Contenido

Objetivo

El objetivo de esta política es establecer el marco general para gestionar la seguridad de la información en **Super Pagos S.A.S. (Refácil)** de acuerdo con la norma **ISO/IEC 27001:2022**. Se busca proteger los activos de información de la organización, preservando su **confidencialidad, integridad y disponibilidad de la información**, y asegurar la continuidad del negocio.

Mediante la implementación del Sistema de Gestión de Seguridad de la Información (**SGSI**), la empresa pretende minimizar el riesgo de incidentes que puedan comprometer sus operaciones (por ejemplo, **brechas de datos** que generarían pérdidas significativas en notificaciones, investigación y tiempos caídos), garantizar el **cumplimiento de los requisitos legales** aplicables, y **fortalecer la confianza** de clientes, aliados e inversionistas en sus servicios Fintech. En alineación con los objetivos estratégicos corporativos, un SGSI robusto servirá como habilitador para el **crecimiento sostenible e innovación segura** de la empresa, protegiendo su reputación y ventaja competitiva en el mercado.

Alcance

Esta política es de **cumplimiento obligatorio** para **toda la organización**, incluyendo a la Alta Dirección, empleados de todos los niveles, **contratistas**, **proveedores** de servicios y **terceros** que manejen o tengan acceso a información de **Super Pagos S.A.S.** El alcance cubre **todas las áreas y procesos** de la empresa, así como **todos los activos de información** que posea o administre, independientemente de su formato (digital o físico) o ubicación. Esto incluye, entre otros, los sistemas y aplicaciones de la plataforma **Refácil**, las bases de datos y repositorios de información, la infraestructura tecnológica (servidores, redes, dispositivos de almacenamiento), los equipos de cómputo corporativos, y la documentación confidencial. La Política General de Seguridad de la Información se aplicará en todas las sedes, operaciones y entornos de TI de la organización, y será comunicada a **todos los colaboradores y terceros relevantes**, quienes deberán adherirse a sus lineamientos. Cualquier excepción o situación no contemplada en esta política deberá ser evaluada y aprobada por el Responsable de Seguridad de la Información, garantizando siempre que no se comprometan los principios y objetivos aquí establecidos.

Contexto de la organización

Contexto interno: *Super Pagos S.A.S.* es una empresa Fintech con sede principal en Pereira, que opera la plataforma transaccional **Refácil** a nivel nacional. La organización se caracteriza por un rápido crecimiento, con innovación constante en productos digitales, y por atender a miles de micro comercios en los 32 departamentos del país. Hasta la fecha,

la seguridad de la información se había abordado de forma **reactiva y fragmentada**, sin un SGSI formalizado; por ejemplo, no existía un **inventario completo de activos y riesgos documentados** ni auditorías internas periódicas de seguridad. La cultura organizacional prioriza la rapidez y la innovación, lo cual implica el desafío de **integrar la seguridad** en todos los procesos tecnológicos y de negocio sin frenar la agilidad. Aunque el personal tiene cierta **conciencia básica** sobre protección (uso de cifrado en conexiones, autenticación, etc.), se identificó la **falta de capacitación continua** y de políticas claras que unifiquen la gestión de seguridad. Este contexto interno evidencia la necesidad de reforzar la seguridad con un enfoque sistémico: asignación de roles y responsabilidades específicas, definición de políticas y procedimientos, gestión periódica de riesgos y establecimiento de una cultura de mejora continua en seguridad.

Contexto externo: Super Pagos opera en el dinámico ecosistema **Fintech colombiano**, enfrentando un entorno de crecientes riesgos y obligaciones. En cuanto a **amenazas**, las Fintech son objetivos atractivos para actores maliciosos debido al manejo de dinero y datos sensibles. Se observa un incremento sostenido de ataques cibernéticos (malware, phishing, fraudes en pagos digitales, ransomware, etc.) en la industria financiera digital. De hecho, según reportes, alrededor del **60% de las Fintech pequeñas y medianas quiebran tras un ciberataque exitoso**, dada la magnitud del impacto y sus vulnerabilidades. Un incidente grave (por ejemplo, un ataque de ransomware) podría interrumpir bruscamente las operaciones y el crecimiento de *Super Pagos*, comprometiendo su continuidad. Por otro lado, el **entorno regulatorio** en Colombia está volviéndose más estricto con la seguridad digital: si bien *Super Pagos S.A.S.* no es un banco, interactúa con redes de pago y servicios financieros, estando bajo el escrutinio de autoridades como la **Superintendencia Financiera** y la **Superintendencia de Industria y Comercio**. Leyes como la de protección de datos personales (Ley 1581) y lineamientos específicos de ciberseguridad en finanzas imponen obligaciones claras que la empresa debe cumplir para evitar sanciones y demostrar diligencia. Adicionalmente, los **aliados comerciales** (bancos corresponsales, franquicias de tarjetas, empresas aliadas) y los **clientes** finales demandan **altos estándares de seguridad**. En un mercado Fintech competitivo, varias empresas líderes ya cuentan con certificaciones y prácticas avanzadas; por tanto, *Super Pagos* debe igualar o superar esos estándares para mantener su posición. La **confianza** de los usuarios es un activo crítico: la plataforma Refácil ha construido una reputación de ser "altamente confiable y segura", por lo que **un solo incidente público podría erosionar la confianza lograda** y afectar la imagen de la compañía. En síntesis, el contexto externo obliga a *Super Pagos* a gestionar proactivamente los riesgos de seguridad, cumplir rigurosamente con las normativas aplicables y adoptar las mejores prácticas de la industria, para proteger su negocio en el largo plazo.

Compromiso de la Alta Dirección

La **Alta Dirección** de *Super Pagos S.A.S.* manifiesta su total compromiso y apoyo hacia la seguridad de la información y la implementación del SGSI conforme a **ISO/IEC 27001:2022**. La Gerencia se responsabiliza de proveer los **recursos necesarios** (financieros, humanos y tecnológicos) para establecer, operar, mantener y mejorar continuamente el SGSI. Asimismo, se compromete a liderar con el ejemplo, **fomentando una cultura de seguridad** en toda la organización y asegurando que la seguridad de la información se integre en la toma de decisiones estratégicas. La Alta Dirección entiende que la seguridad de la información no es solo un requisito técnico, sino un **habilitador estratégico**: invertir en controles y buenas prácticas de seguridad permite **prevenir pérdidas significativas por incidentes evitados** (una sola brecha de datos moderada podría costar cientos de millones de pesos en remediación, notificaciones y tiempo de inactividad) y **evitar sanciones regulatorias onerosas** que podrían superar los mil millones de pesos en casos graves de filtraciones masivas. Adicionalmente, fortalecer la seguridad brinda ventajas competitivas, al **proteger la confianza de clientes e inversionistas** y abrir oportunidades comerciales; por ejemplo, contar con la certificación ISO 27001 puede habilitar contratos con grandes empresas que exigen altos estándares, lo que se traduce en incremento de transacciones e ingresos para el negocio. Por todo lo anterior, la Alta Dirección **aprueba y respalda esta Política** General de Seguridad de la Información, exige su estricto cumplimiento y participará activamente en su difusión, revisión periódica y mejora continua. Cualquier incumplimiento a la política será tomado con seriedad y podrá conllevar medidas disciplinarias, contando siempre con el apoyo de la Gerencia para hacer valer las disposiciones aquí descritas.

Principios Generales de Seguridad de la Información

La gestión de la seguridad de la información en *Super Pagos S.A.S.* se rige por una serie de **principios fundamentales**, alineados con las mejores prácticas internacionales, que sirven de base para todas las medidas de seguridad implementadas. Estos principios incluyen:

- **Confidencialidad:** Garantizar que la información solo sea **accesible por personas autorizadas**, protegiéndola contra accesos, uso o divulgación no autorizados. Esto implica controlar y limitar el acceso a los datos sensibles de la empresa y de los clientes, conforme al nivel de autorización de cada usuario, evitando filtraciones o fugas de datos.
- **Integridad:** Mantener la **exactitud y completitud** de la información y de los sistemas, asegurando que los datos no puedan ser alterados, manipulados o eliminados de forma indebida o por personas no autorizadas. La empresa debe salvaguardar la confiabilidad de la información a lo largo de su ciclo de vida,

previniendo modificaciones no autorizadas, errores intencionados o accidentales, y conservando evidencias ante cualquier cambio legítimo.

- **Disponibilidad:** Asegurar que la información y los recursos de procesamiento estén **disponibles cuando se requieran** por las personas autorizadas, evitando interrupciones que afecten las operaciones del negocio. Esto conlleva implementar medidas de continuidad (respaldos, planes de recuperación, redundancias) para que los servicios críticos de la plataforma *Refácil* se mantengan operativos incluso ante fallas, desastres o ataques, garantizando que los usuarios puedan realizar sus transacciones en todo momento.
- **Legalidad:** Cumplir con todas las **leyes, regulaciones y obligaciones contractuales** aplicables en materia de seguridad de la información y protección de datos. La organización se asegurará de que el tratamiento de la información (especialmente de datos personales de clientes, empleados y terceros) respete la normativa vigente – por ejemplo, la Ley 1581 de 2012 de Protección de Datos Personales y sus decretos reglamentarios – implementando medidas de seguridad apropiadas que eviten accesos o usos no autorizados de dichos datos. Este principio implica también la observancia de las leyes penales sobre delitos informáticos y el cumplimiento de los lineamientos exigidos por los entes reguladores del sector.
- **Trazabilidad y No Repudio:** Mantener la capacidad de **rastrear todas las acciones** realizadas sobre la información y los sistemas, de forma que se pueda determinar **quién, cuándo, cómo y qué** cambios o accesos se han efectuado. Esto garantiza la **responsabilidad** sobre el uso de la información y provee evidencia en caso de auditorías o investigaciones. La trazabilidad se logra mediante registros de auditoría detallados (logs) y controles de monitoreo que capturan eventos relevantes. Asociado a ello, el principio de **No Repudio** asegura que ninguna de las partes pueda negar legítimamente haber realizado una acción o transacción digital específica. Para reforzar el no repudio y la trazabilidad, se emplearán mecanismos como firmas electrónicas, controles de autenticidad y registros inalterables, que ofrezcan pruebas verificables de cada interacción con los activos de información.
- **Transparencia y Privacidad:** (En el contexto de protección de datos personales) Tratar los datos de manera transparente ante sus titulares y respetar su **privacidad** como derecho fundamental. La empresa informará y capacitará a los usuarios internos en las prácticas adecuadas de manejo de información personal, garantizando que cualquier procesamiento de datos personales cuente con las autorizaciones requeridas y se ajuste a los principios de la Ley de Protección de Datos (legalidad, finalidad, libertad, veracidad, acceso y circulación restringida, seguridad y confidencialidad). Asimismo, se adoptarán medidas para que los titulares de datos puedan ejercer sus derechos (conocer, actualizar, rectificar y suprimir información) conforme a la normatividad vigente.

Estos principios generales sirven de guía para todas las políticas específicas, estándares, procedimientos y controles que conforman el SGSI de *Super Pagos S.A.S.* Su cumplimiento es mandatorio y cualquier acción que los contravenga será considerada como una desviación de la política de seguridad.

Directrices y compromisos

Para materializar los principios anteriores, *Super Pagos S.A.S.* establece las siguientes **directrices y compromisos estratégicos** en materia de seguridad de la información:

- **Implementación del SGSI:** La empresa se compromete a establecer y mantener un **Sistema de Gestión de Seguridad de la Información** acorde con ISO/IEC 27001:2022, asegurando que todas las actividades de seguridad estén **alineadas con los objetivos de negocio** e integradas en los procesos organizacionales. Se definirán **objetivos de seguridad** medibles y coherentes con la estrategia corporativa, los cuales serán periódicamente revisados y actualizados conforme a la evolución del negocio y el entorno de amenazas.
- **Enfoque basado en riesgos:** Todas las decisiones de seguridad se tomarán siguiendo un **enfoque basado en la gestión de riesgos**. La organización **identificará, analizará y evaluará los riesgos** de seguridad de la información de manera regular, priorizando la implementación de **controles de seguridad** en función del nivel de riesgo (impacto y probabilidad) que enfrenten los activos. Se mantendrá un **Registro de Riesgos** actualizado y se desarrollarán Planes de Tratamiento de Riesgos para mitigar los riesgos inaceptables, seleccionando los controles apropiados (conforme a la Declaración de Aplicabilidad, SoA).
- **Protección de activos de información:** La empresa **mantendrá un inventario actualizado** de todos sus activos de información relevantes (incluyendo datos, sistemas, infraestructura, personas, servicios y suministros). Cada activo tendrá un **propietario responsable** y será **clasificado** según su nivel de sensibilidad y criticidad para el negocio. En función de dicha clasificación, se aplicarán **medidas de protección adecuadas** para preservar la confidencialidad, integridad y disponibilidad de cada activo. Por ejemplo, se protegerán rigurosamente los activos críticos identificados – tales como *datos de clientes*, *bases de datos transaccionales*, *servidores y aplicaciones* de la plataforma Refácil – aplicando controles de seguridad proporcionales al riesgo (cifrado de información sensible, copias de seguridad frecuentes, seguridad perimetral en la red, etc.). Asimismo, se implementarán controles físicos donde corresponda (p. ej., acceso restringido a centros de datos u oficinas donde se encuentren archivos confidenciales).
- **Control de accesos:** Se gestionarán los accesos lógicos y físicos a los sistemas e información bajo el principio de **mínimo privilegio** y **necesidad de saber**. Esto significa que a cada usuario, sistema o proceso se le otorgarán únicamente los

permisos indispensables para desempeñar sus funciones, evitando accesos indiscriminados o no justificados. El otorgamiento de accesos requerirá la autorización correspondiente y un registro formal, y todos los accesos privilegiados serán objeto de monitoreo y control adicionales. Se adoptarán mecanismos de **autenticación robusta** para verificar la identidad de los usuarios (incluyendo contraseñas con complejidad adecuada y, donde sea posible, **autenticación de múltiples factores** para sistemas críticos). Los accesos de usuarios serán **revisados periódicamente** (al menos cada seis meses) para revocar o ajustar privilegios que ya no correspondan con las funciones del rol, especialmente tras movimientos de personal o terminaciones de contrato. Igualmente, se controlará el **acceso físico** a las instalaciones y equipos sensibles (oficinas, cuartos de servidores), permitiéndolo solo a personal autorizado y utilizando métodos de seguridad como tarjetas de acceso personal, cerraduras especializadas, registros de visitantes y vigilancia, a fin de prevenir que individuos no autorizados puedan acceder a recursos críticos.

- **Seguridad por diseño y por defecto:** En el desarrollo o adquisición de nuevos sistemas, productos o servicios, la organización se compromete a incorporar la seguridad de la información **desde la etapa de diseño** (Security by Design) y a aplicar configuraciones seguras por defecto (Security by Default). Esto implica realizar **evaluaciones de riesgo y revisiones de seguridad** en proyectos de TI desde sus inicios, incluir requerimientos de seguridad en los contratos con proveedores de software o servicios, y seguir estándares de codificación segura en los desarrollos internos. Cualquier cambio significativo en la infraestructura de TI (actualizaciones, nuevos componentes) deberá pasar por un proceso de **gestión de cambios** que considere el impacto en la seguridad y garantice las pruebas necesarias antes de la puesta en producción.
- **Criptografía y protección de datos sensibles:** La empresa utilizará técnicas de **cifrado** y controles criptográficos para proteger la información sensible tanto en tránsito como en reposo. Se cifrarán, por ejemplo, las comunicaciones transaccionales de Refácil, las contraseñas y credenciales almacenadas, y aquellos campos de datos personales o financieros de clientes que requieran secreto. Se implementarán además controles de **gestión de claves criptográficas** adecuadas, asegurando su generación, distribución, almacenamiento, rotación y destrucción segura según políticas definidas. De igual manera, se protegerán los datos sensibles mediante **seudonimización o enmascaramiento** cuando corresponda, y se aplicarán controles de integridad (firmas digitales, hashes) para detectar cualquier alteración no autorizada de la información.
- **Gestión de cambios y parches:** Como parte del compromiso con la integridad y disponibilidad, la organización mantendrá procedimientos de **gestión de cambios** en los sistemas de información, de modo que cualquier modificación de software, hardware o configuraciones sea planificada, evaluada en cuanto a riesgos, probada

en ambientes controlados y aprobada antes de su implementación en producción. Asimismo, se establecerá un proceso de **gestión de parches y actualizaciones de seguridad**, asegurando que los sistemas operativos, aplicaciones y dispositivos de red reciban oportunamente las correcciones suministradas por los fabricantes para remediar vulnerabilidades conocidas, reduciendo la ventana de exposición a ataques.

- **Responsabilidad individual y colectiva:** Todos los miembros de la organización, sin excepción, tienen la responsabilidad de proteger la información de *Super Pagos*. Se espera de cada colaborador un comportamiento proactivo y alineado con esta política: desde **cumplir las normas y procedimientos** de seguridad en su trabajo diario (por ejemplo, manejo adecuado de contraseñas, no divulgación de información confidencial, bloqueo de sesión al ausentarse, uso seguro del correo y de Internet), hasta **reportar oportunamente** cualquier incidente o debilidad de seguridad que observen. La Alta Dirección se compromete a apoyar una cultura en la cual se promueva la **comunicación abierta** de problemas de seguridad (sin temor a represalias), comprendiendo que la seguridad de la información es una responsabilidad compartida.
- **Cumplimiento y disciplina:** El cumplimiento de esta política y de las políticas específicas derivadas de ella es **obligatorio**. Se realizarán **verificaciones periódicas** (auditorías internas, autoevaluaciones, monitoreo continuo) para asegurar la adherencia a los lineamientos establecidos. Cualquier incumplimiento o violación a la política será evaluado por el Comité de Seguridad de la Información (o la instancia designada) y puede resultar en **acciones disciplinarias**, incluyendo sanciones laborales conforme al reglamento interno de trabajo, e incluso **acciones legales** en caso de que se evidencie dolo o negligencia grave que derive en daños a la compañía o terceros. Los terceros que incumplan las medidas de seguridad acordadas contractualmente también enfrentaran consecuencias, que pueden implicar la terminación de contratos y reclamaciones por los perjuicios ocasionados.

Estos compromisos generales sientan las bases para un programa robusto de seguridad. Las secciones siguientes desarrollan con mayor detalle aspectos específicos como responsabilidades, cumplimiento legal, gestión de riesgos y otros, los cuales se desprenden y armonizan con las directrices aquí enumeradas.

Roles y responsabilidades

Para el funcionamiento eficaz del SGSI y el cumplimiento de esta política, se definen claramente **roles y responsabilidades** en la organización:

- **Alta Dirección:** Aprobar la Política General de Seguridad de la Información y demostrar liderazgo y compromiso con su implementación. Los directivos deben

garantizar la asignación de recursos necesarios, integrar la seguridad en los objetivos estratégicos y realizar un **seguimiento activo** del desempeño del SGSI. La Alta Dirección presidirá (o delegará) la **Revisión por la Dirección** del SGSI al menos anualmente, evaluando resultados e impulsando mejoras. También vela por que todas las unidades cumplan sus responsabilidades de seguridad y por establecer una cultura organizacional que valore la protección de la información.

- **Comité de Seguridad de la Información (si aplica):** Órgano multidisciplinario conformado por representantes de diferentes áreas (TI, Riesgos, Legal, Operaciones, etc.) que apoyan la gobernanza del SGSI. Sus responsabilidades incluyen coordinar la elaboración y actualización de políticas de seguridad, priorizar iniciativas y planes de acción en materia de seguridad, hacer seguimiento a indicadores y riesgos clave, y servir de puente entre la Alta Dirección y las áreas operativas para la toma de decisiones relacionadas con seguridad. El Comité sesionará periódicamente para revisar el estado del SGSI, los incidentes ocurridos, las evaluaciones de riesgo y proponer mejoras o inversiones requeridas.
- **Responsable de Seguridad de la Información (CISO/Oficial de Seguridad):** Profesional designado para liderar la implementación diaria del SGSI. Actúa como **propietario** de esta política y de las políticas específicas de seguridad, asegurando que se mantengan actualizadas y efectivas. Sus funciones incluyen: coordinar los análisis de riesgos y las auditorías internas de seguridad; supervisar la implementación de controles y proyectos de seguridad; gestionar el plan de formación y concienciación en seguridad; monitorear el cumplimiento de las políticas; asesorar a las distintas áreas en materia de seguridad; reportar a la Alta Dirección sobre el desempeño del SGSI; y liderar la respuesta ante incidentes de seguridad. El Responsable de Seguridad tiene la **autoridad** para intervenir en cualquier proceso o sistema cuando se identifiquen brechas de seguridad, actuando en el mejor interés de la protección de la información de la compañía.
- **Propietarios de Activos de Información:** Para cada activo de información crítico identificado en el inventario, se asignará un **Propietario** (generalmente un gerente o jefe de área relacionado con el proceso de negocio vinculado al activo). El propietario del activo es responsable de **garantizar la protección adecuada** de dicho activo a lo largo de su ciclo de vida. Esto implica: clasificar el activo según su sensibilidad, definir quién puede usarlo y con qué privilegios, asegurar que se implementen los controles necesarios (con apoyo del área de TI/Seguridad), y revisar periódicamente la criticidad y uso del activo. Por ejemplo, el Gerente de Operaciones podría ser propietario de la base de datos de transacciones, debiendo asegurar que esté cifrada, respaldada y accesible solo para personal autorizado, etc. Si se presentan riesgos o incidentes relacionados con el activo, el propietario colabora estrechamente con el Responsable de Seguridad en su tratamiento.
- **Custodios/Tecnología (Equipos de TI y Desarrollo):** Son las áreas o personas encargadas de la **administración técnica** de los activos de información (por

ejemplo, administradores de sistemas, de bases de datos, desarrolladores de software, personal de infraestructura y soporte TI). Actúan como **custodios** implementando los controles de seguridad en la práctica: gestionan cuentas de usuario en sistemas, aplican parches de seguridad, realizan backups, monitorean la red, desarrollan aplicaciones seguras siguiendo las directrices establecidas, y atienden las alertas de seguridad que se presenten. Deben cumplir estrictamente con los procedimientos y estándares técnicos de seguridad definidos (configuraciones seguras, separación de entornos, controles de acceso, etc.) y apoyar las evaluaciones de riesgo aportando información técnica. Aunque estos equipos ejecutan las tareas técnicas, lo hacen en coordinación con los propietarios de los activos y bajo la supervisión del Responsable de Seguridad.

- **Todos los empleados y usuarios con acceso a la información:** Cada empleado, contratista o tercero autorizado con acceso a sistemas o datos de *Super Pagos* tiene la **responsabilidad individual** de proteger la información conforme a esta política y las normas asociadas. Deben **conocer y acatar** las políticas y procedimientos de seguridad (se les brindará capacitación para ello), usar la información únicamente para los fines autorizados y conforme a su rol, mantener la confidencialidad de la información sensible a la que acceden, y notificar de inmediato cualquier incidente o debilidad de seguridad que detecten. Se espera de todos una actitud diligente: por ejemplo, evitar prácticas inseguras como compartir contraseñas, conectar dispositivos desconocidos a la red corporativa, instalar software no autorizado, o divulgar información de clientes sin autorización. El desconocimiento de las políticas no exime de responsabilidad; por ello la empresa proveerá los recursos formativos necesarios, pero cada empleado debe comprometerse activamente con la seguridad.
- **Terceros (proveedores, aliados, contratistas externos):** Cualquier tercero que, por la naturaleza de su servicio o relación con *Super Pagos*, tenga acceso a información de la empresa o interactúe con sus sistemas, deberá **cumplir con las políticas y controles de seguridad** equivalentes a los exigidos internamente. La organización se asegurará de incluir en los contratos cláusulas de **confidencialidad** y de **seguridad de la información**, estableciendo las obligaciones que el tercero debe cumplir (por ejemplo, protección de datos personales según la ley, notificación de incidentes de seguridad, medidas mínimas de seguridad técnica, etc.). Los terceros críticos podrán ser sometidos a **evaluaciones o auditorías** de seguridad periódicas, y deberán acatar las recomendaciones de mejora que se deriven. En particular, proveedores de servicios en la nube, procesamiento de pagos, desarrollo de software u otros que manejen información sensible de *Super Pagos* estarán sujetos a un monitoreo activo. La falta de cumplimiento por parte de un tercero puede dar lugar a la terminación de la relación contractual y a las acciones legales correspondientes. Este control de terceros es crucial dado que los **aliados comerciales y entes del sector** esperan que *Super Pagos* gestione

adecuadamente la seguridad en toda su cadena de suministro para no introducir riesgos al ecosistema financiero.

En resumen, la seguridad de la información es responsabilidad de **todos** en la organización, con distintos niveles de responsabilidad según el rol. La colaboración y comunicación entre estos roles será fundamental para el éxito del SGSI: cada quien debe entender su función y trabajar conjuntamente para proteger los activos de información de la empresa.

Cumplimiento legal y normativo

Super Pagos S.A.S. se compromete a **cumplir plenamente** con la legislación colombiana vigente y con cualquier requerimiento normativo aplicable en materia de seguridad de la información, protección de datos y continuidad de negocio, así como con los estándares de la industria financiera que correspondan a sus operaciones. En particular, la organización observará lo siguiente:

- **Ley 1581 de 2012 – Protección de Datos Personales:** Como responsable de bases de datos personales de clientes, empleados y terceros, *Super Pagos* cumplirá con la Ley Estatutaria de Protección de Datos Personales y sus normas reglamentarias. Esto incluye aplicar los principios de tratamiento de datos (finalidad, necesidad, veracidad, seguridad, confidencialidad, etc.), obtener las autorizaciones de los titulares, implementar medidas técnicas y administrativas para la seguridad de los datos sensibles, notificar y registrar las bases de datos ante la Superintendencia de Industria y Comercio (SIC) cuando sea obligatorio, y en general garantizar el derecho de Habeas Data de las personas. Se tendrá una Política de Tratamiento de Datos Personales disponible para los titulares y se atenderán oportunamente sus consultas o reclamos, tal como exige la ley.
- **Ley 1273 de 2009 – Delitos Informáticos:** Esta ley incorporó al Código Penal colombiano los delitos relacionados con la protección de la información y los datos. *Super Pagos S.A.S.* apoyará activamente el cumplimiento de esta norma, no solo absteniéndose de incurrir en conductas ilícitas, sino también **protegiendo sus sistemas** para prevenir acciones de terceros tipificadas en dicha ley (como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, daños o sabotaje informático, uso de software malicioso, suplantación de sitios web para capturar datos –phishing–, entre otros). Se implementarán los controles necesarios (firewalls, sistemas antimalware, monitoreo de accesos, mecanismos de autenticación robusta, etc.) para reducir la probabilidad de que la empresa sea víctima o plataforma involuntaria de estos delitos. En caso de presentarse un incidente que pudiera constituir un delito informático, la organización colaborará con las autoridades competentes (ej. denuncia ante la Fiscalía) aportando evidencias de auditoría y tomando acciones internas para mitigar el daño.

- **Normativas de la Superintendencia Financiera de Colombia (SFC):** Dado que *Super Pagos* opera en el sector de pagos electrónicos y podría estar sujeta a la vigilancia o regulación indirecta de la SFC, se mantendrá en conformidad con los **lineamientos y circulares** que dicho ente emita respecto a la gestión de riesgos tecnológicos, seguridad cibernética y calidad en servicios financieros digitales. Por ejemplo, la empresa tomará como referencia los estándares de la **Circular Externa 052 de 2017 de la SFC** sobre requisitos de ciberseguridad para entidades financieras, en la medida que tales lineamientos resulten aplicables a su operación como compañía de servicios tecnológicos/financieros. También se observarán las instrucciones relacionadas con **Seguridad y Continuidad del Negocio** contenidas en la Circular Básica Contable y Financiera, y cualquier requerimiento específico que la SFC pueda comunicar a empresas de pago de bajo valor o Fintech dentro de sus programas de innovación financiera (Sandbox regulatorio, etc.).
- **Regulación sobre Banca Abierta (Open Banking/Finance):** *Super Pagos S.A.S.* se preparará para cumplir con el marco regulatorio emergente en Colombia sobre **finanzas abiertas**, incluyendo las disposiciones del **Decreto 1297 de 2022** y normas complementarias, que establecen estándares de seguridad reforzada para el intercambio de datos financieros entre entidades. Esto implicará asegurar la **disponibilidad de APIs** con autenticación y autorización robustas, protección de datos en tránsito y en reposo, y controles de acceso estrictos para terceros que integren con la plataforma, de acuerdo a los estándares definidos por las autoridades financieras. La adopción de ISO 27001 posiciona a la empresa un paso adelante en este ámbito, facilitando demostrar conformidad con las expectativas de seguridad en esquemas de open banking.
- **Normativa de la Superintendencia de Industria y Comercio (SIC):** Además de la Ley 1581, la SIC expide guías y circulares relacionadas con la seguridad de la información y la protección de los consumidores en entornos electrónicos. *Super Pagos* velará por cumplir con, por ejemplo, las disposiciones sobre comercio electrónico seguro, la Ley 1480 de 2011 (Estatuto del Consumidor) en lo referente a la protección de datos de tarjetas de crédito/débito durante transacciones, y atenderá cualquier requerimiento de la Delegatura de Protección de Datos de la SIC en caso de investigaciones por incidentes de seguridad. Mantener un SGSI robusto y evidencia de controles ayudará a demostrar ante la SIC la debida diligencia en la protección de los datos personales.
- **Estándares y mejores prácticas de la industria:** La empresa alineará sus controles también con estándares reconocidos internacionalmente que apliquen a su sector. Por ejemplo, de ser necesario por la naturaleza de las transacciones con tarjetas, se observarán los lineamientos de **PCI DSS** (Payment Card Industry Data Security Standard) para la protección de datos de tarjetas de pago. Asimismo, se considerarán las recomendaciones de la **Asobancaria** en materia de ciberseguridad para pagos digitales, y las mejores prácticas publicadas en estándares como

ISO 27002, NIST CSF, COBIT, entre otros marcos relevantes. Cuando la empresa participe en ecosistemas o redes de negocio (ej. integraciones con bancos, agregadores de pagos, pasarelas), cumplirá los **acuerdos de nivel de seguridad** exigidos por esos aliados, evitando introducir riesgos sistémicos al ecosistema financiero.

- **Otras leyes y regulaciones aplicables:** *Super Pagos* también dará cumplimiento a otras normativas que puedan aplicar, tales como la Ley 1266 de 2008 (habeas data financiero), regulaciones de Lavado de Activos y Financiación del Terrorismo en lo relacionado con reportes de operaciones sospechosas (SARLAFT, en cuanto al manejo seguro de información de clientes y reportes a autoridades), la Ley 527 de 1999 (comercio electrónico y firmas digitales), la Ley 1523 de 2012 (gestión de riesgo y continuidad en servicios esenciales) en aquello que corresponda, entre otras. La compañía se mantendrá atenta a cambios legislativos o nuevos requerimientos regulatorios en materia de seguridad/ciberseguridad, ajustando su SGSI de forma proactiva para garantizar la conformidad.

El cumplimiento legal y normativo será objeto de **monitoreo continuo**. La empresa asignará a su área legal o de cumplimiento, en colaboración con el Responsable de Seguridad, la tarea de vigilar cambios en las leyes/regulaciones y evaluar su impacto. Adicionalmente, se llevarán a cabo **auditorías de cumplimiento** donde se verifique periódicamente que las operaciones, controles y políticas de *Super Pagos* estén alineados con las obligaciones mencionadas. El no cumplimiento de requerimientos legales podría exponer a la organización a sanciones severas (multas, investigaciones e incluso restricción de operaciones), por lo que la empresa adopta una postura de **cero tolerancia** frente a desviaciones en este ámbito. Cada empleado y área de la empresa deberá apoyar el cumplimiento normativo en sus funciones, bajo la coordinación general del Oficial de Seguridad de la Información y la asesoría de la unidad jurídica.

Gestión de riesgos

La **Gestión de Riesgos de Seguridad de la Información** es un pilar central del SGSI de *Super Pagos S.A.S.* La organización adopta un proceso sistemático para **identificar, evaluar, tratar y monitorear** los riesgos que puedan afectar la seguridad de sus activos de información, con el fin de reducirlos a niveles aceptables de acuerdo con el apetito de riesgo definido por la Alta Dirección.

En términos generales, el proceso de gestión de riesgos seguirá estos pasos:

1. **Identificación de activos, amenazas y vulnerabilidades:** La empresa mantiene un **Inventario de Activos de Información** completo (hardware, software, datos, personas, procesos, infraestructura, proveedores, etc.). Para cada activo, se

identificarán las **amenazas potenciales** (eventos que podrían causarle daño, como ataques cibernéticos, errores humanos, fallos de hardware, desastres naturales, fraude interno, etc.) y las **vulnerabilidades** o debilidades que pudieran ser explotadas por dichas amenazas (por ejemplo, falta de parches, configuraciones inseguras, capacitación insuficiente del personal, ausencia de respaldos, etc.). Este análisis abarca tanto riesgos tecnológicos como riesgos físicos y organizacionales.

2. **Evaluación del riesgo:** Se analizará el impacto potencial que tendría cada riesgo identificado sobre el negocio (ej. impacto financiero, reputacional, legal, operacional) y la probabilidad de que dicho riesgo se materialice, considerando los controles existentes. *Super Pagos* utilizará metodologías de valoración (cualitativas o semicuantitativas) para asignar una **calificación de riesgo** a cada escenario identificado (por ejemplo, niveles de riesgo bajo, medio, alto o puntuaciones en una matriz de calor). Los **riesgos clave** – tales como la brecha de datos personales masiva, un ataque de **ransomware** que paralice la plataforma, fraudes en transacciones electrónicas, indisponibilidad prolongada del sistema central de pagos, o fallos en la cadena de proveedores críticos – recibirán especial atención en la evaluación, dada su posibilidad de causar pérdidas severas o comprometer la continuidad del negocio.
3. **Tratamiento del riesgo:** Para cada riesgo identificado, se definirán estrategias de tratamiento, que pueden incluir: **mitigación** (implementar nuevos controles o reforzar los existentes para reducir la probabilidad y/o impacto), **aceptación** (cuando el riesgo residual es bajo o el costo de mitigarlo excede el beneficio, con aprobación de la Alta Dirección), **transferencia** (por ejemplo mediante seguros o contratos con terceros que compartan el riesgo) o **evitación** (cese de la actividad de riesgo, si ninguna mitigación lo reduce a niveles aceptables). Se elaborará un **Plan de Tratamiento de Riesgos** formal que detalle las medidas a tomar, los responsables y plazos de implementación. Las medidas de seguridad (controles) seleccionadas para mitigar riesgos se documentarán en la **Declaración de Aplicabilidad (SoA)**, justificando su inclusión o exclusión en base a los resultados del análisis de riesgos.
4. **Implementación de controles:** Las acciones y controles definidos en el plan de tratamiento serán implementados por las áreas correspondientes (TI, RRHH, Operaciones, etc.), bajo la coordinación del Responsable de Seguridad. Los controles pueden abarcar soluciones tecnológicas (p. ej. sistemas de detección de intrusos, autenticación 2FA, cifrado de bases de datos), controles administrativos (p. ej. procedimientos de gestión de incidencias, políticas de acceso, separación de funciones) y controles físicos (p. ej. mecanismos antincendios, control de acceso a oficinas). Se asignarán métricas o indicadores donde sea posible para medir la eficacia de los controles (por ejemplo, número de incidentes de cierto tipo antes y después, resultados de pruebas de penetración, etc.).
5. **Monitoreo y revisión de riesgos:** La empresa llevará a cabo **revisiones periódicas de riesgos** (por lo menos de manera anual, y también cuando ocurran

cambios significativos en los sistemas, en la estructura de la organización, amenazas emergentes o incidentes relevantes). Estas revisiones permitirán actualizar el inventario de riesgos, verificar si las calificaciones de riesgo han cambiado (por mejoras en controles o nuevas vulnerabilidades), y evaluar la eficacia de las medidas implementadas. Adicionalmente, se implementará un **monitoreo continuo** a través de herramientas de seguridad (ej. monitoreo de eventos SIEM, análisis de vulnerabilidades periódico, revisiones de configuración) para detectar a tiempo condiciones de riesgo. Los resultados de la gestión de riesgos serán reportados a la Alta Dirección y discutidos en la Revisión Gerencial del SGSI, a fin de **tomar decisiones informadas** sobre inversiones o ajustes necesarios en la estrategia de seguridad.

Este ciclo de gestión de riesgos garantiza que *Super Pagos S.A.S.* destine esfuerzos y recursos de seguridad de manera **priorizada**, enfrentando primero aquellos riesgos que puedan tener impacto más crítico en la operación, los clientes o el cumplimiento regulatorio. Cabe destacar que la **aceptación de riesgos residuales significativos** solo la podrá realizar la Alta Dirección, documentando las razones de negocio para hacerlo y siempre que se mantengan dentro del apetito de riesgo acordado. La gestión de riesgos está intrínsecamente ligada a la mejora continua: cada incidente de seguridad ocurrido o cada cambio en el entorno proveerá retroalimentación para recalibrar el análisis de riesgos y fortalecer el SGSI. En conclusión, *Super Pagos* adopta una postura proactiva y preventiva frente a los riesgos, entendiendo que invertir en mitigarlos es ampliamente más costo-efectivo que enfrentar las consecuencias de eventos adversos no controlados.

Protección de los activos de información

Los **activos de información** de *Super Pagos S.A.S.* constituyen todos aquellos recursos que poseen valor para la organización en materia de datos y procesos de información. Esto incluye, entre otros: la **información** en sus diversas formas (datos electrónicos de clientes, registros transaccionales, informes financieros, documentos en papel), los **sistemas y aplicaciones** (p. ej. la plataforma web y app móvil *Refácil*, aplicaciones internas de gestión, servicios en la nube utilizados), la **infraestructura tecnológica** (servidores físicos y virtuales, bases de datos, dispositivos de red, equipos de cómputo, centros de datos), los **servicios de soporte** (servicios de internet, comunicaciones, energía que sostienen las TI), y las **personas** que interactúan con la información (empleados, usuarios, terceros con acceso). Cada uno de estos activos, identificados en el Inventario de Activos de Información corporativo, debe estar debidamente **protegido contra amenazas** que puedan comprometer su confidencialidad, integridad o disponibilidad.

Las directrices para la protección de activos son:

- **Clasificación de la información:** Toda la información de la empresa será categorizada según su nivel de sensibilidad y criticidad. Se utilizará un esquema de **clasificación** (por ejemplo: **Pública, Interna, Confidencial, Secreta**), definido en una política específica. Cada información o documento recibirá un nivel de clasificación acorde a su contenido: datos personales y financieros de clientes, contraseñas, claves privadas y estrategia corporativa serían *Información Confidencial o Secreta*; información operativa interna de uso cotidiano podría ser *Información Interna*; contenidos divulgables o publicados (como información comercial ya pública) serían *Información Pública*. Esta clasificación determinará los controles mínimos aplicables: por ejemplo, la *información Confidencial* deberá cifrarse para su almacenamiento o trasmisión, tendrá acceso restringido solo a roles autorizados, y no podrá ser compartida externamente sin acuerdos de confidencialidad, etc.
- **Inventario y propietarios:** Se mantendrá un **Inventario detallado de activos** que incluya la descripción del activo, su ubicación, el propietario responsable, su clasificación, y otras características relevantes (software asociado, versión, etc.). Los activos más críticos identificados – v.gr. la **Base de Datos central de Refácil** que contiene el historial de transacciones, el **servidor de autenticación** de usuarios, el **repositorio de código fuente** de las aplicaciones, la **información financiera** y contable, o las **computadoras portátiles** con acceso a información sensible – tienen asignados **propietarios** que gestionan su protección. Los propietarios de activos trabajan conjuntamente con TI/Seguridad para definir qué medidas de protección se requieren y verificar periódicamente que dichas medidas estén funcionando adecuadamente.
- **Medidas de protección por tipo de activo:** Dependiendo de la naturaleza del activo, se aplicarán controles específicos:
    - *Activos de hardware e infraestructura:* Todos los servidores, equipos de comunicaciones y dispositivos de almacenamiento críticos estarán ubicados en entornos seguros (p. ej. centro de datos con control de acceso físico, aire acondicionado, protección contra incendios y fallos eléctricos mediante UPS o plantas). Se llevará control de quién tiene acceso físico a estos equipos. Los equipos de usuario final (computadores portátiles, USB, móviles corporativos) contarán con **cifrado de disco** y mecanismos de borrado remoto en caso de pérdida o robo, además de soluciones antimalware actualizadas.
    - *Aplicaciones y Software:* El **desarrollo seguro** es fundamental para aplicaciones de la plataforma Refácil; se seguirá un ciclo de vida que incluya revisiones de código (code review), pruebas de penetración antes de lanzamientos, y remediación de vulnerabilidades identificadas. Las aplicaciones tendrán implementadas **controles de validación de entradas**, gestión segura de sesiones y protección contra las principales amenazas

web (SQL injection, XSS, CSRF, etc.). Los componentes de software de terceros (frameworks, librerías) serán actualizados regularmente para mitigar riesgos.

- *Bases de datos e información en reposo:* Los repositorios de datos (bases de datos SQL, almacenamientos de archivos) que contengan información sensible serán **cifrados** al nivel de almacenamiento, y solo personal autorizado (DBAs y sistemas con cuentas de servicio aprobadas) podrá acceder a ellos. Se habilitarán **logs de auditoría** en las bases de datos para registrar accesos a datos críticos (consultas, modificaciones), con alertas ante operaciones inusuales. Se realizarán **copias de seguridad (backups) periódicas** de todos los datos esenciales, almacenándolas de forma segura (cifradas y preferiblemente fuera del sitio principal o en la nube) y probando regularmente la restauración para garantizar la recuperabilidad de la información.
- *Redes y comunicaciones:* La red corporativa estará segmentada para aislar entornos críticos (por ejemplo, segmentar la red de servidores de la de usuarios, y ésta de la red pública). Se implementarán **firewalls y sistemas de detección/prevención de intrusos (IDS/IPS)** para monitorear y filtrar el tráfico de red entrante y saliente, bloqueando accesos no autorizados o actividad sospechosa. Todo acceso remoto a la red de la empresa (por administradores o teletrabajadores) deberá realizarse a través de canales seguros (VPN con cifrado robusto, autenticación multifactor). Las APIs o servicios de integración con socios externos estarán protegidas con autenticación fuerte (tokens, certificados digitales) y límites de uso (throttling) para prevenir abusos. Asimismo, la información que viaje por redes públicas o enlaces de comunicaciones será cifrada usando protocolos seguros (HTTPS/TLS, SFTP, etc.) evitando en lo posible protocolos no seguros (FTP, Telnet, HTTP sin cifrado).
- *Documentación física:* Cualquier documento en papel o medio removible que contenga información confidencial (por ejemplo, contratos con clientes, expedientes de personal, reportes financieros) deberá guardarse en **archivadores bajo llave** o áreas de acceso controlado. Habrá lineamientos para el **descarte seguro** de documentos físicos (uso de trituradoras para destruir papel con datos sensibles) y de equipos electrónicos obsoletos (borrado seguro de discos antes de su disposición final). Además, se etiquetará la documentación conforme a su clasificación (p. ej. marcas de “Confidencial” en portadas) y se restringirá su copia o reproducción sin autorización.

- **Control de ambientes y continuidad:** Los entornos donde residen los activos críticos (p. ej. el centro de datos o la sala de servidores de Refácil) contarán con medidas de **seguridad ambiental** que incluyen detección y supresión de incendios,

control de humedad y temperatura, y sistemas de energía de respaldo para tolerar fallos eléctricos. A nivel de continuidad, se elaborarán **Planes de Continuidad del Negocio y Recuperación de Desastres** para escenarios de indisponibilidad mayor (fallo total del centro de datos, desastres naturales, ciberataques devastadores), de forma que la empresa pueda reanudar sus operaciones en tiempos definidos. Estos planes identificarán los activos vitales y establecerán estrategias como sitios alternos, redundancia de comunicaciones, procedimientos manuales temporales, etc., para asegurar que la información y servicios clave se mantengan disponibles. Dichos planes serán probados a intervalos regulares para verificar su eficacia.

En síntesis, cada activo de información de *Super Pagos S.A.S.* recibirá una protección acorde a su valor y riesgos asociados. La conjunción de **clasificación, controles técnicos, físicos y administrativos, y planes de continuidad** garantiza un enfoque integral de protección. La empresa revisará y actualizará sus esquemas de protección de activos ante cambios en el entorno de amenazas o descubrimiento de nuevas vulnerabilidades, manteniendo así una postura de seguridad actualizada.

Control de accesos

El **Control de Accesos** adecuado es fundamental para asegurarse de que solo las personas autorizadas (o procesos legítimos) pueden interactuar con los sistemas y datos de *Super Pagos S.A.S.*, según lo establecido en los principios de confidencialidad y disponibilidad. La organización implementará una **política de control de accesos** que abarca tanto los accesos lógicos a sistemas informáticos como los accesos físicos a instalaciones y equipos.

Las medidas y lineamientos principales en este aspecto son:

- **Gestión de identidades y cuentas de usuario:** Toda persona que requiera acceso a los sistemas de información de la empresa deberá tener una **identidad digital única** (por ejemplo, un nombre de usuario individual) y sus accesos se concederán basados en roles de trabajo predefinidos. No se permiten cuentas genéricas o compartidas para uso regular de sistemas críticos; las cuentas con privilegios especiales (administradores de sistemas, DBA, etc.) tendrán controles adicionales y serán nominativas. El proceso de **aprobación de usuarios** incluirá la autorización explícita del jefe del área o propietario del activo correspondiente, siguiendo el principio de mínima asignación de privilegios. La asignación de cada nuevo acceso quedará documentada (solicitud y aprobación), manteniéndose un registro centralizado de cuentas y permisos otorgados.
- **Autenticación y control de credenciales:** Todos los accesos a sistemas estarán protegidos por mecanismos de **autenticación**. Se exigirá el uso de **contraseñas**

robustas en concordancia con la política corporativa (mínimo de longitud, complejidad de caracteres, prohibición de reutilizar contraseñas anteriores, caducidad periódica si aplica). Cuando sea posible, se implementará **autenticación de múltiples factores (MFA)**, especialmente para accesos remotos, cuentas con privilegios elevados o sistemas que contengan datos sensibles de clientes. Las credenciales (contraseñas, llaves privadas, tokens) deberán almacenarse y transmitirse de forma segura: por ejemplo, las contraseñas se almacenarán en formato **hash con algoritmo criptográfico fuerte**, y nunca en texto plano; los canales de autenticación utilizarán conexiones cifradas. Adicionalmente, se educará a los usuarios para que mantengan la confidencialidad de sus credenciales (no compartir contraseñas, no anotarlas en lugares visibles, etc.).

- **Autorización y control de privilegios:** Una vez autenticado un usuario, el sistema debe aplicar controles de **autorización** para garantizar que solo accede a la información y funcionalidades para las cuales tiene permiso. Para esto, se definirán **perfiles de acceso** según roles laborales (ej.: cajero corresponsal, supervisor de operaciones, analista de riesgo, administrador de red) y se asignarán usuarios a estos perfiles en base a la necesidad de sus funciones (modelo **role-based access control, RBAC**). Se aplicará estrictamente el **principio de necesidad de saber**: por ejemplo, un usuario del área comercial no debería tener acceso a datos de la base de datos técnica de sistema, y un desarrollador no debería acceder a datos de producción sin supervisión. Cualquier **excepción o elevación temporal de privilegios** (por ejemplo, para tareas de soporte) deberá ser aprobada y registrada, y revocada inmediatamente tras cumplir su propósito. Los sistemas críticos registrarán en bitácora cada intento de acceso denegado y cada acceso a datos sensibles para posibilitar auditorías posteriores.
- **Revisiones periódicas de accesos:** Se realizarán **revisiones de permisos** de forma periódica (al menos semestralmente, y adicionalmente ante eventos relevantes como reorganizaciones internas). En estas revisiones, los propietarios de activos y los responsables de RR.HH. verificarán que cada usuario mantenga únicamente los accesos correspondientes a su cargo vigente. Cualquier cuenta huérfana (por ejemplo, de ex-empleados) o privilegio no justificado identificado deberá ser **revocado de inmediato**. Asimismo, existe un proceso establecido para la **revocación de accesos** cuando un empleado deja la compañía o cambia de rol: Recursos Humanos notificará al área de TI/Seguridad con antelación o inmediatamente, para que se deshabiliten sus cuentas, se recupere cualquier dispositivo corporativo y se rescindan sus accesos físicos (devolución de tarjetas de ingreso, llaves, etc.) en el momento oportuno, evitando accesos no autorizados posteriores.
- **Control de accesos físicos:** El acceso a las instalaciones de *Super Pagos* donde se encuentren recursos importantes (oficinas administrativas, centros de cómputo, archivos físicos) estará restringido. Se emplearán mecanismos como **tarjetas de**

proximidad o identificación biométrica para la entrada a áreas seguras, con registros de ingreso y salida de personal y visitantes. Las áreas especialmente sensibles (como el cuarto de servidores) solo podrán ser accedidas por personal de TI autorizado y personal de seguridad física, quedando registro de cada ingreso. Los visitantes o personal de mantenimiento externo deberán siempre estar **acompañados** por un empleado responsable durante su permanencia en zonas restringidas. Periódicamente se revisarán los permisos de acceso físico asignados (por ejemplo, las autorizaciones en el control de acceso de la oficina) para revocar aquellos innecesarios.

- **Seguridad en estaciones de trabajo y dispositivos móviles:** Los equipos de cómputo de los usuarios contarán con mecanismos de **autobloqueo de sesión** tras un período de inactividad breve, requiriendo reautenticación para reanudar su uso, de modo que se prevenga el acceso no supervisado. Se prohibirá la instalación de software no autorizado en las estaciones de trabajo y se restringirán los privilegios de administrador local para usuarios finales salvo justificación (lo que también es una medida de control de acceso a nivel de endpoint). Los dispositivos móviles con correo corporativo u otros datos de la empresa deberán estar protegidos con PIN/biometría y administrados mediante soluciones de **MDM (Mobile Device Management)** que permitan borrar datos en caso de extravío.
- **Principio de menor privilegio en redes y servicios:** No solo las personas, también los procesos y servicios seguirán el principio de menor privilegio. Las aplicaciones y servicios en la arquitectura de Refácil deben correr con **cuentas de servicio** que tengan los permisos mínimos requeridos. Por ejemplo, si una aplicación web necesita acceder a una base de datos, la cuenta utilizada tendrá solo privilegios de ejecutar los procedimientos requeridos, sin acceso ilimitado a todas las tablas. Igualmente, en la configuración de la red, los puertos, protocolos y servicios habilitados serán únicamente los necesarios; todo lo demás se mantendrá deshabilitado por defecto para reducir superficies de ataque.
- **Segregación de funciones:** En la medida de lo posible, se implementará la **separación de funciones (SoD)** para prevenir conflictos de interés o fraudes. Esto también es parte del control de accesos: por ejemplo, quien aprueba un pago no debe ser la misma persona que lo registra; en términos de sistemas, los roles que permiten operaciones críticas estarán segregados para que no recaigan en un mismo individuo sin controles compensatorios. Cualquier excepción deberá ser aprobada con controles adicionales (como doble revisión de transacciones).
- **Monitoreo y respuesta a accesos indebidos:** El área de Seguridad monitoreará los **logs de acceso** y eventos relevantes en sistemas clave. Intentos reiterados fallidos de autenticación, accesos fuera de horarios habituales, o acceso a volúmenes inusuales de datos sensibles generarán **alertas de seguridad** que serán investigadas de inmediato. En caso de detección de un acceso no autorizado o sospechoso, se activarán los protocolos de **respuesta a incidentes** para contener

la amenaza (por ejemplo, bloqueo de la cuenta comprometida, aislamiento de un equipo, etc.).

En resumen, el control de accesos en *Super Pagos S.A.S.* está diseñado para **garantizar que cada usuario tenga acceso únicamente a aquello que necesita y nada más**. Combinando políticas de identidad, autenticación fuerte, gestión cuidadosa de privilegios, revisiones regulares y monitoreo, la empresa mitigará el riesgo de accesos indebidos que pudieran derivar en filtraciones de información o uso malicioso de sus sistemas.

Formación y concienciación

La **formación y concienciación** en seguridad de la información es uno de los componentes críticos para el éxito del SGSI, dado que las personas suelen ser el eslabón más débil en la cadena de seguridad. *Super Pagos S.A.S.* se compromete a desarrollar un programa continuo de capacitación que promueva una **cultura de seguridad** en todos los niveles de la organización.

Las iniciativas y lineamientos en este aspecto incluyen:

- **Capacitación obligatoria para nuevos colaboradores:** Todo nuevo empleado, al momento de su inducción, recibirá una **formación inicial en seguridad de la información**. Esta formación cubrirá los aspectos básicos de la política de seguridad, las responsabilidades individuales, las mejores prácticas de manejo de información sensible, el uso seguro de contraseñas, el reconocimiento de correos electrónicos sospechosos (phishing) y demás temas relevantes al puesto. Ningún empleado debería empezar a manejar información crítica sin antes haber sido informado de las normas de seguridad que debe seguir. En el caso de contratistas o terceros con acceso a sistemas de la empresa, también deberán certificar que han recibido y entendido las políticas de seguridad pertinentes antes de acceder.
- **Capacitaciones periódicas y actualización de conocimientos:** La empresa realizará **entrenamientos y refrescos periódicos** en materia de seguridad, al menos **una vez al año** para todo el personal, y con mayor frecuencia o profundidad para aquellos roles con mayores privilegios o responsabilidades de seguridad (por ejemplo, administradores de sistemas, desarrolladores, personal de soporte). Estas capacitaciones anuales pueden adoptar la forma de cursos en línea, talleres presenciales, o una combinación, y su contenido se actualizará continuamente para incluir nuevas amenazas (p.ej. ingeniería social emergente, ransomware, etc.) y cambios en las políticas o procedimientos internos. La **formación constante del equipo ayuda a disminuir los errores humanos, que son una de las causas principales de incidentes de seguridad**; por tanto, *Super Pagos* enfocará la educación en prevenir esos errores comunes (como clicar enlaces maliciosos, usar

dispositivos no autorizados, compartir información confidencial inadvertidamente, etc.).

- **Campañas de concienciación y cultura organizacional:** Además de la formación formal, se implementarán **campañas de concienciación** continuas para mantener la atención del personal sobre la importancia de la seguridad. Esto puede incluir: boletines informativos mensuales con tips de seguridad, afiches en las oficinas con recordatorios (p. ej. "Bloquea tu equipo antes de ausentarte", "No compartas tu contraseña"), *infografías* o recursos visuales en la intranet corporativa, y eventos como *la Semana de la Seguridad de la Información* con charlas y actividades lúdicas que refuercen conceptos. También se podrían realizar **simulacros de phishing** periódicos (enviando correos señuelo al personal para probar su reacción) como herramienta pedagógica para mejorar la detección de correos fraudulentos y medir el nivel de conciencia. Cada campaña o acción estará respaldada por la Alta Dirección para darle visibilidad y demostrar que la seguridad es un valor corporativo.
- **Entrenamiento especializado según rol:** Para ciertas funciones, se proveerá capacitación especializada. Por ejemplo, el equipo de desarrollo recibirá entrenamiento en **desarrollo seguro de software** (OWASP, mitigación de vulnerabilidades comunes), el equipo de respuesta a incidentes será capacitado en **gestión de incidentes y forense digital**, el personal de atención al cliente será entrenado en **protección de la privacidad** y verificación de identidad al tratar con usuarios, etc. Asimismo, el Responsable de Seguridad y su equipo asistirán a cursos avanzados y mantendrán certificaciones profesionales pertinentes (CISSP, CISM, ISO 27001 Lead Implementer/Auditor, CEH, etc.) para asegurar que sus habilidades técnicas y de gestión estén actualizadas.
- **Evaluación de la eficacia:** La empresa medirá la efectividad de su programa de concienciación mediante diversos indicadores: por ejemplo, tasas de participación en los cursos (todos los empleados deben completar la capacitación anual obligatoria), evaluaciones cortas después de cada capacitación para comprobar la asimilación de conceptos, comparativa de resultados de simulacros (¿disminuye la cantidad de clics en correos de phishing de prueba a lo largo del tiempo?), y reducción en incidentes atribuibles a error humano. Estos resultados serán analizados en las reuniones del Comité de Seguridad para ajustar el enfoque de las capacitaciones según áreas de mayor debilidad detectadas.
- **Comunicación de políticas y actualizaciones:** Cada vez que se emita o actualice una política, procedimiento o instrucción relacionada con seguridad, se comunicará efectivamente a toda la organización. Esto puede ser mediante correo corporativo informativo, publicación en la intranet y, de ser un cambio de gran importancia, a través de sesiones explicativas virtuales o presenciales. El entendimiento y **aceptación formal** de las políticas por parte de los empleados podría ser requerido (por ejemplo, haciendo que firmen electrónicamente un acuse de recibo de la Política General de Seguridad y sus posteriores revisiones). De esta manera, se

asegura que todos estén al tanto de sus obligaciones y de cualquier cambio en las expectativas de seguridad.

En conclusión, *Super Pagos S.A.S.* reconoce que la tecnología por sí sola no es suficiente para garantizar la seguridad; se requiere un personal **consciente, informado y comprometido**. Mediante un robusto programa de formación y concienciación, la organización busca empoderar a sus colaboradores para actuar como la **primera línea de defensa** contra las amenazas a la información, creando un ambiente donde la seguridad sea parte integral del comportamiento cotidiano. La alta dirección apoyará consistentemente estas iniciativas, entendiendo que cada peso invertido en educación en seguridad se recupera con creces al evitar incidentes y fortalecer la resiliencia organizacional.

Control de terceros

Los **terceros** (proveedores, aliados comerciales, contratistas externos) que interactúan con *Super Pagos S.A.S.* pueden introducir riesgos de seguridad si no se gestionan adecuadamente. Por ello, la empresa implementará controles rigurosos para asegurar que dichos terceros mantengan **niveles de seguridad equivalentes** a los de la organización al manejar información o sistemas de *Super Pagos*. Los lineamientos claves en el control de terceros son:

- **Políticas de seguridad para terceros y acuerdos contractuales:** Antes de establecer una relación con cualquier tercero que pueda tener acceso a información sensible o sistemas críticos (por ejemplo, un proveedor de servicios en la nube, una empresa de desarrollo de software outsourcing, un aliado en la operación de pagos), *Super Pagos* evaluará las implicaciones de seguridad. Se incluirán en los **contratos cláusulas específicas** que obliguen al tercero a cumplir con las políticas de seguridad de la información de *Super Pagos* y con las leyes de protección de datos. Entre dichas cláusulas típicamente estarán: acuerdos de **confidencialidad (NDA)** para proteger la información compartida; requisitos de **implementación de controles** (p.ej., cifrado, controles de acceso, gestión de incidentes) alineados con nuestro SGSI; derecho de la empresa a **auditar o requerir evidencia** de los controles de seguridad del tercero; notificación obligatoria y oportuna por parte del tercero ante cualquier incidente de seguridad que afecte la información que maneja de *Super Pagos*; y, en su caso, acuerdos sobre **responsabilidad** en caso de brechas de seguridad atribuibles al tercero.
- **Evaluación y selección de proveedores seguros:** En la fase de selección de proveedores o socios críticos, se incorporarán **criterios de seguridad**. Por ejemplo, se puede exigir a proveedores de tecnología que demuestren certificaciones o marcos de seguridad (ISO 27001, SOC 2, PCI DSS si corresponde, etc.), o se les

hará **cuestionarios de seguridad** para entender su postura (cantidad de personal dedicado a seguridad, uso de cifrado, historiales de incidentes, continuidad del negocio, localización de datos, subcontratistas, etc.). *Super Pagos* preferirá trabajar con aquellos terceros que puedan evidenciar una sólida cultura de seguridad. En caso de proveedores que manejen datos personales en nombre de la empresa (Encargados del Tratamiento, según Ley 1581), se verificará que cumplan con estándares de protección de datos similares, y se registrarán esos contratos en las bases de datos si es menester.

- **Control durante la relación con terceros:** Una vez contratado el tercero, *Super Pagos* aplicará un **seguimiento activo** a su cumplimiento en seguridad. Esto puede implicar: solicitar **reportes periódicos** de cumplimiento (ej., reporte anual de vulnerabilidades corregidas, evidencias de backup de la información de *Super Pagos* que hospedan, resultados de pruebas de penetración si las hicieron); realizar **reuniones de servicio** donde además de nivel de servicio (SLA) se discuta la seguridad (por ejemplo, incluir KPIs de seguridad en los comités de seguimiento con proveedores críticos); y eventualmente, llevar a cabo **auditorías o visitas in situ** cuando sea justificable (especialmente para proveedores que procesan información altamente sensible). Si un tercero sufre un incidente de seguridad que afecte a *Super Pagos*, la empresa analizará conjuntamente las causas e implementará medidas para evitar recurrencia, pudiendo exigir planes de remediación al proveedor.
- **Acceso de terceros a los sistemas:** En casos donde personal de un tercero requiera acceso a los sistemas de información corporativos (p. ej., un técnico de soporte del proveedor, consultores, auditores externos), se controlará estrictamente dicho acceso. Se seguirán los mismos principios de **mínimo privilegio** y control de cuentas: se crearán cuentas temporales o restringidas si es posible, que serán deshabilitadas al terminar el trabajo; se supervisarán las actividades realizadas (monitoreo o logging especial durante la ventana de acceso); y siempre que sea viable, esas tareas de terceros se harán **bajo supervisión** de personal interno. No se permitirá a terceros conectar dispositivos no autorizados en la red interna sin validación previa. Los acuerdos de conexión remota y entrega de herramientas diagnósticas se revisarán para que no introduzcan vulnerabilidades.
- **Seguridad en la cadena de suministro:** *Super Pagos* reconocerá que algunos terceros a su vez contratan sub-proveedores, lo que extiende la cadena de suministro. Por tanto, se procurará que en los contratos principales quede reflejado que el tercero **fluya las obligaciones de seguridad** hacia cualquier subcontratista que participe en el servicio. Por ejemplo, si *Super Pagos* contrata un servicio en la nube, y ese proveedor usa a su vez un proveedor de datacenter, el contrato principal debe exigir la seguridad en ambos niveles. La empresa se mantendrá informada sobre cambios relevantes del tercero (fusiones, brechas públicas, cambios de localización de datos) para valorar cualquier nuevo riesgo.

- **Terminación de la relación:** Al finalizar la relación con un tercero, *Super Pagos* se asegurará de **revocar todos los accesos** que dicho tercero tuviera (cuentas de usuario, llaves, VPN, etc.), y de que retorne o destruya de manera segura cualquier información confidencial de *Super Pagos* bajo su custodia. Estas condiciones estarán estipuladas en el contrato (incluyendo certificación de destrucción de datos si aplica). La no observancia de este proceso podría dejar brechas, por lo que se le dará seguimiento riguroso en la lista de verificación de terminación de contratos.

Con estas medidas, *Super Pagos S.A.S.* busca que la participación de terceros en sus operaciones **no debilite su postura de seguridad**, sino que por el contrario estos aliados sumen a la fiabilidad general del servicio. En el sector Fintech especialmente, los socios (como redes de pago, corresponsales bancarios, integradores) **esperan altos estándares de seguridad** de parte de todos los involucrados, y la confianza mutua es clave para habilitar negocios. La empresa comprende que un fallo de seguridad en un proveedor puede repercutir en su propia reputación y continuidad, por lo que extiende su gestión de seguridad más allá de los límites organizacionales, abarcando la **seguridad de la cadena de valor**. De esta forma, se minimizan riesgos sistémicos y se cumple también con expectativas regulatorias de supervisar a los terceros relevantes (tal como lo requieren entes como la Superfinanciera en sus guías de tercerización). En conclusión, ningún tercero tendrá acceso a la información o sistemas de *Super Pagos* sin antes adherirse a estrictos controles y compromisos de seguridad equivalentes a los de la organización.

Gestión de incidentes de seguridad

A pesar de todas las medidas preventivas, es posible que ocurran **incidentes de seguridad de la información**. La capacidad de *Super Pagos S.A.S.* para responder rápida y eficazmente a estos incidentes es fundamental para mitigar su impacto. Por ello, la empresa establece un **proceso formal de gestión de incidentes de seguridad** que incluye la preparación, detección, contención, erradicación, recuperación y aprendizaje posterior a cada incidente.

Los puntos clave de este proceso son:

- **Definición de incidente de seguridad:** Se considerará *incidente de seguridad de la información* a cualquier evento que comprometa o amenace la **confidencialidad, integridad o disponibilidad** de los activos de información, así como el cumplimiento de los requisitos legales y las políticas de la organización. Esto abarca, entre otros, accesos no autorizados a sistemas o datos, sospechas de brecha de datos personales, malware detectado en equipos, denegaciones de servicio que afecten la plataforma, pérdida o robo de dispositivos corporativos, errores humanos que expongan información sensible, o el incumplimiento deliberado de políticas de

seguridad. También se incluyen *incidentes de seguridad física* que puedan afectar a la información (ej.: intrusión en áreas restringidas, robo de documentos).

- **Canales de reporte y detección:** *Super Pagos* implementará mecanismos fáciles y confidenciales para que los empleados y terceros puedan **reportar incidentes o eventos sospechosos** de seguridad. Se dispondrá de un correo electrónico específico (ej. *seguridad@empresa.com*), una línea telefónica de emergencias de TI, y/o una herramienta de gestión de tickets donde se puedan notificar incidentes 24/7. Todos los colaboradores tienen la responsabilidad de **reportar inmediatamente** cualquier indicio de incidente, sin importar cuán pequeño parezca (por ejemplo, un correo de phishing recibido, un dispositivo extraviado, un comportamiento extraño en un sistema). Adicionalmente, se contará con sistemas automáticos de **detección**: herramientas de monitoreo (SIEM) que correlacionen eventos, antivirus que alerten sobre infecciones, sistemas IDS/IPS, etc., para identificar eventos en tiempo real.
- **Respuesta inicial y clasificación:** Al recibir un reporte de incidente, el **Equipo de Respuesta a Incidentes** (dirigido por el Responsable de Seguridad, e involucrando a personal de TI y otras áreas según el caso) realizará una **evaluación inicial** para clasificar el incidente según su severidad y alcance. Esta clasificación (por ejemplo: Crítico, Alto, Medio, Bajo) considerará factores como el tipo de activo afectado, cantidad de datos comprometidos, impacto en el servicio (¿hay caída del sistema?), impacto regulatorio (¿hay que notificar a clientes o autoridades?), etc. Por ejemplo, la detección de un **ransomware** activo en servidores nucleares se clasificaría como incidente Crítico dado que puede paralizar operaciones, mientras que un virus aislado en la PC de un usuario podría ser Medio si se contiene a tiempo. Esta priorización guiará los recursos y urgencia en la respuesta.
- **Contención y erradicación:** Ante un incidente confirmado, el primer objetivo es **contener** el daño para que no siga propagándose o empeorando. Dependiendo del tipo de incidente, las acciones de contención pueden incluir: aislar redes o sistemas comprometidos (desconectarlos de la red), revocar accesos o cuentas afectadas (por ej., si se sospecha de credenciales comprometidas), aplicar parches temporales o reglas de firewall para bloquear una entrada explotada, etc. Una vez contenido, se procederá a la **investigación técnica** para entender la causa raíz y el alcance completo: se recolectarán evidencias (logs de servidores, copias de malware, timestamp de modificaciones), se analizará cómo ocurrió el incidente (vector de ataque) y qué activos fueron afectados. Con esa información, se realizarán acciones de **erradicación**, que implican eliminar la amenaza del entorno (por ejemplo, limpiar malware de todos los equipos infectados, cerrar brechas de seguridad explotadas, cambiar contraseñas comprometidas, eliminar cuentas maliciosas). *Super Pagos* podría recurrir a expertos externos en forense digital si el incidente lo amerita, para asegurar una remediación completa. Durante todo el proceso, se cuidará mantener

evidencias forenses válidas en caso de que sean requeridas para denuncias o acciones legales posteriores (cadena de custodia, copias de evidencia).

- **Recuperación y restauración de servicios:** Tras la erradicación de la causa, se trabajará en restaurar la normalidad de las operaciones. Esto incluye **recuperar datos desde respaldos** si hubo pérdida o alteración, reconstruir sistemas desde cero si fueron comprometidos en su integridad (ej. reinstalar un servidor), y verificar minuciosamente que los sistemas restaurados estén libres de la vulnerabilidad o malware original. Se comunicará internamente (y eventualmente externamente) cuándo un servicio afectado ha sido restaurado y qué medidas se tomaron. Se monitoreará más de cerca en el corto plazo el sistema recuperado para detectar cualquier signo de persistencia de la amenaza. El objetivo es volver al estado operativo lo antes posible, minimizando el downtime y el impacto en clientes; por ejemplo, si la plataforma Refácil sufrió una interrupción, la meta es restablecerla cumpliendo con los RTO definidos en la estrategia de continuidad. Durante esta fase también se considerará si es necesario notificar a **clientes u otros stakeholders**: por obligaciones legales, *Super Pagos* informará a los titulares de datos si su información pudo verse comprometida, de acuerdo a las guías de la SIC, y/o notificará a la Superintendencia Financiera si un incidente relevante pudo afectar la estabilidad del servicio financiero ofrecido.
- **Notificación a autoridades y comunicación:** En ciertos casos, *Super Pagos* deberá **notificar incidentes** a entidades externas. Por ejemplo, si ocurriera una fuga masiva de datos personales, se evaluará la notificación a la Superintendencia de Industria y Comercio y a los titulares afectados, siguiendo lo dispuesto en la regulación de datos personales. Si el incidente involucra posibles delitos informáticos (intrusiones deliberadas, fraudes), se presentará la **denuncia ante la autoridad competente** (Fiscalía) aportando evidencia para apoyar la investigación penal, en cumplimiento de la Ley 1273. A socios comerciales relevantes (bancos aliados, etc.) también se les informará oportunamente si sus intereses pudieran estar afectados (por ejemplo, si claves de API compartidas se ven comprometidas). En cuanto a comunicación, la empresa designará voceros oficiales (usualmente el área de Comunicaciones o el gerente general con apoyo de seguridad) para manejar la **comunicación pública** sobre incidentes, en caso de ser necesario, asegurando transparencia y control del mensaje para proteger la reputación de la compañía.
- **Lecciones aprendidas y mejoras:** Una vez resuelto el incidente y retomada la normalidad, el equipo de respuesta, junto con las partes involucradas, llevará a cabo una **reunión de revisión post-incidente**. El propósito es analizar qué sucedió, qué se hizo bien, qué falló o pudo mejorarse en la respuesta, y lo más importante: identificar **acciones de mejora** para evitar incidentes similares en el futuro. Esto puede llevar a: ajustar o crear nuevos controles (p. ej., si el incidente fue un phishing exitoso, reforzar las capacitaciones o implementar autenticación más fuerte; si fue una intrusión por parche faltante, mejorar el proceso de gestión de parches),

actualizar procedimientos de respuesta (mejorar checklists, contactos de emergencia), o incluso reconsiderar la evaluación de ciertos riesgos. Estas lecciones se documentarán en un **informe de incidente** completo, que incluirá la cronología de eventos, el impacto, las medidas tomadas y las recomendaciones. Dicho informe será presentado a la Alta Dirección y alimentará la **mejora continua del SGSI**.

Todo el personal será consciente de este proceso y de su rol en él (por ejemplo, saber a quién llamar y qué hacer inmediatamente ante una computadora potencialmente infectada, o cómo reconocer y reportar un intento de ingeniería social). La rápida escalación y respuesta puede marcar la diferencia para contener un incidente antes de que cause daños mayores.

Cabe resaltar que la organización probará periódicamente sus capacidades de respuesta (por ejemplo, realizando simulacros de incidentes, *table-top exercises*, escenarios de ciberataque controlados) para validar que los **protocolos de incidentes** funcionan en la práctica y que los equipos están familiarizados con ellos. Estas pruebas ayudarán a afinar la coordinación entre las diferentes áreas (TI, Legal, Comunicaciones, Dirección) bajo situaciones de estrés simulado, de modo que ante un incidente real se actúe con rapidez y efectividad.

En síntesis, *Super Pagos S.A.S.* adopta una postura de **preparación y resiliencia** ante incidentes: asume que pueden ocurrir fallos o ataques, y por tanto desarrolla la capacidad interna no solo de prevenir, sino de **detectar y reaccionar** adecuadamente. Esto minimizará el impacto financiero, operativo y reputacional de los incidentes que eventualmente se presenten, protegiendo en última instancia a nuestros clientes, la continuidad del servicio y los intereses de la organización.

Mejora continua

La seguridad de la información es un proceso dinámico, por lo que *Super Pagos S.A.S.* establece el compromiso de la **mejora continua** en todos los aspectos de su SGSI. Esto significa que la empresa evaluará y perfeccionará regularmente sus políticas, controles y procedimientos de seguridad, con el fin de adaptarse a las nuevas amenazas, corregir debilidades identificadas y alinearse con cambios en el entorno de negocio o regulatorio.

Los mecanismos para impulsar la mejora continua incluyen:

- **Revisiones periódicas del SGSI:** La Alta Dirección, en conjunto con el Responsable de Seguridad, llevará a cabo al menos una **Revisión Gerencial anual** del Sistema de Gestión de Seguridad de la Información. En dicha revisión se

considerarán: los resultados de las auditorías internas y/o externas realizadas, el estado de cumplimiento de objetivos de seguridad, los informes de incidentes ocurridos y sus lecciones aprendidas, las evaluaciones de riesgos recientes, el estado de los planes de tratamiento de riesgos, retroalimentación de partes interesadas (clientes, reguladores, personal), y las recomendaciones de mejora propuestas. A partir de este análisis global, la dirección emitirá **directrices para mejora** y asignará recursos para implementarlas, ajustando si es necesario la política, los objetivos o cualquier parte del SGSI para el siguiente ciclo. Este ciclo de revisión se alinea con la filosofía **PDCA (Plan-Do-Check-Act)** promovida por ISO 27001, asegurando la retroalimentación formal a nivel gerencial.

- **Auditorías internas y externas:** Se planificarán **auditorías internas** de seguridad de la información con una periodicidad definida (por ejemplo, semestral o anual), en las cuales auditores internos o personal independiente evaluará objetivamente el cumplimiento de las políticas, la efectividad de los controles implementados y el grado de conformidad con ISO 27001. Las no conformidades o hallazgos identificados en estas auditorías serán documentados y seguidos mediante acciones correctivas concretas. Adicionalmente, con miras a la certificación ISO 27001, *Super Pagos* se someterá a **auditorías externas** por parte de un organismo de certificación acreditado, que validará la conformidad del SGSI con la norma. Los informes de auditoría externa igualmente pueden traer observaciones u oportunidades de mejora que la empresa incorporará en sus planes.
- **Monitoreo de indicadores de seguridad (KPI/KRI):** Se establecerán **indicadores clave de desempeño** (KPI) y de riesgo (KRI) para la función de seguridad, los cuales serán medidos y reportados periódicamente. Ejemplos de estos indicadores pueden ser: número de incidentes de seguridad ocurridos por mes y su severidad, tiempos de respuesta promedio a incidentes, porcentaje de personal capacitado en seguridad al año, porcentaje de cumplimiento de parches críticos aplicados en tiempo objetivo, resultados de evaluaciones de phishing (tasa de clics), entre otros. Un análisis de tendencias de estos indicadores permitirá identificar áreas donde se esté mejorando o empeorando. Por ejemplo, si se observa una disminución consistente en incidentes derivados de errores humanos después de ciertas capacitaciones, esto refuerza la efectividad de esas acciones; por el contrario, un incremento en incidentes de malware podría disparar una revisión de los controles antivirus o políticas de acceso a webs. Los **KRI** (indicadores de riesgo) también avisarán si algún riesgo está aumentando (por ejemplo, número de vulnerabilidades críticas detectadas en scanners que no se corrigen en X días). Esta cultura de métricas soporta la mejora continúa basada en datos objetivos.
- **Gestión de cambios en el entorno:** La empresa dará seguimiento a los **cambios externos** que puedan requerir ajustes en la seguridad. Esto abarca mantenerse al día con boletines de vulnerabilidades y nuevas amenazas (ciberinteligencia), vigilar cambios regulatorios (nuevas leyes, guías de entes supervisores) y también la

evolución del propio negocio (por ejemplo, lanzamiento de nuevos servicios Fintech, expansión a nuevas regiones) para analizar su impacto en el SGSI. Cuando haya cambios significativos (tecnologías emergentes adoptadas, reestructuración interna, integraciones con terceros, etc.), se revisarán las evaluaciones de riesgo pertinentes y se actualizarán o crearán controles según se requiera. Se fomenta una mentalidad de **"siempre alerta"**: no asumir que el estado actual de seguridad es suficiente, sino cuestionarlo frente a cada cambio y mejorar proactivamente.

- **Acciones correctivas y preventivas:** Cualquier desviación encontrada (incidente, auditoría, indicador fuera de umbral) generará la apertura de **acciones correctivas** dentro del SGSI. Estas acciones se registrarán y realizarán seguimiento hasta su cierre, verificando que efectivamente resuelven la causa raíz del problema identificado. De igual forma, la organización promueve la identificación de **acciones preventivas** cuando se detecten áreas de mejora antes de que ocurra un problema (por ejemplo, notando que un proceso es demasiado manual y propenso a error, se automatiza antes de que cause un incidente). Toda mejora implementada se documentará (actualizando políticas, procedimientos o configuraciones) y se comunicará a quienes corresponda.
- **Fomento de la innovación en seguridad:** Así como la empresa innova en sus productos Fintech, también se buscará innovar en las prácticas de seguridad. Se evaluará la adopción de nuevas herramientas o enfoques que puedan fortalecer el SGSI (por ejemplo, soluciones de *machine learning* para detección de anomalías, tecnologías de *Zero Trust*, etc.), siempre analizando costo-beneficio y madurez de las mismas. Se motivará al equipo de seguridad y TI a mantenerse actualizados profesionalmente y a traer ideas frescas que puedan traducirse en mejoras. La Alta Dirección apoya la mejora continúa entendiendo que un SGSI estancado equivale a exponerse a riesgos crecientes, mientras que un SGSI en evolución constante es un factor diferenciador y de confianza para la empresa.

En conclusión, *Super Pagos S.A.S.* asegura que su Política y el SGSI no sean estáticos, sino que **evolucionen constantemente**. La **mejora continua** garantiza que la organización no solo reaccione a los problemas, sino que aprenda de ellos y se adelante a futuros desafíos. Este compromiso queda formalizado y respaldado al más alto nivel, permeando en todos los procesos de seguridad. De esta manera, la política de seguridad seguirá siendo efectiva y relevante con el paso del tiempo, contribuyendo a la resiliencia y excelencia operacional de la empresa.

Periodicidad de revisión de la política

Esta **Política General de Seguridad de la Información** será **revisada regularmente** para asegurar que se mantiene adecuada a la realidad de la organización, de la tecnología y de las amenazas emergentes. Como lineamiento general, la política se revisará **al menos una**

vez al año. La revisión estará coordinada por el Responsable de Seguridad de la Información (CISO) con la participación del Comité de Seguridad y deberá ser **aprobada por la Alta Dirección** en cada ciclo de actualización.

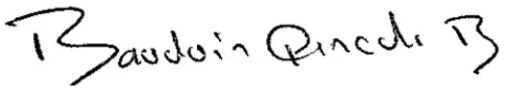
No obstante, la política podrá ser revisada y actualizada **antes del periodo anual** si ocurren cambios significativos que así lo ameriten, tales como: cambios sustanciales en la estructura organizacional o en los procesos de negocio, introducción de nuevas tecnologías o modificaciones importantes en la arquitectura de TI, detección de vulnerabilidades graves o incidentes de seguridad relevantes que revelen brechas en la política actual, cambios en la legislación o regulaciones aplicables (por ejemplo, una nueva ley de ciberseguridad, disposiciones de la Superfinanciera, etc.), o cualquier otro cambio en las circunstancias que pudiera afectar los supuestos bajo los cuales fue emitida la versión vigente de la política.

El procedimiento de revisión incluirá:

- **Evaluación de adecuación:** Verificar si los objetivos, alcance, principios y controles contemplados en la política siguen siendo pertinentes y efectivos para la situación actual de *Super Pagos*. Esto podría incluir recoger retroalimentación de los usuarios de la política (empleados, auditores) sobre dificultades de comprensión o aplicación, y considerar las lecciones aprendidas de auditorías e incidentes.
- **Actualización del contenido:** Modificar, adicionar o eliminar apartados de la política conforme a la evaluación anterior. Cualquier cambio propuesto será documentado con su justificación. Por ejemplo, podría incorporarse un nuevo principio rector si la empresa decide enfatizarlo, o actualizar la sección de cumplimiento legal si surgió una nueva regulación, etc. Se procurará mantener la coherencia y evitar contradicciones con otras políticas o procedimientos derivados.
- **Aprobación formal:** Todo cambio en la política deberá ser **validado por la Alta Dirección** (Gerencia General y otras autoridades designadas). La versión revisada se considerará oficial solo una vez que conste su aprobación en acta o firma competente. Cada versión tendrá un **código de versión y fecha de aprobación** para control.
- **Comunicación de cambios:** Tras la aprobación, la nueva versión de la política será **comunicada a toda la organización** y, de ser necesario, a terceros pertinentes. Se pondrá a disposición en los repositorios internos (intranet, manuales) indicando claramente que reemplaza a la versión anterior. Si los cambios son sustanciales, se realizarán sesiones de socialización o capacitaciones específicas para explicar las novedades y garantizar su entendimiento y adopción.

La versión anterior de la política será archivada para historial, pero quedará **obsoleta** una vez entre en vigencia la nueva. La vigencia de la política actual se mantendrá hasta que una nueva versión sea oficialmente aprobada y comunicada.

Super Pagos S.A.S. garantiza que esta política no sea un documento estático, sino un instrumento **vivo**, que **se revisa y evoluciona periódicamente** conforme cambian las necesidades estratégicas, los riesgos y el entorno operacional de la empresa. La periodicidad mínima anual de revisión asegura un balance entre estabilidad y actualización, mientras que la posibilidad de revisiones ad-hoc ante cambios importantes brinda la flexibilidad necesaria para que la política siga siendo eficaz y relevante en todo momento. La Alta Dirección ratifica con ello su compromiso de mantener una política siempre alineada con las mejores prácticas y requerimientos vigentes, y de sustentar con ella un SGSI confiable y actualizado.



BAUDOIN PINEDA BENITEZ
CEO