Política de Seguridad Cibernética

Preparado por el equipo legal de FacilitaPay en mayo de 2023.

1. OBJETIVO

Establecer los principios, lineamientos y atribuciones relacionados con la seguridad de la información, protegiendo la información de la institución, clientes y público en general, observando las mejores prácticas del mercado y normatividad aplicable.

2. PÚBLICO OBJETIVO

Empleados del Grupo FacilitaPay ("FacilitaPay"), independientemente del país en el que se encuentren. Los empleados son:
• Socios y accionistas • Directores • Empleados • Pasantes • Aprendices menores • Clientes y/o personas físicas/jurídicas que tienen una relación comercial con FacilitaPay.

3. INTRODUCCIÓN

La información es uno de los principales activos de la institución. Así, FacilitaPay define la estrategia de Seguridad de la Información y Seguridad Cibernética para proteger la integridad, disponibilidad y confidencialidad de la información. Esta estrategia se basa en la detección, prevención, monitoreo y respuesta de incidentes y fortalece la gestión de riesgos de ciberseguridad y la construcción de una base sólida para el futuro cada vez más digital de FacilitaPay.

Para lograr este objetivo, utilizamos la estrategia de protección perimetral ampliada. Este concepto considera que la información debe protegerse independientemente de dónde se encuentre, ya sea internamente, en una filial, en un proveedor de servicios o en una unidad internacional, a lo largo de su ciclo de vida, desde la recopilación hasta la eliminación.

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Nuestro compromiso con el tratamiento adecuado de la información de FacilitaPay, los clientes y el público en general se basa en los siguientes principios:

• Confidencialidad: garantizar que el acceso a la información sea obtenido únicamente por personas autorizadas;
• Disponibilidad: garantizar que las personas autorizadas tengan acceso a la información siempre que sea necesario;
• Integridad: garantizar la exactitud e integridad de la información y los métodos de su procesamiento, así como la transparencia en el trato con los públicos involucrados.

5. DIRECTRICES

Todas las políticas de seguridad de la información deben estar disponibles en un lugar accesible para los empleados y protegido de cambios. Las políticas de seguridad de la información son revisadas anualmente por FacilitaPay con aplicación en Brasil y en el extranjero.

La inclusión de lineamientos o excepciones por requerimiento reglamentario y la publicación en las unidades en el exterior, serán identificadas por el responsable de seguridad de la información de la unidad, quien deberá formalizar y presentar previamente la propuesta de lineamientos o excepciones para su aprobación por el Consejo de Seguridad Corporativa.

El cumplimiento de esta Política y cualquier desviación, en Brasil y en unidades en el extranjero, son reportadas periódicamente por el Departamento de Seguridad Corporativa al Comité Ejecutivo, Comité de Cumplimiento y otros comités de riesgos.

La información debe ser utilizada de manera transparente, para los fines informados al cliente y de acuerdo con la legislación vigente. Las directrices y las eventuales excepciones se complementan en procedimientos con normas específicas que deben observarse.

6. PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

Para garantizar la adecuada protección de la información tratada, FacilitaPay adopta los siguientes procesos:

a) Gestión de activos

Se entiende por activo todo aquello que la institución considere relevante para el negocio, desde activos tecnológicos (por ejemplo, software y hardware) hasta activos no tecnológicos (por ejemplo, personas, procesos y dependencias físicas) siempre que relacionados con la protección de la información. Los activos, de acuerdo con su criticidad, deben ser identificados, inventariados, mantenidos actualizados, tener un propietario, disponer de forma segura y estar protegidos contra accesos indebidos. La protección puede ser tanto física (por ejemplo, salas de acceso controlado) como lógica (por ejemplo, configuración de blindaje o endurecimiento, administración de parches, autenticación y autorización). Los activos de FacilitaPay, los clientes y el público en general deben ser tratados de manera ética y confidencial y de acuerdo con las leyes vigentes y las regulaciones internas, promoviendo el uso adecuado y evitando la exposición indebida de la información.

b) Clasificación de la información

La información debe clasificarse de acuerdo con la confidencialidad, de acuerdo con las políticas internas. Para ello, se deben considerar las necesidades relacionadas con el negocio, el intercambio o restricción de acceso y los impactos en caso de mal uso de la información. De acuerdo con la clasificación de confidencialidad, se deben establecer las protecciones necesarias a lo largo de su ciclo de vida. El ciclo de vida de la información comprende: Generación, Manejo, Almacenamiento, Transporte y Eliminación.

c) Gestión de accesos

Las subvenciones, revisiones y eliminaciones de acceso deben utilizar las herramientas y procesos corporativos de FacilitaPay. Los accesos deben ser rastreables para permitir la identificación individual del empleado o proveedor de servicios que ha accedido o cambiado la información, permitiendo su responsabilidad. La concesión de acceso debe cumplir con el criterio de privilegio mínimo, en el que los usuarios deben tener acceso únicamente a los recursos de información esenciales para el pleno desempeño de sus actividades y debidamente autorizados. La segregación de funciones debe impregnar

todos los procesos críticos, evitando que una sola persona a cargo pueda ejecutar y controlar el proceso a lo largo de su ciclo de vida. La identificación de cualquier empleado debe ser única, personal e intransferible, calificándolo como responsable de las acciones realizadas. La contraseña es información confidencial, personal e intransferible, debe ser utilizada como firma electrónica, y su intercambio está prohibido.

d) Gestión de riesgos

Los riesgos deben identificarse a través de un proceso establecido para analizar amenazas, vulnerabilidades, probabilidades e impactos en los de FacilitaPay, de modo que se recomienden protecciones adecuadas. Las recomendaciones se debaten en los foros apropiados. Los productos, procesos y tecnologías deben tener la gestión adecuada de los riesgos de Seguridad de la Información, para reducir los riesgos a niveles aceptables, independientemente si están dentro de la infraestructura de FacilitaPay, socios o proveedores de servicios. Las tecnologías en uso por la institución deben estar en versiones soportadas por sus fabricantes y debidamente actualizadas. Cualquier excepción debe ser aprobada por la autoridad competente o tener controles compensatorios.

e) Gestión de riesgos en proveedores de servicios y socios

Los proveedores de servicios y socios contratados por FacilitaPay deben clasificarse considerando algunos criterios, según el documento interno. Dependiendo de la clasificación, el proveedor de servicios o socio se someterá a una evaluación de riesgos, que puede incluir la validación in loco de los controles de SI, la evaluación remota de la evidencia o otras evaluaciones, así como la supervisión de cualquier corrección y mejora implementada por los proveedores de servicios y socios. Los proveedores de servicios y socios deben informar los incidentes relevantes (como se define en el punto 6.f de este Manual) relacionados con la información de FacilitaPay almacenada o procesada por ellos de conformidad con las determinaciones legales y reglamentarias.

f) Tratamiento de incidentes de seguridad de la información y ciberseguridad

El área de Ciberseguridad monitorea la seguridad del entorno tecnológico de FacilitaPay, analizando eventos y alertas para identificar posibles incidentes. Los incidentes que son identificados por las alertas se clasifican con respecto al impacto, de acuerdo con los criterios adoptados por FacilitaPay. Por su grado de relevancia se considerarán aspectos

como el impacto en el sistema financiero y el compromiso de los datos de los clientes y del público en general. Las incidencias clasificadas como relevantes deberán ser reportadas al Regulador, al interesado y al Comité de Cumplimiento, cuando involucren datos personales que puedan implicar riesgo o causar daños materiales a los titulares. Todas las incidencias pasan por un proceso de tratamiento y comunicación, donde se registra toda la información pertinente a las incidencias como causa, impacto, clasificación, etc.

La información sobre incidentes que puedan afectar a las instituciones financieras en Brasil debe compartirse con otras instituciones, con el fin de colaborar con la mitigación de riesgos de acuerdo con las determinaciones legales y regulatorias. En el exterior, la gestión de la seguridad de la información y los incidentes cibernéticos es realizada por la Unidad Internacional, que debe informarlos oportunamente a la Dirección de Seguridad Corporativa en Brasil.

El área de Riesgos elaborará un Informe Anual que contenga los incidentes relevantes ocurridos en el período, las acciones tomadas para prevenir y responder a los incidentes y los resultados de las pruebas de continuidad. Este informe será presentado al Comité de Riesgos y al Consejo de Administración, de acuerdo con las determinaciones legales y reglamentarias. Con el fin de mejorar la capacidad de respuesta a incidentes, FacilitaPay realiza pruebas de continuidad del negocio simulando escenarios de incidentes críticos de Ciberseguridad, que pueden comprometer la disponibilidad y/o confidencialidad de la información. Cada empleado debe ser proactivo y diligente en la identificación, comunicación con el área de Seguridad de la Información y mitigación de riesgos relacionados con la seguridad de la información.

g) Seguridad de la información y conciencia de seguridad cibernética

FacilitaPay promueve la difusión de los principios y directrices de Seguridad de la Información a través de programas de sensibilización y capacitación para fortalecer la cultura de Seguridad de la Información. Periódicamente, se ponen a disposición campañas de sensibilización o capacitación que pueden ser presenciales o online, relacionadas con la confidencialidad, integridad y disponibilidad de la información. Estas campañas se transmiten a través de correos electrónicos, portal corporativo, e-learning, medios de comunicación o redes sociales a empleados y clientes.

h) Gobernanza con las Áreas de Negocio y Tecnología

Las iniciativas y proyectos de las áreas de negocio y tecnología deben estar alineados con los principios y lineamientos de seguridad de la información.

i) Seguridad física del medio ambiente

El proceso de Seguridad Física establece controles relacionados con la concesión de acceso físico a los ambientes, de acuerdo con la criticidad de la información manejada en estos ambientes, según lo descrito en documentos internos.

j) Seguridad en el desarrollo de sistemas de aplicación

El proceso de desarrollo de sistemas debe garantizar el cumplimiento de los documentos internos y las buenas prácticas de seguridad de la institución. Los entornos productivos deben estar separados de otros entornos y con acceso solo a través de la aplicación por usuarios previamente autorizados o herramientas aprobadas.

k) Registro de grabación

Es obligatorio registrar registros o pistas de auditoría del entorno informático, para todas las plataformas, con el fin de identificar: quién realizó el acceso, cuándo se realizó el acceso, a qué se accedió y cómo se accedió. Esta información debe estar protegida contra modificaciones y accesos no autorizados.

l) Programa de Cyber Security

El Programa de Seguridad Cibernética de FacilitaPay se guía por los siguientes principios: • Normativa vigente; • Mejores prácticas; • Escenarios mundiales; • Análisis de riesgos de la propia institución.

Según su criticidad, las acciones del programa se dividen en:

• Críticas: Consiste en correcciones de emergencia e inmediatas para mitigar riesgos inminentes; • Apoyo: Iniciativas a corto/mediano plazo para mitigar el riesgo en el entorno actual, manteniendo el ambiente seguro, respetando el apetito de riesgo de la institución y permitiendo llevar a cabo acciones de largo plazo/estructuración; • Estructuración: Iniciativas a medio/largo plazo que abordan la causa raíz de los riesgos y preparan a la empresa para el futuro.

m) Protección perimetral

Para proteger la infraestructura de FacilitaPay contra un ataque externo, utilizamos, como mínimo, herramientas y controles contra: DDoS, Spam, Phishing, ataques APT/Malware, intrusión de dispositivos y servidores de red, ataques a aplicaciones y escaneo externo. Para mitigar el riesgo de fuga de información utilizamos herramientas preventivas instaladas en dispositivos móviles, estaciones de trabajo, en el servicio de correo electrónico, en el servicio de navegación web, en el servicio de impresión, además del uso de cifrado para datos en reposo y en transporte. Con el fin de aumentar la protección, no se permite la conexión física o lógica a la red corporativa de la institución por equipos privados no administrados o no aprobados.

n) Gobernanza con unidades internacionales

Las unidades internacionales deben contar con un oficial de seguridad de la información, independiente de las áreas de negocios y tecnología, que reporta al Departamento de Seguridad Corporativa.

6.1 Propiedad intelectual

La propiedad intelectual es la protección que recae sobre bienes intangibles, tales como: marcas, signos distintivos, eslogan publicitarios, nombres de dominio, nombres comerciales, indicaciones geográficas, diseños industriales, patentes de invención y modelos de utilidad, obras intelectuales (tales como obras literarias, artísticas y científicas, bases de datos, fotografías, dibujos, ilustraciones, proyectos arquitectónicos, obras musicales, obras audiovisuales, textos, etc.), programas informáticos y secretos comerciales (incluidos los secretos comerciales y de la industria). Todas y cada una de las invenciones, creaciones, trabajos y mejoras que han sido o serán creadas o realizadas por el empleado a FacilitaPay, en calidad de administrador, empleado y / o pasante, durante todo el término del mandato del empleado, contrato de trabajo o contrato de pasantía, pertenecen exclusivamente a FacilitaPay. Cualquier información y contenido cuya propiedad intelectual pertenezca a FacilitaPay, o haya sido puesta a disposición por ella, incluyendo información y contenido que haya sido obtenido, inferido o desarrollado por el propio empleado en su entorno de trabajo o utilizando recursos de la empresa no será utilizado para fines privados, ni transmitido a terceros, sin autorización previa y expresa de FacilitaPay. Es deber de todos los empleados garantizar la protección de la propiedad intelectual de FacilitaPay.

6.2 Declaración de responsabilidad

Periódicamente los empleados de FacilitaPay deben adherirse formalmente a un término, comprometiéndose a actuar de acuerdo con las políticas de Seguridad de la Información. Los contratos firmados con FacilitaPay deben tener una cláusula que asegure la confidencialidad de la información.

7. FUNCIONES Y RESPONSABILIDADES

Las políticas, estrategias y procesos corporativos de Seguridad de la Información son supervisados en Brasil y en el exterior por el Departamento de Seguridad Corporativa y discutidos en los foros de riesgo específicos de las áreas y en los Comités Ejecutivos que se ocupan del Riesgo Operacional o Tecnología.

7.1 Controles internos Las funciones y responsabilidades de los controles internos se describen en los siguientes manuales de FacilitaPay:

- Código de conducta de FacilitaPay;
- Política de prevención de lavado de dinero de FacilitaPay.

7.2 Seguridad corporativa

• Mejorar la calidad y eficacia de sus procesos, buscando la integridad, disponibilidad y confidencialidad de la información; • Proteger la información de las amenazas que buscan asegurar la continuidad del negocio y minimizar los riesgos para el negocio; • Establecer, implementar, operar, monitorear y asegurar la mejora continua del sistema de gestión de seguridad de la información. • Definir y formalizar los objetivos, controles y estrategia de gobierno de seguridad de la información, junto con el Comité Ejecutivo de Seguridad de la Información. • Coordinar acciones para alcanzar los objetivos y estrategia de gobernanza de seguridad de la información aprobados por los comités, involucrando a las áreas responsables. • Establecer y difundir una cultura de seguridad de la información. • Proponer inversiones para la seguridad de la información. • Definir las políticas y estándares de seguridad de la información a aplicar en los procesos, productos y tecnologías. • Definir estándares mínimos de seguridad para Unidades Internacionales y Empresas Controladas en Brasil y en el exterior y Entidades mantenidas o administradas por FacilitaPay, asegurando la alineación con los objetivos de seguridad de la información definidos por la empresa.

7.3 Unidades internacionales

Deben actuar de forma proactiva en la identificación, prevención y corrección de riesgos e informar periódicamente al Departamento de Seguridad Corporativa.

7.4 Empresas y entidades relacionadas

Las empresas relacionadas controladas en Brasil y en el exterior y las entidades mantenidas o administradas en relación con FacilitaPay deben evaluar las directrices y requisitos establecidos en esta política y sus anexos, informando periódicamente al Consejo de Seguridad Corporativa los riesgos identificados, adaptando sus procedimientos internos de seguridad de acuerdo con su segmento de negocio y apetito de riesgo. Estas empresas deben estar clasificadas y contar con un modelo de gobernanza basado en la evaluación de riesgos, que considere los siguientes aspectos: Impacto en la imagen de la Sociedad, Modelo de Arquitectura y Conectividad con la Sociedad, y Volumen de datos sensibles almacenados. Este modelo de gobierno puede variar entre la evaluación y el seguimiento directo de la adhesión a los controles definidos o tras una declaración de adhesión a realizar por la propia empresa.

7.5 Comité Ejecutivo de Seguridad de la Información

Debe acreditar la estrategia, objetivos, presupuesto y acciones necesarias para la mitigación de los riesgos de los procesos de seguridad de la información.

7.6 Área de Tecnología

Mantener el parque tecnológico disponible y actualizado con los estándares de seguridad implementados, dentro de los plazos compatibles con los niveles de riesgo.

7.7 Área de negocio

Proteja la información de FacilitaPay bajo su responsabilidad.

8. SANCIONES DISCIPLINARIAS

Las violaciones de esta política están sujetas a sanciones disciplinarias previstas en las normas internas y la legislación vigente donde se encuentran las empresas.

9. DOCUMENTOS RELACIONADOS

Esta Política Corporativa de Seguridad de la Información se complementa con procedimientos específicos de Seguridad de la Información de acuerdo con aspectos legales y regulatorios y aprobados por la Superintendencia de Proyectos de Gobierno y Seguridad Cibernética y la Superintendencia Operativa de Seguridad Cibernética, subordinada al Departamento de Seguridad Corporativa, dentro de la estructura del Área de Riesgos y Finanzas de FacilitaPay.

9.1 Marcos y reglamentos

• Resolución 4.658 del Banco Central Resolución 4.752 del Banco Central Ley General de Protección de Datos Personales - Ley N° 13.709/2018 10. ••

10. GLOSARIO

• APT (Advanced Persintent Threat): Ataques persistentes avanzados. • Ciberseguridad: es el término que designa el conjunto de medios y tecnologías utilizados en la defensa de los sistemas de información, infraestructura, redes informáticas y/o dispositivos personales, con el fin de evitar daños, robos, intrusiones, alteraciones o destrucción de la información. Daño Relevante: Acción que puede afectar la privacidad del individuo y puede causar un alto riesgo para su integridad física o moral. Parque tecnológico: conjunto de activos de infraestructura y sistemas tecnológicos. Segregación de funciones: consiste en la separación de actividades entre áreas y personas potencialmente conflictivas o que tienen información privilegiada, en la que el empleado no puede ejercer más de una función en los procesos de autorización, aprobación, ejecución, control y contabilidad. •••

11. CANALES DE COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BRASIL:

• ¿Recibió un correo electrónico sospechoso y desea enviarlo para su revisión? Reenviar correo electrónico a: legal@facilitapay.com • ¿Sospecha de incidentes de seguridad de la información? Reenviar correo electrónico a: legal@facilitapay.com