Política de seguridad informática (externos y terceros)

CIRCULACIÓN	
Para la aplicación: Todos **PÚBLICO**	**Para más información: Toda la empresa**

Todas las modificaciones de documentos deben rastrearse y notificarse a continuación:

Versión	Autor	Fecha	Objeto
V.1.0	Christian Koschmieder	28/08/2024	Creación

Versión	validador	Papel	Fecha	Objeto
V1.0	Christian Koschmieder	CISO	28/08/2024	Validación
V1.0	Alberto Méndez	DIRECTOR GENERAL	28/08/2024	Validación
V 2.0	Christian Koschmieder	CISO	17/09/2024	Modificación
V 2.0	Alberto Méndez	DIRECTOR GENERAL	17/09/2024	Validación

ÍNDICE

1 INTRODUCCIÓN

1.1 OBJETIVO

El objetivo principal de este Anexo Externo a la Política de Seguridad Informática de Plexigrid (en adelante "Política") es definir los principios y reglas básicas para la gestión de la seguridad de la información para Externos. Esta Política esboza las directrices y procedimientos para que los Externos garanticen la confidencialidad, integridad y disponibilidad de la información y los sistemas de nuestra organización.

El objetivo final es que Plexigrid garantice la seguridad de la información y minimice los riesgos derivados de un impacto causado por una gestión ineficaz de la información.

1.2 OBJETIVOS ESPECÍFICOS

- Disponer de plataformas adecuadas que protejan los mecanismos de procesamiento, almacenamiento y comunicación donde se contengan y soporten los servicios prestados por Plexigrid.

- Educar a los Externos para lograr una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.
- Educar a los Externos para lograr que sean competentes y comprometidos, con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.
- Implantar una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante situaciones que puedan afectar a la continuidad, confidencialidad e integridad de la información en Plexigrid.

1.3 ALCANCE DEL DOCUMENTO

Esta Política establece los criterios y comportamientos que deben seguirse para preservar la seguridad de la información en Plexigrid por parte de Externos y terceros.

1.4 ÁMBITO DE LA POLÍTICA

Esta Política se aplica a todos los Externos.
Se entiende por externo cualquier persona no empleada que tenga acceso a la información y sistemas de la organización Plexigrid, incluyendo Contratistas, Vendedores, Socios, Consultores, Trabajadores Temporales y Practicantes.
Si al Externo se le facilitan equipos informáticos de Plexigrid y una cuenta de correo electrónico de Plexigrid, le será de aplicación la Política de Seguridad Informática de Plexigrid, con la excepción, en materia de derecho laboral, del régimen disciplinario por incumplimiento.
Todos los Externos deben cumplir estos requisitos mínimos sin perjuicio de disponer de políticas más restrictivas y mejorar la seguridad en la medida de lo posible. Adicionalmente, los proyectos en otros países deberán adaptar y desarrollar esta política e informar al Comité de Dirección de Plexigrid de su adecuación, en ejecución de los procesos de seguimiento del sistema de gestión de incidencias.

El ámbito de aplicación de esta Política abarca toda la información y los servicios de Plexigrid, independientemente de la forma en que se procese, de quién acceda a ella, del soporte que la contenga o del lugar en que se encuentre, tanto si se trata de información impresa como almacenada.

La Política debe ser mencionada en el sitio web corporativo de Plexigrid, www.plexigrid.com. Pero no debe ser publicada o compartida sin el permiso y conocimiento del CISO.

Esta Política debe seguir un proceso de actualización sujeto a cambios organizativos relevantes: crecimiento de la plantilla, cambios en la infraestructura informática, desarrollo de nuevos servicios, entre otros.

Todos los Externos deben reconocer que han leído, entendido y que cumplirán con esta Política antes de que se les conceda acceso a los sistemas e información de Plexigrid mediante la firma de la última página de la Política No empleados.

Una vez firmado, el departamento de Administración se hará cargo del documento firmado.

Aquellos Externos que hayan prestado servicios a Plexigrid con anterioridad a la aprobación de esta Política, deberán firmarla lo antes posible y enviarla al departamento de Administración.

1.5 PRINCIPIOS DE LA POLÍTICA DE INFORMACIÓN

Esta Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información contenidas en la Norma Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos de carácter personal y normativa que, en el ámbito de la Seguridad de la Información, pueda afectar a Plexigrid.

Plexigrid establece los siguientes principios básicos como pautas fundamentales de seguridad de la información que deben tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de la información:

- Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los responsables de Plexigrid, de forma que pueda coordinarse e integrarse con el resto de iniciativas estratégicas para formar un marco plenamente coherente y eficaz.
- Seguridad integral: La seguridad de la información se entenderá como un sistema de procesos integrado por elementos técnicos, humanos, materiales y organizativos, evitando, salvo en casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa normal, estando presente y aplicándose en todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.
- Gestión de riesgos: El análisis y la gestión de riesgos serán una parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá mantener un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción de estos niveles se llevará a cabo mediante el despliegue de medidas de seguridad, que establezcan un equilibrio entre la naturaleza de los datos y el tratamiento, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.
- Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación debe ser proporcional a los riesgos potenciales y a la criticidad y valor de la información y servicios afectados.
- Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adaptar su eficacia a la constante evolución de los riesgos y de los sistemas de protección. La seguridad de la información será abordada, revisada y auditada por personal cualificado.
- Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.
- Documentación: Para garantizar la seguridad, robustez y fiabilidad del sistema, es obligatorio crear la documentación pertinente antes y después de la ejecución.
- Gestión de códigos: La gestión de códigos es una práctica esencial para mantener bajo control la propiedad intelectual de la empresa.

Plexigrid considera que las funciones de Seguridad de la Información deben estar integradas en todos los niveles jerárquicos del personal de terceros. Ya que la Seguridad de la Información es responsabilidad de todo Plexigrid y de terceros o externos incluidos. Esta Política debe ser conocida, entendida y asumida por todos.

Para alcanzar los objetivos de esta Política, todos los externos y terceros deben establecer una estrategia de análisis preventivo de los riesgos que puedan afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos periódicos para su reevaluación. A lo largo de este ciclo de mejora continua, es importante realizar un seguimiento de la definición tanto del nivel de riesgo residual aceptado (apetito de riesgo) como de sus umbrales de tolerancia.

1.6 COMPROMISO DE LA DIRECCIÓN

Los externos y terceros deben comprometerse:

- Promover en la organización las funciones y responsabilidades en torno a la seguridad de la información.
- Proporcionar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Ofrecer formación interactiva y clases magistrales sobre seguridad.
- Promover la difusión y el conocimiento de la Política de Seguridad de la Información entre los empleados.
- Exigir el cumplimiento de la Política, la legislación vigente y los requisitos de los reguladores en materia de seguridad de la información.
- Considerar los riesgos para la seguridad de la información en la toma de decisiones.

1.7 FORMACIÓN Y SENSIBILIZACIÓN

Garantizar que todo el personal reciba un nivel adecuado de formación y concienciación en materia de seguridad de la información, especialmente en términos de confidencialidad y prevención de fugas de información.

Asimismo, los externos y terceros deberán informar a sus empleados de las actualizaciones de las políticas y procedimientos de seguridad en los que se vean afectados y de las amenazas existentes, de forma que se garantice el cumplimiento de esta Política.

Por otro lado, los externos y terceros tienen la obligación de actuar con diligencia con respecto a la información, asegurándose de que dicha información no caiga en poder de entidades no autorizadas.

1.8 RESPONSABILIDADES

Todo el modelo de responsabilidad puede encontrarse en la política del SGSI de Plexigrid:

Política del Sistema de Gestión de la Seguridad de la Información.docx

1.9 GENERAL

- Los externos y terceros son responsables de comunicar inmediatamente las anomalías e incidentes de seguridad que observen en los sistemas.
- Las modificaciones de datos e información en los sistemas de producción deben restringirse estrictamente a las transacciones y procesos expresamente diseñados para ello.
- Todos los equipos informáticos (ordenadores, estaciones de trabajo, estaciones gráficas, servidores y equipos accesorios, dispositivos móviles, tabletas, Smartphones), que se conecten a la Red deben acatar las normas y parámetros de instalación y configuración siguiendo como mínimo las mejores prácticas de seguridad emitidas por Plexigrid.
- Los sistemas serán gestionados por personal debidamente formado y cualificado para supervisar su

funcionamiento cotidiano y preservar la seguridad e integridad en colaboración con los propietarios individuales de los sistemas, como mínimo:

- Tecnologías de cifrado
- Ciberseguridad
- Vulnerabilidades del sistema y del software
- Gestión de accesos e identidades
- Tecnologías de seguridad en la nube

2 SISTEMAS DE INFORMACIÓN

- Todos los sistemas de información[1] , herramientas de datos (programas, bases de datos, sistemas de información, interfaces y otros) desarrollados con o a través de los recursos de Plexigrid seguirán siendo propiedad de Plexigrid, respetando su propiedad intelectual, incluidos sus diseños, fuentes, documentación y otros aspectos del desarrollo.
- Todos los sistemas de información realizados para Plexigrid deben desarrollarse y documentarse de acuerdo con la metodología estándar, basada en las hojas de concepto técnico del área del proyecto.
- Para todos los sistemas de información, la seguridad debe considerarse obligatoria desde los principios del ciclo de vida. Asimismo, se deben realizar las pruebas de vulnerabilidad y seguridad que el área encargada considere pertinentes y no se pondrán en producción hasta que se hayan corregido las vulnerabilidades existentes.
- Durante cada fase del proceso de desarrollo, mantenimiento y puesta a punto del sistema, los aspectos de seguridad deben definirse explícitamente, ser documentados por el equipo de desarrollo y establecerse como un requisito de seguridad específico.
- En la fase inicial de definición del proyecto, de un nuevo sistema, se debe asignar el "propietario" del sistema, en cumplimiento de las responsabilidades básicas en seguridad informática, así como estipular los formatos de seguimiento y control de cambios.
- Plexigrid podría exigir realizar un test de vulnerabilidades o Ethical Hacking realizado por quien ellos consideren a terceros, que garantice que el sistema es óptimo y seguro.
- Las pruebas deben realizarse en un entorno de pruebas antes de poner la aplicación en producción y hay que tener en cuenta el uso paralelo del nuevo sistema y el antiguo, para detectar errores.
- El proceso de producción de las aplicaciones, sistemas o sus actualizaciones debe realizarse de forma que no deteriore los servicios a los usuarios o el normal funcionamiento, por lo que debe estar debidamente coordinado y realizarse con calendarios preestablecidos.
- Debe asegurar que cada sistema cuente con un esquema de contingencia que debe considerar aspectos de software, hardware y personal necesarios para la continuidad del servicio; Esto debe ser revisado por el responsable de cada proceso en conjunto con la Dirección.
- Todo sistema de información debe tener asignado un administrador del sistema responsable de las actividades de explotación, gestión, cumplimiento de la seguridad establecida.
- Por defecto, ftp y sftp no son formas estándar para trabajar en Plexigrid, evitar siempre que sea posible. Sin embargo, en caso de necesidad, al menos un sftp seguro será el enfoque de seguridad mínima.
- Todos los cambios deben estar documentados. Dichas ventanas de mantenimiento deben quedar debidamente documentadas indicando la fecha, responsable, servidor y aplicación afectada, así como el motivo de los cambios realizados. Siguiendo el "proceso de procedimiento de gestión de cambios".

[1] Por sistemas de información se entiende todo lo que tiene que ver con la informática.

3 TRANSFERENCIA DE ARCHIVOS / INFORMACIÓN

1. Toda la información debe estar debidamente etiquetada.
2. La documentación del software, o cualquier tipo de información de uso propiedad de Plexigrid, no debe ser transferida a terceros sin previa autorización o acuerdo de confidencialidad con Plexigrid.
3. Toda la información que se genera, procesa, almacena y/o transita por la red de Plexigrid se considera propiedad de Plexigrid.
4. Sólo Plexigrid empresa datastore plataforma está autorizada para almacenar archivos.
5. Si es necesario transferir información sensible a un tercero, el propietario de la información debe solicitar asesoramiento informático sobre el cifrado de la información y el uso de claves criptográficas; se debe procurar transferir la información siempre cifrada.

4 BACKUPS

Los externos son responsables de realizar copias de seguridad de los datos esenciales que gestionan para respaldar la continuidad de la actividad y garantizar la recuperación de los datos en un plazo razonable.

Los requisitos de copia de seguridad deben aplicarse de acuerdo con la evaluación de riesgos establecida. Esto significa definir adecuadamente los medios, métodos y frecuencia de las copias de seguridad aceptables.

Plexigrid puede requerir acceso a esas copias de seguridad externas relacionadas con las copias de seguridad de Plexigrid en cualquier momento si es necesario. O solicitar simulaciones de recuperación.

5 SEGURIDAD DE LA INFORMACIÓN

5.1 GESTIÓN DEL CICLO DE VIDA DE LA INFORMACIÓN

Los terceros deben gestionar adecuadamente el ciclo de vida de la información, de modo que pueda evitarse un uso incorrecto durante cualquiera de las fases. El ciclo de vida de un activo de información consta de las siguientes fases:

1. **Crear o recopilar:** Esta fase se ocupa de los registros en su punto de origen.

2. **Distribución:** Es el proceso de gestión de la información una vez creada o recibida.
3. **Uso o acceso**: Ocurre después de que la información se distribuye internamente, y puede impulsar decisiones empresariales, generar nueva información o servir para otros fines.
4. **Almacenamiento:** es el proceso de organizar la información en una secuencia predeterminada y crear un sistema de gestión para garantizar su utilidad.
5. **Destrucción**: Establece prácticas para la eliminación de la información cuyos periodos de conservación definidos se han cumplido y la información que ya no lo está.

También deben tenerse en cuenta las necesidades empresariales. Si ninguno de estos requisitos exige que se conserve la información, deberá desecharse por medios que garanticen su confidencialidad durante el proceso de destrucción.

5.2 GESTIÓN DE ACCESOS Y RESPONSABILIDADES

- La clasificación de los datos y el etiquetado de sensibilidad correrán a cargo del creador de los datos. Los datos deben protegerse contra accesos no deseados, almacenándose en la carpeta correcta, con los permisos correctos y el etiquetado de sensibilidad correcto.
- Es necesario definir el acceso RBAC para almacenar los datos de forma segura y proteger los accesos no deseados.

5.3 ACTIVACIÓN DE INCIDENTES, APOYO Y RECUPERACIÓN EN CASO DE CATÁSTROFE

Los terceros deben actuar de acuerdo con las recomendaciones de la norma ISO27001 aunque no dispongan de la certificación ISO. Esto significa que los terceros deben utilizar las mejores prácticas y disponer de los procesos respectivos para activar y resolver una petición de un cliente en caso de incidente.

6 AUDITORÍAS Y CUMPLIMIENTO

Debe garantizarse el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software propietarios.

Debe garantizarse la seguridad de los datos personales. Los sistemas informáticos deben apoyar la protección de los datos personales mediante la aplicación de controles técnicos, lo que incluye:

- Tecnologías de cifrado
- Controles de acceso

- Mecanismos de disponibilidad
- Copias de seguridad

El tratamiento de los datos personales debe ajustarse a los requisitos de la normativa local, así como a los requisitos específicos que puedan solicitar los clientes, entre los que se pueden incluir:

- Eliminar datos personales tras un determinado periodo de almacenamiento
- Para que los datos estén disponibles durante un periodo determinado
- Permitir a los clientes que lo soliciten modificar sus datos personales
- Gestionar las solicitudes específicas de los clientes en relación con sus datos personales

El cumplimiento de la normativa local relativa a los mecanismos criptográficos también debe ser garantizado por los equipos de Plexigrid, ya que algunos países imponen limitaciones o tienen peticiones específicas como la directiva CIS en Europa, por ejemplo.

7 SOFTWARE Y LICENCIAS

Plexigrid no se hace responsable del uso de software sin licencia.

8 VARIOS

Responsabilidades

Los externos son responsables del cumplimiento de esta Política y de cualquier otra política y procedimiento de seguridad informática pertinente.

En caso de duda, Plexigrid proporcionará orientación y apoyo a los Externos sobre las mejores prácticas y procedimientos de seguridad informática.

Tratamiento de datos

Los externos deben manejar los recursos de Plexigrid con el mismo nivel de cuidado y confidencialidad que los empleados de Plexigrid. Los externos no deben compartir, copiar o distribuir los recursos de Plexigrid sin el permiso previo por escrito de nuestra organización.

Uso del sistema

Los externos deben utilizar los recursos de Plexigrid sólo para fines autorizados.

Los externos no deben instalar o utilizar software o hardware no autorizado en los sistemas de Plexigrid.

Finalización del acceso

En caso de terminación o salida de un Externo de la relación con Plexigrid, cualquier acceso a los recursos de Plexigrid debe ser terminado inmediatamente.

Control y ejecución

Los externos son conscientes de que el departamento informático de Plexigrid supervisará su acceso y uso de los recursos de Plexigrid para garantizar el cumplimiento de esta política.

El incumplimiento de esta politica puede resultar en una accion disciplinaria, hasta e incluyendo la terminacion del contrato o acuerdo del Externo asi como una penalidad financiera para cubrir los perjuicios causados a Plexigrid por el incumplimiento del Externo. El monto de la penalidad financiera sera fijado por Plexigrid, el Externo ya acepta el monto a ser fijado por Plexigrid de compensacion como justo y balanceado.

Enmiendas

Esta Política podrá modificarse o actualizarse en cualquier momento sin previo aviso.

Los Externos estarán obligados a cumplir cualquier cambio en esta Política.