POLITICA DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES (TIC)

Historial de versiones.

Versión	Fecha	Modificado por	Descripción breve
V0.1	NOV.2024	Auditores Consultores Recad Limitada	Política de Tecnología de la Información y Comunicaciones (TIC)
V0.1	NOV.2024	Directores y Abogado	Política de Tecnología de la Información y Comunicaciones (TIC)
V0.1.	NOV.2024	Gerente General	Política de Tecnología de la Información y Comunicaciones (TIC)

Aprobada por Directorio 30/11/2024

7) Procedimientos de seguridad de las operaciones y comunicaciones de la entidad, mediante la implementación de:

i) Herramientas y controles para la detección y protección proactiva de ataques cibernéticos y otras actividades anómalas. Por ejemplo, el uso de firewalls de aplicaciones web, sistemas de prevención de intrusos, sistemas de prevención de pérdida de datos, sistemas anti-denegación de servicios, filtrado de correo electrónico, antivirus, antispyware y antimalware, entre otros.

ii) Un proceso de gestión de la configuración de los sistemas y activos de información.

iii) Herramientas y procedimientos para el respaldo, transferencia, restauración y eliminación segura de la información, al interior de la organización y con terceros, incluyendo medios físicos y electrónicos. Para ello se deberá considerar:

a) Las disposiciones relativas al respaldo, transferencia, restauración y eliminación de información en las normas que resguardan la protección de datos y los derechos de los inversionistas, incluyendo acuerdos de no divulgación.

b) Los procesos de administración de respaldos que aseguren la disponibilidad, confidencialidad e integridad de la información ante la ocurrencia de un incidente, el que debe ser concordante con el análisis de los riesgos para la gestión de la continuidad del negocio de acuerdo con lo dispuesto en la sección E.4.2 siguiente. Los respaldos de la información se debiesen mantener en lo posible en ambientes libres de códigos maliciosos y en instalaciones distintas a los sitios de producción. Además, se deben realizar pruebas de restauración de respaldos periódicas, al menos anuales, con el fin de verificar que la información crítica puede ser recuperada en caso de que los datos originales se pierdan o se dañen.

c) Herramientas y procedimientos de identificación, autenticación y control de acceso para los canales digitales a través de los cuales la entidad interactúa con sus clientes.

d) Herramientas y procedimientos para que la información que la entidad decidiere almacenar o procesar mediante servicios en la nube conserve sus características de disponibilidad, confidencialidad e integridad.

iii) Procedimientos de comunicaciones para mantener informado en forma oportuna al directorio u órgano equivalente, a otras partes interesadas (tanto internas como externas), a las autoridades pertinentes en materia de seguridad de la información y ciberseguridad, y a esta Comisión, de la ocurrencia de un incidente y las medidas adoptadas para resolverlo. Estos procedimientos deberán considerar las disposiciones relativas al registro, reporte y comunicación de incidentes de la sección V.E de esta norma. Asimismo, tratándose de incidentes que afecten la calidad o continuidad de los servicios a los clientes o de un hecho de público conocimiento, la

institución será responsable de informar oportunamente a los usuarios sobre la ocurrencia de dicho evento, debiendo actualizar la información disponible hasta que se conozcan las conclusiones sobre las causas del incidente y las medidas adoptadas para resolverlo, incluyendo el cumplimiento de las normas que resguardan la protección de datos personales y los derechos de los inversionistas.

f) Se deberá implementar un Plan de Crisis en el que se determine los procedimientos de escalamiento, comunicaciones, gestión y reporte de eventos de continuidad operacional para mantener informado en forma oportuna al directorio u órgano equivalente, a todas las partes interesadas y a esta Comisión, respecto de información relevante respecto del evento de continuidad, las medidas adoptadas para resolverlo y para coordinar una respuesta adecuada dentro de los puntos objetivos y tiempos objetivos de recuperación previstos en el BIA (entidades clasificadas en el Bloque 3 al que se refieren las secciones anteriores).

Política de Tecnologías de la Información y Comunicación (TIC)

1. **Introducción**

   Establecer la política de TIC para garantizar una gestión adecuada de los activos de información, la continuidad de las operaciones, y la seguridad en la plataforma de Cobranza de Factoring.

2. **Objetivo**

   Desarrollar un marco de gestión para los recursos de TIC en la aplicación de cobranza, asegurando el diseño, implementación y control adecuado de los sistemas en la nube (AWS) y locales.

3. **Alcance**

   La política aplica a toda la infraestructura TIC (Tecnologías de la Información y Comunicación) de la plataforma de cobranza, incluyendo servidores, bases de datos y servicios de integración externa, como el Servicio de Impuestos Internos (SII).

4. **Líneas de Responsabilidad**

   Desarrollador de la Aplicación: Responsable de implementar y documentar los algoritmos y funcionalidades en PHP (Yii2) y MariaDB

   - Administrador de Sistemas: Responsable de gestionar el entorno en AWS (respaldo IAM diario, monitorización, actualizaciones de seguridad).
   - Equipo de Seguridad: Realiza auditorías periódicas y establece controles de acceso.

5. **Procesos TIC**

   - **Diseño y Operación del Servicio**

Definir y aplicar los procesos para el diseño, la operación y la transición de los servicios TIC. Esto incluye:

- ✓ Gestión de cambios: Verificación y pruebas antes del despliegue en producción.
- ✓ Monitoreo continuo: Evaluación de rendimiento y disponibilidad del sistema en AWS.
- ✓ Gestión de Incidentes y Continuidad del Servicio
- ✓ Definir procedimientos de respuesta ante incidentes para la continuidad operativa. Esto abarca:

  - Evaluación de Riesgos y Contingencia: Análisis del impacto en la operación de cobranza.
  - Respaldo y Restauración: Copias de seguridad automáticas en Amazon S3 y pruebas de restauración.

➢ **Procedimientos de Gestión de TIC**

- ✓ Actualización de Seguridad y Obsolescencia

  Implementar un proceso de actualización de seguridad (parches) y gestión de obsolescencia para el software en uso (PHP y MariaDB), evitando vulnerabilidades y manteniendo soporte actualizado.

- ✓ Capacitación y Concientización del Personal
- ✓ Capacitar al personal sobre seguridad de la información Incluyendo:

  - Talleres de concientización: Riesgos de seguridad, vulnerabilidades, y gestión de incidentes.
  - Difusión de políticas de TIC: Información continua sobre responsabilidades y medidas de protección de los activos TIC.

- ✓ Control de Acceso y Seguridad de la Información

➢ **Autenticación y Autorización**

- ✓ Definir roles y permisos en la aplicación de cobranza para limitar el acceso a información sensible. En el entorno de AWS, utilizar IAM para gestionar los accesos, garantizando que solo los usuarios autorizados puedan acceder.
- ✓ Control de Acceso a la Nube
- ✓ Administrar el acceso a los recursos de AWS mediante políticas de IAM, con autenticación multifactorial para accesos críticos, y auditorías periódicas para asegurar el cumplimiento.

➢ **Auditoría y Revisión**

- ✓ Auditoría de TIC
- ✓ Realizar auditorías anuales del sistema TIC, evaluando:
- ✓ Cumplimiento de Políticas: Verificación de que se siguen los procedimientos definidos.

- ✓ Evaluación de Eficacia: Evaluar la efectividad de los controles y mejoras continuas.

6. Conclusión

Esta política establece el marco para la gestión de las TIC en la plataforma de cobranza, asegurando un enfoque integral que mantiene la seguridad, disponibilidad, y confidencialidad de la información de los deudores y clientes de la entidad de ASESORIAS E INVERSIONES FSJ SPA.

Política de Seguridad de la Información y Ciberseguridad

1. Introducción

El objetivo de esta política es establecer directrices claras para proteger la información y los activos digitales de la empresa, así como mitigar los riesgos asociados a la ciberseguridad. Esta política es aplicable a toda la infraestructura de tecnologías de la información, los sistemas y los usuarios que tienen acceso a los datos, incluidos los sistemas alojados en la nube de AWS, el software de cobranza basado en PHP y la base de datos en MariaDB.

2. Alcance

Esta política se aplica a todos los usuarios, empleados, socios y proveedores que interactúan con los sistemas de la empresa. También cubre el acceso y uso de recursos de AWS, la gestión de la base de datos, y el sistema de control de versiones en GitHub.

3. Principios de Seguridad de la Información

- ➢ Confidencialidad
  - ✓ Garantizar que solo los usuarios autorizados tengan acceso a la información sensible.
    Los roles y permisos son gestionados en la aplicación de cobranza para asegurar que cada usuario tiene acceso únicamente a los datos y funciones necesarias para su rol.
  - ✓ Integridad
    Proteger los datos y los activos digitales contra modificaciones no autorizadas.
    Implementar mecanismos de control para verificar la integridad de los datos en el proceso de sincronización de información con el Servicio de Impuestos Internos (SII).
  - ✓ Disponibilidad
    Asegurar la disponibilidad de los sistemas críticos en todo momento mediante políticas de respaldo diarias en AWS y un plan de recuperación ante desastres.
  - ✓ Realizar pruebas periódicas de restauración y monitoreo del rendimiento de los sistemas.

- ➢ Niveles de Tolerancia al Riesgo

Para gestionar los riesgos de seguridad de la información, la empresa ha establecido niveles de tolerancia al riesgo que reflejan la aceptación de ciertos niveles de exposición. Estos niveles están alineados con los objetivos estratégicos y las capacidades de mitigación de la empresa.

- Evaluación de Riesgos

- ✓ Identificación de Riesgos: Identificar los riesgos específicos asociados al sistema de cobranza, el almacenamiento en AWS y el acceso a datos sensibles.
- ✓ Análisis de Impacto: Evaluar el impacto de cada riesgo en función de su probabilidad y potencial de daño.

- Estrategias de Mitigación

- ✓ Prevención: Implementar medidas para reducir la probabilidad de incidentes, tales como la autenticación multifactorial para accesos sensibles y la aplicación de políticas de control de acceso en AWS.
- ✓ Detección y Respuesta: Monitorear los eventos de seguridad y establecer alertas para identificar y responder rápidamente a posibles amenazas.
- ✓ Recuperación: Asegurar la restauración de datos críticos a partir de respaldos en caso de un incidente.

- Controles de Acceso y Autenticación

- ✓ Gestión de Identidades y Control de Acceso (IAM)
- ✓ Utilizar políticas de IAM en AWS para restringir el acceso a los recursos en la nube.
- ✓ Implementar permisos basados en roles para asegurar que solo los usuarios autorizados puedan acceder y modificar los datos de clientes y deudores.

- Autenticación y Autorización en la Aplicación

- ✓ La aplicación cuenta con un sistema de autenticación que verifica la identidad de cada usuario antes de otorgar acceso.
- ✓ La autorización se gestiona mediante roles y permisos para asegurar que cada usuario solo tenga acceso a los módulos y datos necesarios.

- Gestión de Incidentes

La empresa establece un procedimiento de respuesta ante incidentes de seguridad que permite la detección, análisis y mitigación rápida de cualquier evento de seguridad:

- ✓ Detección de Incidentes: Monitoreo continuo de logs de sistema y alertas de seguridad.
- ✓ Evaluación de Impacto: Análisis del alcance y gravedad del incidente.
- ✓ Respuesta y Recuperación: Activación de un plan de respuesta que incluye la contención del

incidente y la restauración de los sistemas afectados.

- ✓ Documentación y Aprendizaje: Registro de incidentes y lecciones aprendidas para mejorar la postura de seguridad.

➢ Respaldo y Recuperación ante Desastres

- ✓ Respaldo Diario: Realización de copias de seguridad diarias en Amazon S3 para garantizar la recuperación de datos en caso de pérdida.
- ✓ Pruebas de Restauración: Verificación periódica de la capacidad de recuperación de los respaldos.
- ✓ Plan de Continuidad del Negocio: Estrategias para mantener la operatividad del sistema de cobranza en caso de desastres naturales o fallos críticos.

➢ Monitoreo y Auditoría

- ✓ Se implementarán auditorías periódicas para verificar el cumplimiento de la política de seguridad de la información, así como para identificar y abordar vulnerabilidades de manera proactiva.
- ✓ Auditorías de Seguridad: Exámenes trimestrales de la seguridad de la infraestructura y el software de cobranza.
- ✓ Monitoreo de Accesos: Registro y análisis de accesos a la plataforma para identificar patrones inusuales o intentos de acceso no autorizados.

4. Capacitación y Concientización

La empresa se compromete a capacitar regularmente a su equipo en buenas prácticas de seguridad de la información y ciberseguridad para minimizar el riesgo de errores humanos.

➢ Cumplimiento Legal y Normativo

- ✓ Cumplimiento con las leyes y regulaciones aplicables en materia de protección de datos y ciberseguridad, especialmente en relación con el tratamiento de la información de los clientes y deudores.
- ✓ Colaboración con terceros y proveedores para asegurar que cumplen con los estándares de seguridad exigidos.

➢ Conclusión

Esta política de Seguridad de la Información y Ciberseguridad establece los lineamientos necesarios para proteger los activos digitales de la empresa y mitigar los riesgos asociados a la operación del sistema de cobranza. La implementación de controles de acceso, respaldo, auditorías y capacitación asegura que el sistema cumpla con altos estándares de seguridad, apoyando la continuidad del negocio y la confianza en el manejo de datos críticos.

FJD FACTORING

Prosystem

POLITICAS DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN (ITC)

Prosystem ofrece a sus clientes, mediante una serie de aplicaciones, el manejo de carteras de Factoring:

- Registro de movimientos contables en las operaciones
- Incluyendo créditos
- Cesiones electrónicas
- Pagos
- Reversas
- Liquidaciones de excedentes
- Cesiones a fondos de inversión.
- Otorgamientos
- Múltiples Documentos
  - ✓ Factura
  - ✓ Cheque
  - ✓ Letra
- Prorrogas
- Aplicación de Intereses
- Entre Otros

Las aplicaciones de Factoring y Contabilidad están desarrolladas en lenguaje Visual Basic 6.0 y la información se almacena en bases de datos Microsoft SQL.

Los algoritmos de cálculo y control están desarrollados como Procedimientos Almacenados (Stored Procedures) los que corren en el mismo motor de base de datos.

Cada usuario tiene un acceso propio a las aplicaciones, el cual es creado por un administrador de la empresa. Este último también otorga diferentes niveles de acceso, privilegios y visualización de múltiples carteras de ejecutivos.

Dado que se trata de aplicaciones de 32 bits éstas corren en un ambiente de escritorio, es decir se instalan localmente en los equipos de los usuarios. Las bases de datos se encuentran virtualizadas en un centro de datos local. La conexión entre las aplicaciones y las bases de datos se realiza mediante una conexión IP al servidor con un usuario y clave propia para cada cliente (Factoring)

Como una capa extra de seguridad se configura también una conexión VPN exclusiva para cada equipo, con lo cual la información se traspasa en forma encriptada de extremo a extremo.

En relación con el Datacenter en cuestión Prosystem mantiene contratos de servicio con la empresa Data byte S.A. (www.databyte.cl), dicha empresa provee del servicio de Virtual Prívate Server (VPS) en el cual se aloja y administra la información.

Data byte es un centro de datos con dirección en Santiago de Chile, el cual se encuentra tramitando la Certificación de su Sistema de Gestión de Calidad y Seguridad de la Información basado en las Normas ISO 9001:2015 e ISO 27001:2022

El servicio incluye respaldos diarios de bases de datos, los cuales son mantenidos por un período de 3 meses; luego de eso se resguarda una copia de la base al último día hábil de cada mes.

El servicio también incluye un protocolo de alojamiento de imágenes tanto de clientes, operaciones y documentos – los cuales se respaldan por un período de un año.

Francisco Valdivieso
Administración y Proyectos
Prosystem Ltda.