POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PRESTIGE SOFTWARE

Contenido

Control de Versiones:

Fecha	Versión	Descripción	Autor	Aprobación	Estado
23/07/2023	0.1	Creación	A2SECURE		Aprobado
29/11/2024	1.1	Se añaden aspectos específicos de PCI DSS	A2SECURE		Aprobado
04/12/2024	1.2	Se modifica el apartado de Excepciones con la inclusión del “Acta de registro de excepciones a la política”, así como el pie de página y otros detalles	A2SECURE		Aprobado

1. Introducción y objetivos

La seguridad de la información es un reto a tener en cuenta en la gestión del riesgo empresarial. La falta de protección adecuada y de gestión de los riesgos que afectan a la seguridad de la Información puede resultar en pérdidas financieras para Prestige Software, y tener un impacto en su marca y reputación.

La Política de Seguridad de la Información de Prestige Software establece requisitos de seguridad mínimos y concisos que la empresa debe satisfacer en sus entornos para garantizar unos niveles adecuados de confidencialidad, disponibilidad e Integridad de todos sus activos.

Esta política representa los mínimos requisitos en Seguridad de la Información que todos los departamentos de Prestige Software han de seguir, siguiendo las normativas legales y regulatorias que deben cumplirse para asegurar la protección de la información de la empresa.

Esta política de Seguridad de la Información está alineada con los estándares internacionales UNE-ISO/IEC 27001:2022 y UNE-ISO/IEC 27002:2022, así como con la normativa de PCI DSS 4.0.

1.1. Normativa interna relacionada

- Política de clasificación de la información
- Política de contraseñas
- Política de control de acceso lógico
- Política de Escritorio Limpio
- Política de Gestión de vulnerabilidades
- Política de mantenimiento, desarrollo seguro y adquisición de sistemas
- Política de Métodos de Cifrado
- Política de Retención de datos
- Política de Seguridad de Proveedores
- Política de Seguridad en las Operaciones
- Política de Seguridad en el Trabajo Remoto
- Política de Uso Aceptable de Activos
- Procedimiento de Gestión de Cambios
- Procedimiento de Gestión de Llaves Mecánicas
- Procedimiento de respuesta a incidentes
- Procedimiento de Seguridad Física
- Procedimiento para la transferencia de información
- Política de seguridad en los recursos humanos
- Plan de recuperación de desastres
- Plan de continuidad del negocio
- Política de requisitos legales
- Procedimiento de copias de seguridad
- Acta de registro de excepciones a la política
- Metodología de evaluación de riesgos

2. Alcance

Esta política de seguridad de la Información y los procedimientos relacionados serán de aplicación para todos los departamentos de Prestige Software y todas las sociedades del grupo adecuándose tanto a la ISO 27001:2022 como a la PCI DSS v4.0.

3. Audiencia

Todo el personal de Prestige Software tiene que conocer y cumplir obligatoriamente esta política, particularmente aquellos con responsabilidades en tecnología o en gestión de Información, así como el Responsable de Seguridad de la Información (CISO a partir de ahora).

El incumplimiento de esta política, así como el resto de la normativa relacionada puede llevar a la organización a tomar medidas disciplinarias o sanciones contra el responsable del incumplimiento.

4. Excepciones y correcciones a la política

Excepciones, modificaciones y comentarios a la presente política se realizarán bajo comunicación con dirección o la Oficina de Seguridad, mediante el completado del "Acta de registro de excepciones a la política" por parte del solicitante.

5. Política de Seguridad de la Información

5.1. Gestión y dirección de la seguridad de la Información

5.1.1. Políticas para Seguridad de la información

La Política de Seguridad de la Información de Prestige Software y su normativa relacionada establecen los requisitos a cumplir por todos los departamentos de la empresa.

El responsable de la Política de Seguridad de la Información es el CISO de Prestige Software y debe ser aprobada por el Comité de Dirección.

Los procedimientos y políticas relativos a los que se haga referencia en la Política de Seguridad de la Información serán asimismo responsabilidad del CISO de la compañía y para su modificación será necesario, como mínimo, la aprobación por parte de los siguientes roles:

- CISO
- CTO
- CEO
- Product Manager

5.1.2. Distribución de las políticas de Seguridad de la información

La política de Seguridad de la Información y las políticas y procedimientos asociados de Prestige Software estarán disponibles para todos los trabajadores de la empresa en el espacio corporativo.

El CISO velará por que dicha política sea conocida por todos los trabajadores de Prestige Software.

5.1.3. Revisión de las políticas de Seguridad de la información

El CISO junto con el Comité de Seguridad de la Información se debe encargar de liderar la revisión anual de la Política de Seguridad de la Información, así como de las políticas y procedimientos relacionados.

6. Organización de Seguridad de la Información

6.1. Organización Interna

6.1.1. Roles y responsabilidades en Seguridad de la Información

A continuación, se describen los roles implicados en la gestión de la Seguridad de la Información y sus responsabilidades:

- **Consejero delegado (CEO)**
  - Es informado de la política de la Seguridad de la Información y es el responsable de proveer el liderazgo y la estructura de gestión necesaria, así como los recursos necesarios, para la implementación de la Política de Seguridad de la Información.
  - Participa en la revisión de las políticas y actividades de Seguridad de la Información.
  - Es informado de la implementación de la Política de la Seguridad en los diferentes departamentos, incluyendo el cumplimiento legal y normativo.
  - Es responsable de la aprobación de la financiación de las actividades de Seguridad de la Información.
  - Se encarga de, en consulta con el CISO, establecer la responsabilidad de la protección del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y de la información de identificación personal (PII) y aplicar los procedimientos acordados para las infracciones de la PII y los riesgos de seguridad y otras obligaciones en virtud de la PCI DSS y otras leyes de protección de datos.
- **Responsable de Seguridad de la Información (CISO)**, (rol actualmente delegado en el COO).
  - Asegurar que la Política de Seguridad de la Información esté alineada con la actividad de la empresa.
  - Se asegura de la integración de los requisitos de Seguridad de la Información en todos los procesos de negocio.
  - Se le informa de todas las actividades del negocio relacionadas con Seguridad de la Información.
  - Comunica e interactúa regularmente con empleados y la dirección acerca de los procesos y actividades definidos en la política de Seguridad de la Información.
  - Da soporte al negocio en la implementación y ejecución de la Política de Seguridad de la Información y sus procesos relacionados.

- Colabora en la creación y mantenimiento de la información relativa a los riesgos de Seguridad de la compañía.
- Participa en el ciclo de vida de los proyectos tecnológicos cuando es necesario o requerido.
- Es el responsable de la creación y comunicación a la compañía de las tareas de concienciación en Seguridad, así como de preparar el material necesario referente a los nuevos empleados.
- Debe estar informado de las tendencias de la industria. Por ejemplo, asistiendo a conferencias, cursos o grupos de trabajo y/o foros relacionados con la Seguridad de la Información.
- Junto con el departamento de TI y el resto de la oficina de seguridad, es el responsable de analizar los incidentes de seguridad y liderar el plan de Respuesta a Incidentes en caso de ser necesario.

- **Propietario de la Información**
  - Es propietario de la información que su departamento genera, almacena o procesa.
  - Es el responsable de aplicar y monitorizar los procesos de seguridad bajo su control para cumplir con la Política de Seguridad de la Información.
  - Es el responsable de proteger los activos individuales.
  - Es el responsable de identificar los incidentes de seguridad relacionados con la información de la que es responsable y notificarlos acorde a los pasos establecidos en el Procedimiento de Respuesta a Incidentes de Prestige Software.

6.1.2. Segregación de tareas

Se deben implementar controles para asegurar que una persona no pueda realizar las siguientes funciones simultáneamente:

- Gestión de usuarios (añadir, modificar o borrar usuarios o permisos y autorizaciones, así como cambio de contraseñas) y aprobación de cambios en los usuarios.
- Revisión auditoría de la seguridad y sus registros e Implementación/operación de los controles de seguridad.

Cuando la separación de funciones no sea técnicamente posible, deberán aplicarse otros controles compensatorios, como la vigilancia de las actividades, los registros de auditoría y la supervisión de la gestión.

Riesgos y Cumplimiento velará por asegurar el correcto cumplimiento de los controles de segregación de tareas.

6.1.3. Contacto con las autoridades

El departamento legal será el encargado de contactar con las autoridades en lo referente a incidentes de Seguridad de la Información, salvo con las diferentes Autoridades en materia de Protección de Datos, con las que se comunicará el representante designado al respecto.

6.1.4. Contacto con grupos de interés especial

El CISO mantendrá contactos y/o participará en grupos de especial interés, así como en foros especializados en seguridad de la Información con los objetivos de compartir información sobre actividades fraudulentas, mejorar el conocimiento de las mejores prácticas en materia de Seguridad de la Información, mantenerse al día de las tendencias en tecnologías de seguridad y en tecnologías o métodos utilizados en el mercado para vulnerar la seguridad de las empresas, mantener contacto con especialistas en seguridad, y conocer el estado del arte de las principales vulnerabilidades y amenazas existentes en el sector.

Las peticiones de información por parte de interesados referentes a Seguridad de la Información serán gestionadas en coordinación con el CISO.

6.1.5. Seguridad de la tarjeta de pago

Prestige Software tiene la responsabilidad de implementar y cumplir con el último Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI).
Para lograr el cumplimiento de la norma de seguridad de datos de la industria de las tarjetas de pago (PCI), todas las Entidades tienen la responsabilidad de asegurar la confidencialidad de la información de las tarjetas de crédito transmitida, almacenada y procesada por Prestige Software de la siguiente manera:

1. Construir y mantener una red segura instalando y manteniendo configuraciones de firewall para proteger los datos de los titulares de las tarjetas y evitando el uso de las contraseñas del sistema y otros parámetros de seguridad suministrados por los proveedores.
2. Proteger al titular de la tarjeta aplicando controles para proteger los datos almacenados del titular de la tarjeta en reposo y encriptando la transmisión de los datos del titular de la tarjeta a través de redes públicas abiertas;
3. Mantener un Programa de Gestión de Vulnerabilidades para proteger todos los sistemas contra el malware, actualizar regularmente el software o los programas antivirus y desarrollar y mantener sólo sistemas y aplicaciones seguras;
4. Aplicar fuertes medidas de control de acceso que restrinjan el acceso a los datos de los titulares de las tarjetas por la necesidad de las empresas de conocerlos. Identificar y autenticar el acceso a los componentes del sistema y que restringen el acceso físico a los datos del titular de la tarjeta;
5. Supervisar y probar las redes mediante el seguimiento y la vigilancia de todos los accesos a los recursos de la red y a los datos de los titulares de las tarjetas, y mediante el ensayo periódico de los sistemas y procesos de seguridad; y
6. Mantener una Política de Seguridad de la Información que aborde la seguridad de la información para todo el personal.
7. Revisar la documentación y controles de seguridad asociados a PCI DSS al menos una vez al año.

6.1.6. Seguridad de la información en la gestión de proyectos

En cada nuevo proyecto que implique cambios tecnológicos a implementar por la empresa se incluirá un proceso de revisión por parte del CISO para asegurar el correcto cumplimiento de la presente Política de Seguridad de la Información.

Todos los procesos de revisión que afecten a la gestión de la información de la compañía serán documentados en el proyecto en base a las recomendaciones del CISO.

Los proyectos que impliquen tratamientos de datos personales deberán ser informados asimismo al departamento de protección de datos: GDPR@Prestige-soft.es.

7. Gestión y validez del documento

Este documento es válido a partir de 28/11/2024.
El propietario de este documento es el Responsable de Seguridad de Prestige Software, quien debe revisar y, si es necesario, actualizar el documento al menos una vez al año.