objetivos y la Política de Seguridad de la Información se alineen con la dirección estratégica de la compañía.
b. Asegurar la disponibilidad de los recursos necesarios para el desarrollo y cumplimiento de los requisitos establecidos en el SGSI.
c. Promover el seguimiento, revisión y la mejora continua del SGSI.

5.3.2. Comité de seguridad de la información y protección de datos personales.

Es el órgano consultivo para la administración y el direccionamiento estratégico, conformado por representantes de los procesos de la compañía relacionadas con la gestión integral de la seguridad de la información; su rol es velar por el desarrollo y la implementación de las políticas de gestión, directrices y demás lineamientos en seguridad de la información que se acuerden con la gerencia general, entre sus funciones principales se encuentran:

a. Asesorar a la gerencia y alta dirección en el direccionamiento de la seguridad de la información y protección de datos personales de GML SOFTWARE S.A.S.
b. Fortalecer la seguridad de la información y datos personales de la compañía mediante la incorporación de buenas prácticas acordes con la operación y la misión.
c. Definir, aprobar y promover la implementación, desarrollo y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información - SGSI.
d. Promover la cultura de la seguridad de la información y datos personales a todas las partes interesadas.
e. Evaluar y analizar los informes periódicos sobre el estado de la seguridad de la información.
f. Definir los planes de acción para mitigar y/o eliminar los riesgos asociados a la información.
g. Evaluar, definir y promover propuestas de implementación de seguridad de la información.
h. Gestionar y tratar los incidentes críticos de seguridad de la información y datos personales.
i. Aprobar el manual de seguridad de la información y el de accesos, asimismo, gestionar las actualizaciones a que surjan como mejoramiento al SGSI.

5.3.3. Oficial de seguridad de la información

Es el rol responsable de planificar, desarrollar y gestionar la seguridad de la información en la compañía, desempeñando las siguientes responsabilidades:

a. Establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información de la compañía.
b. En coordinación con el líder de Talento Humano, la promoción de la cultura de seguridad de la información entre todos los colaboradores de la compañía.
c. En coordinación con el líder de Infraestructura y soporte técnico, gestionar los activos de información y controles de seguridad técnicos.
d. En coordinación con los lideres de área gestionar los riesgos relacionados con la seguridad en los activos críticos de información asociado al proceso de desarrollo de software de la compañía.
e. Gestionar el desarrollo e implementación de políticas y/o procedimientos de seguridad de la información en la compañía.
f. Hacer seguimiento y/o gestionar la respuesta a incidentes de seguridad de la información, así como la investigación de las violaciones de la seguridad.
g. Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de las políticas y procedimientos en materia de Seguridad de la Información.
h. Estimar y obtener aprobación del presupuesto anual de mantenimiento del SGSI.
i. En coordinación con el líder de infraestructura y soporte técnico gestionar el Plan de Recuperación de Desastres - DRP relacionado con el Plan de la Continuidad del Negocio – BCP, de la compañía.
j. Reportar a la gerencia oportunamente el estado, mantenimiento y cumplimiento del SGSI y la gestión de riesgos asociada a seguridad de la información.
k. Ser el punto de contacto con las autoridades competentes en materia de seguridad de la información y gestionar con el responsable y encargado de la protección de datos personales.

5.3.4. Líder de talento humano

Es el rol responsable de garantizar que se cumpla los requisitos de seguridad de la información relacionados con las personas que interactúan con la compañía, cumple, entre otras, con las siguientes funciones principales:

a. Asegurar que los empleados y contratistas, comprendan la responsabilidad y que son para el rol que desempeñan, antes, durante y después de la terminación del contrato.
b. Asegurar que los empleados y contratistas reciban capacitación y tomen conciencia de sus responsabilidades de la información al igual que las cumplan.
c. Ejecutar, validar y asegurar que se desarrolle el plan de cultura y sensibilización de seguridad de la información.
d. Definir y velar por el cumplimiento de los procesos disciplinarios en lo referente a violaciones de la seguridad de la información.

5.3.5. Líder de infraestructura y soporte técnico

Es el rol responsable de garantizar el cumplimiento en la aplicación de los controles de seguridad digital definidos para la planeación, implementación y operación de los servidores físicos y virtuales, el almacenamiento, las redes y telecomunicaciones y los demás dispositivos que conforman la plataforma tecnológica de GML SOFTWARE S.A.S. cumple, entre otras, con las siguientes funciones principales:

a. Planificar, dirigir y gestionar los Sistemas de Información, en cuanto accesos, soporte, ofreciendo mecanismos de entrega de información oportuna, confiable y veraz a las partes interesadas.
b. Validar que las soluciones tecnológicas, sistemas de información, Bases de datos y aplicativos cumplan con los controles de acceso y tratamiento en seguridad de la información y protección de datos personales.
c. Validar los lineamientos para definir los requerimientos y los mecanismos de control de acceso a la información según de nivel de clasificación.
d. Validar y actualizar la matriz de seguridad de los sistemas de información, en lineamiento con la gestión de accesos e identidades.
e. Validar el cumplimiento de los controles y herramientas tecnológicas de seguridad, verificar su implementación y coordinar la realización de pruebas de aseguramiento de estos.
f. Gestionar y asegurar la cadena de custodia de las pruebas forenses informáticas.
g. En coordinación con el Oficial de Seguridad de la Información, definir y validar el Plan de Recuperación de Desastres para la Continuidad del Negocio de la compañía.
h. Validar y actualizar la matriz de seguridad de los aplicativos y sistemas de información, en lineamiento con la gestión de accesos e identidades.

5.3.6. Líder de tecnología e Innovación

Es el rol responsable de garantizar la entrega de soluciones y servicios tecnológicos, así mismo que estén enmarcados en la eficiencia y eficacia, a través de tecnologías flexibles y adaptables acorde al entorno, grado de desarrollo y el dinamismo de compañía. Cumple, entre otras, con las siguientes funciones principales:

a. Asegurar que los requisitos de seguridad se incorporen y cumplan en el ciclo de vida de desarrollo de software.
b. Asegurar que los ambientes de desarrollo, pruebas y producción estén siempre en ambientes separados.
c. Aplicar buenas prácticas y marcos de referencia de seguridad en el desarrollo de software y soluciones tecnológicas.
d. Asegurar que la información se anonimice y enmascare en ambientes de pruebas y desarrollo.

5.3.7. Asesor y consultor jurídico

Es el rol responsable de garantizar y asesorar a la Gerencia General el cumplimiento de la leyes, normatividad y lineamientos en lo que respecta cumplimiento normativo y legal en la seguridad de la información y la protección de datos personales que se emitan en GML SOFTWARE S.A.S.

5.3.8. Líderes de procesos o áreas

Es el rol responsable del cumplimiento de las mejoras prácticas y controles definidos en esta Política y Manual de seguridad de la Información, tienen entre otras las siguientes responsabilidades:

a. Apoyar y promover continuamente la apropiación y concienciación de la cultura de la seguridad de la Información en sus áreas y procesos.
b. Dar cumplimiento al SGSI de la compañía.
c. Gestionar los riesgos de su área o procesos relacionados con la seguridad de la Información.
d. Gestionar los activos de información relacionados con su área o procesos.
e. Asegurar que el componente de Seguridad de la información donde se requiera este incorporado en su proceso y procedimientos.
f. Gestión, seguimiento y control de los riesgos del proceso o área.
g. Identificación, análisis y control de acciones correctivas o de mejora que sean registradas a partir de seguimientos, auditorías de cualquier tipo o establecidas internamente, incluyendo su análisis de causas y planes de acción.
h. Ejecución de las actividades asignadas en cumplimiento de la planeación estratégica.
i. Medición, análisis y control de indicadores de gestión, incluyendo la definición de nuevas métricas de acuerdo con las metas que defina en el proceso que lidero.
j. Notificar al Oficial de Seguridad de la Información de cambios u oportunidades del proceso que lidera a partir de modificaciones en estructura, metodologías, herramientas usadas para la gestión de este.
k. Evaluación de controles de seguridad existentes y definición de nuevos.
l. Gestión en tratamiento de Incidentes de seguridad y eventos siempre que el proceso esté involucrado.
m. Revisión y control de los documentos controlados por Sistema de Gestión de Seguridad de la Información - SGSI para el proceso (procedimientos, manuales, formatos, instructivos, guías, matrices entre otros)
n. Participación en las auditorías internas y externas (clientes o ente certificador) siempre que sea convocado dentro del Plan de Auditoría.
o. Participar en toma de decisiones para mejora a partir de retroalimentación de partes interesadas (obtenida de: seguimientos, análisis de contexto, estrategias)

5.3.9. Colaboradores

Este rol tiene el deber y el derecho de conocer las responsabilidades que le asisten y adquieren, así mismo apropiar y dar cumplimiento a la normatividad que en Seguridad de la Información y Privacidad de los datos personales que defina y establezca GML SOFTWARE S.A.S entre otras: Política de Seguridad da la Información, Política de tratamiento de la Información, Manual de Seguridad de la Información, Manual de accesos y los controles de seguridad definidos por la compañía, tienen entre otras las siguientes responsabilidades:.

a. Mantener absoluta reserva sobre los documentos y hechos conocidos en el desempeño de sus funciones.
b. Ser responsable del control y seguridad de la información que tiene a su cargo.
c. Ser consciente de la influencia que su acción o inacción pueda tener sobre la efectividad de la seguridad de la información en los procesos en la compañía.
d. Reportar de manera oportuna todo acto sospechoso o incidente de seguridad que pudiera ocurrir durante la ejecución de sus funciones.

e. Conocer los procesos a las cuales se deben reportar situaciones sospechosas o riesgos asociados con la información con la que interactúe
f. Proteger la información física o digital de la cual es responsable para el desempeño de sus funciones.
g. Conocer los procedimientos y políticas de seguridad de la información y velar por que se mantengan y cumplan.
h. Cumplir con todas las políticas establecidas por la compañía para el manejo de la información en desarrollo de sus funciones.
i. Asistir a las capacitaciones programadas que en temas de seguridad se convoquen en la compañía.
j. Conocer los activos de información que maneja durante el desarrollo de sus funciones.
k. Conocer y tratar la información de acuerdo con los criterios de acceso o clasificación definidos para la misma no alterando el alcance de su divulgación.
l. Hacer cumplir las normas de seguridad definidas para clientes o proveedores y terceros que se encuentren en las instalaciones.

5.3.10. Contratistas, terceros y demás partes interesadas.

Este rol se relaciona con cualquier persona o entidad independiente de su vínculo comercial o contractual adquirido, que hagan uso o tratamiento de la información de GML SOFTWARE S.A.S, al cual deben ser informados o comunicados de los deberes, responsabilidades que le asisten, en el cumplimiento de la Política de Seguridad da la Información, la Política de tratamiento de la Información y del Manual de Seguridad de la Información, además de los controles de seguridad definidos por la compañía.

6. DISPOSICIONES EN POLÍTICAS Y LINEAMIENTOS EN CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Se establecen entre otros los siguientes lineamientos que los procesos y áreas deben implementar y gestionar en GML SOFTWARE S.A.S, así mismo los controles y lineamientos que requieran ser abordados para cubrir áreas en seguridad más específicos se deben profundizar más en el ***"Manual de Seguridad de la información"*** y en las políticas, procedimientos, guías o instructivos en seguridad de la información que requiera definir en cada proceso o área acorde a las necesidades del negocio.

Para el desarrollo y cumplimiento de la presente política GML SOFTWARE S.A.S., adoptan 4 dominios: *1. Organizacional, 2. Personal, 3. Físicos y 4. Tecnológicos*, para el desarrollo y cumplimiento de los objetivos establecidos, los cuales se describen a continuación:

6.1. Políticas y lineamientos en el ámbito de controles organizacionales

6.1.1. Inteligencia de amenazas

La Información relacionada con las amenazas cibernéticas que pueda impactar la seguridad de la información en la compañía se debe recopilar, evaluarse, difundirse, así mismo se debe generar un plan de mitigación de estas.

6.1.2. Gestión de los activos de información

Aplicar los mecanismos, los procedimientos y los controles que permitan la gestión del inventario, la clasificación, la responsabilidad, la propiedad y la custodia de los activos de información de la compañía, así mismo se deben gestionar el inventario de los activos de información desde los procesos y áreas de la compañía

6.1.3. Clasificación de la información

Se debe Clasificar y etiquetar los activos de información en términos de la valoración, el nivel de criticidad, la confidencialidad y los requisitos legales, acordes a las necesidades de seguridad de la información considerando la confidencialidad, la integridad, la disponibilidad acorde con los requisitos pertinentes de las partes interesadas y procesos, entre otros.

6.1.4. Transferencia de la información

a. Se deben definir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la compañía y entre la compañía y otras partes externas.
b. Se deben diseñar controles para proteger la información transferida de la intercepción, el acceso no autorizado, la copia, la modificación, el enrutamiento incorrecto, la destrucción y la denegación de servicios, entre otros.

6.1.5. Control de accesos

a. Se deben asegurar los mecanismos y los controles para la gestión de acceso adecuado a las plataformas tecnológicas mediante la implementación de procesos que incluyan el ciclo de vida del control de acceso para los usuarios, desde la vinculación, hasta el retiro de la compañía de acuerdo con el "**Manual de Control de Acceso**".
b. Se deben definir y actualizar las matrices de roles y perfiles para el acceso a la plataforma tecnológica de acuerdo con las necesidades de GML SOFTWARE S.A.S.
c. Las credenciales (claves de acceso), códigos de acceso, tarjetas inteligentes, dispositivos de autenticación, llaves para protección de software, combinaciones de cajas fuertes o cualquier otro activo de información, son personales e intransferibles; su uso, administración y reserva es responsabilidad de cada usuario.

6.1.6. Relaciones con los proveedores y contratistas

a. Se deben establecer y acordar cláusulas contractuales en seguridad de la información, confidencialidad y protección de datos personales con los proveedores y contratistas que acceden a las plataformas tecnológicas de la compañía.
b. Se debe evaluar el cumplimiento de la seguridad de la información de los servicios de tecnología contratados con los proveedores.

6.1.7. Gestión de incidentes de la seguridad de la información

a. Definir y establecer el procedimiento para el análisis, evaluación, relación de evidencias, tratamiento y reporte de los incidentes relacionados con la seguridad y privacidad de la información, datos personales y ciberseguridad con el fin de mitigar el riesgo asociado a la pérdida de la confidencialidad, integridad y disponibilidad de la información de GML SOFTWARE S.A.S.
b. Reportar los eventos e incidentes de seguridad de la información, protección de datos y ciberseguridad que comprometan la continuidad de la operación por amenazas, como: uso, divulgación, modificación o destrucción no autorizada de información y datos personales; un impedimento en la operación normal de las redes, sistemas de información o recursos informáticos; o una violación a la presente Política de Seguridad de la Información, la Política de Tratamiento de la Información y las disposiciones del Manual de Seguridad de la Información.

6.1.8. Preparación de las TI para la continuidad del negocio

Se debe garantizar la gestión de la continuidad de los servicios tecnológicos a través de un plan de recuperación ante desastres, que permita asegurar que las plataformas tecnológicas críticas estén disponibles para el Sistema GML SOFTWARE S.A.S. en caso de presentarse una interrupción en la operación, asimismo se deben implementar controles y herramientas necesarias para asegurar que los recursos que componen las plataformas tecnológicas sean periódicamente respaldados, monitoreados y proyectados para futuros requerimientos de capacidad en procesamiento, almacenamiento y concurrencia.

6.1.9. Privacidad y protección de datos personales

a. GML SOFTWARE S.A.S. está comprometida con el respeto y cumplimiento del derecho de Habeas data, en cabeza de sus colaboradores y cualquier persona en general. En virtud de lo anterior, adoptó la Política de Tratamiento de Información, la cual es de obligatoria aplicación en todas las actividades y procedimientos que involucre el tratamiento de datos personales. Esta política es de estricto cumplimiento por parte de todos los colaboradores, contratistas y terceros que tengan vínculo con GML SOFTWARE S.A.S.
b. El incumplimiento de la Política de Tratamiento de Información acarreará las investigaciones disciplinarias correspondientes de conformidad con lo establecido en la normativa interna y el ordenamiento jurídico aplicable.

6.1.10. Cumplimiento de requisitos legales y contractuales

Gestionar los procesos y controles para dar cumplimiento a normatividad tanto externa como interna de la compañía, así como también lo establecido en acuerdos contractuales, en lo relacionado con aspectos de seguridad de la información, ciberseguridad y protección de datos personales.

6.1.11. Revisiones independientes de la seguridad de la información

a. Auditar a intervalos planificados o cuando ocurran cambios significativos tanto de regulación normativa de ley, procedimientos o procesos referentes en seguridad de la información y el cumplimiento a la protección de datos personales.

b. Realizar periódicamente auditoría de seguimiento a la plataforma tecnológicas para determinar el cumplimiento de las políticas y normatividad en seguridad de la información y protección de datos personales.

6.2. Políticas y lineamientos en el ámbito de controles de personales

a. El área de Talento Humano debe propender y asegurar que los colaboradores, contratistas, terceros demás partes interesadas, comprendan sus derechos y responsabilidades frente al cumplimiento de la Política de Seguridad de la Información.
b. El área de Talento Humano debe definir un Plan de Socialización de la Seguridad de la Información.
c. Se deben asegurar los acuerdos contractuales con empleados y contratistas sus responsabilidades y las de GML SOFTWARE S.A.S., en cuanto a la seguridad de la información.
d. Los contratos deben contener cláusulas de confidencialidad y no divulgación de la información, así como la obligatoriedad del cumplimiento de las políticas, procedimientos, restricciones y controles de seguridad de la información, aún después de terminada la relación contractual.
e. Se deben comunicar al área de infraestructura y soporte, la desvinculación del colaborador o contratista y/o el cambio de rol dentro de GML SOFTWARE S.A.S., con el fin que realicen los ajustes de acceso a los servicios tecnológicos.

6.3. Políticas y lineamientos en el ámbito de controles físicos

6.3.1. Protección contra amenazas físicas y ambientales

a. Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
b. Aplicar los controles y las restricciones de acceso físico pertinentes, con el fin de evitar los accesos no autorizados y mantener la seguridad sobre las instalaciones, los activos de información y las personas.
c. Aplicar los mecanismos y controles de acceso físico para evitar el daño, la pérdida o el robo de los activos de información y tecnológicos de la compañía.

d. Implementar las medidas para el control del ingreso y el retiro los activos de información de las instalaciones de la compañía.
e. Implementar mecanismos de control de acceso para las áreas seguras; tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, de acuerdo con los procedimientos establecidos por GML SOFTWARE S.A.S.

6.4. Políticas y lineamientos en el ámbito de controles tecnológicos

6.4.1. Configuración y manejo de los dispositivos de punto final de usuario

a. Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos finales de los usuarios.
b. Se debe controlar la restricción de la instalación de software, la cual debe ser exclusivamente por los administradores del sistema.
c. Se debe controlar el tipo de información y nivel de clasificación que los dispositivos de punto final del usuario pueden manejar, procesar, almacenar y admitir.

6.4.2. Gestión de vulnerabilidades técnicas

a. Debe obtenerse información sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluar la exposición de la compañía a tales vulnerabilidades y tomarse las medidas apropiadas.
b. Definir los protocolos, las herramientas emergentes y los servicios necesarios para identificar las vulnerabilidades técnicas de las plataformas tecnológicas.
c. Programar y ejecutar escaneos de vulnerabilidades a los servicios tecnológicos por lo menos una vez al año, para servicios actuales o nuevos y cuando se ejecuten controles de cambio de los sistemas de información, a las aplicaciones e infraestructura tecnológica, con el fin de evaluar y gestionar las brechas de seguridad y proceder a la remediación.
d. Cuando se ejecuten pruebas controladas de intrusión, éstas se deben realizan por un proveedor certificado, quien genera el reporte y plan de remediación.
e. Se deben realizar pruebas anuales de Ética Hacking a la plataforma tecnológica según el nivel de criticidad y de acuerdo con la clasificación de sistemas de información, aplicaciones e infraestructura tecnológica relacionadas con el negocio.
f. Se debe realizar el seguimiento, verificación y remediación de las vulnerabilidades identificadas.

6.4.3. Copias de seguridad de la información

a. Los sistemas de información, aplicaciones e infraestructura tecnológica se deben respaldar periódicamente y almacenar en una zona geográfica diferente de donde se aloja la información original con el fin de asegurar la integridad y disponibilidad de esta.
b. Las copias de seguridad se deben probar periódicamente para asegurar la disponibilidad e integridad de los datos que se encuentran almacenados y que permitan ser restaurados en caso de requerirse.
c. En los espacios donde se almacenan localmente las copias de respaldo y en los sitios de custodia externa, se deben establecer mecanismos de protección ambiental como detección de humo, fuego, humedad, así como control de acceso físico.
d. Se debe identificar el nivel de criticidad de la información a respaldar, así como la frecuencia, los requisitos de seguridad de la información y la importancia en la operación en la compañía.
e. Las copias de seguridad deben tener el mismo tratamiento y manejo conforme el nivel de clasificación de los sistemas de información, aplicaciones e infraestructura tecnológica.
f. Es responsabilidad de cada colaborador respaldar la información en las estaciones de trabajo y hacer uso de la plataforma de colaboración y productividad como medio principal de almacenamiento de la información para el cumplimiento de sus funciones.

g. Al término del contrato o retiro voluntario del colaborador, el jefe inmediato se asegura que la información de GML SOFTWARE S.A.S. sea respaldada a través de la plataforma de colaboración y productividad.
h. Se debe mantener organizada y depurada la información de las carpetas compartidas, como buena práctica para la optimización de recursos de la compañía.

6.4.4. Seguridad de redes

a. La autenticación al servicio de red inalámbrica debe ser gestionada por el sistema de control de acceso a la red dispuesto por GML SOFTWARE S.A.S.
b. Se debe gestionar y controlar la navegación para el servicio de internet.
c. Se debe gestionar y controlar el servicio de DNS y DHCP.
d. Las conexiones desde redes externas hacia servidores o equipos de la red interna son controladas por la plataforma de seguridad perimetral, la cual asegura la confidencialidad, la integridad y la disponibilidad de la información.
e. El direccionamiento de la red interna no debe ser accesible desde redes o equipos externos.
f. El dispositivo de seguridad perimetral de GML SOFTWARE S.A.S. conectado a Internet debe contener una política o regla de seguridad.
g. La administración del firewall por la interfaz de red pública debe permanecer deshabilitada.
h. Realizar monitoreo continuo de los registros de eventos (logs) en el dispositivo de seguridad perimetral, con el fin de identificar posibles novedades de seguridad y aplicar las acciones correspondientes.
i. Todos los cambios de configuración en el dispositivo de seguridad perimetral tienen un registro (log) en el sistema.

6.4.5. Uso de criptografía

a. Se debe garantizar métodos de cifrado para la autenticación de usuarios en los sistemas de información, aplicaciones e infraestructura tecnológica.
b. Se deben proteger las plataformas de autenticación que contengan las contraseñas de acceso con sus respectivos métodos de cifrado, asegurando la no copia o modificación de estas, sin autorización.
c. Se deben evaluar nuevas tecnologías y acoger las mejores prácticas de la industria en productos y servicios relacionados con el cifrado de la información.
d. Se deben asegurar que las copias de seguridad donde repose la información catalogada como confidencial este protegido a través de métodos de cifrado.
e. Se deben aplicar métodos de cifrado y medios de transmisión seguros para información catalogada como confidencial.
f. Se deben administrar y gestionar los certificados digitales, asegurando la generación, almacenamiento, archivo, recuperación, distribución, retirada y destrucción de llaves criptográficas.
g. Se deben Garantizar el cifrado de documentos para:

- Cuando se requiere transmitir información confidencial o sensible de GML SOFTWARE S.A.S. hacia entidades o personas externas.
- Cuando el Líder de Proceso o el responsable de Seguridad de la Información consideren un activo de información crítico para la compañía.

6.4.6. Ciclo de vida de desarrollo seguro

a. Definir los procedimientos y los mecanismos que permitan asegurar la inclusión de requisitos y controles de seguridad digital, durante el ciclo de vida (adquisición, desarrollo, mantenimiento y retiro) de los sistemas de información, aplicaciones e infraestructura tecnológicas.

b. Se deben incorporar tecnologías emergentes que faciliten el fortalecimiento de los recursos y los niveles adecuados de separación lógica y física entre los ambientes de desarrollo, pruebas y producción para la plataforma tecnológica y sistemas de información con el fin de evitar cambios que puedan afectar la operación.
c. Se deben Utilizar diferentes perfiles de usuario para los ambientes de desarrollo, pruebas y producción.
d. Cada ambiente debe tener una única matriz de roles y perfiles.
e. Se deben evitar ejecutar pruebas, instalaciones o desarrollos de software en los entornos de producción.
f. Establecer el instructivo de instalación de software que brinde una guía sobre la instalación y requisitos de cada ambiente.
g. Los ambientes de desarrollo se deben ejecutar de acuerdo con las necesidades funcionales para la implementación final del sistema de información o aplicaciones.
h. En los ambientes de pruebas, se realiza las pruebas unitarias del funcionamiento del sistema de información o aplicaciones.

7. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

a. Se debe auditar a intervalos planificados o cuando ocurran cambios significativos tanto de regulación normativa de ley, procedimientos o procesos referentes en seguridad de la información y el cumplimiento a la protección de datos personales.
a. Se debe realizar periódicamente al menos una vez al año una auditoría de seguimiento a la plataforma tecnológicas para determinar el cumplimiento de las políticas y normatividad en seguridad de la información y protección de datos personales.
b. La presente política debe ser evaluada y actualizada periódicamente, mínimo una vez año, acorde a las necesidades y dinámica del negocio y normativa vigente.

8. DIVULGACIÓN, CULTURA, REVISIÓN Y ADOPCIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

c. Se deben definir los procedimientos, los controles y los mecanismos necesarios, para garantizar que en la compañía y las partes interesadas conozcan y den cumplimiento a la presente política, así como de los documentos que la integran.
d. Se deben articular las estrategias encaminadas a desarrollar competencias digitales en aspectos de seguridad que integre las áreas de la compañía.
e. Se debe implementar y mantener, como parte del desarrollo del modelo de gestión de seguridad de la información y protección de datos personales, el programa, los planes de cultura y adopción y socialización en la compañía, de manera que se minimice la probabilidad y el impacto de incidentes de seguridad de la información y protección de datos personales.

9. DEBERES Y SANCIONES

a. Cualquier persona que tenga vínculo con GML SOFTWARE S.A.S., estará obligado a conocer y cumplir la presente política y demás disposiciones que la desarrollen y que se encuentren publicados en el portal web oficial de la compañía.
b. Cuando se identifique el incumplimiento de la presente política por parte de un colaborador, se pondrá en conocimiento al área de Talento Humano para los efectos de su competencia y atribuciones,
c. Así mismo para los contratistas, terceros o partes interesadas se dará trámite al área jurídica para su concepto desde el ámbito legal.

APROBACIÓN

ELABORACIÓN	REVISIÓN	APROBACIÓN
Gestor SGSI	Oficial de Seguridad de la Información	Gerente General

CONTROL DE VERSIONES

VERSIÓN	FECHA	DESCRIPCIÓN
02	01-11-2024	Se revisó y actualiza el documento acorde la dinámica, organización de la compañía y opciones de mejora al Sistema de Seguridad de la Información – SGSI de la empresa.