POLÍTICA DE SEGURIDAD EN LA NUBE

El uso de la computación en la nube ha cambiado la forma en que las organizaciones deben evaluar y mitigar los riesgos de seguridad de la información debido a los cambios significativos en la forma en que los recursos informáticos se diseñan, operan y gobiernan técnicamente.

Conscientes de la trascendencia de la seguridad de la información, y en consonancia con el camino que marca nuestra propia identidad, desde la dirección de **Grupo Castilla** se ha impulsado la ampliación de su Sistema de Gestión de Seguridad de Información para incluir las directrices necesarias en relación con los controles de seguridad de la información aplicables a la prestación y el uso de servicios en la nube.

Habida cuenta de ello, la dirección, se compromete a:

- proporcionar recursos adecuados para implementar y mantener la ampliación de su sistema de gestión de la seguridad de la información efectivo según los requisitos del estándar ISO 27017;
- establecer roles y responsabilidades claros para esta ampliación;
- fomentar la participación de los empleados en la protección de la información y proporcionar la formación necesaria para mejorar las competencias en seguridad de la información, y;
- evaluar periódicamente el desempeño del sistema de gestión de la seguridad de la información y realizar ajustes según sea necesario.

La presente **Política de Seguridad como proveedor de servicios en la nube** establece los requisitos de seguridad que se aplican al diseño, implementación y operación de nuestros servicios en la nube en cumplimiento con los estándares internacionales como ISO/IEC 27017:

Requisitos Básicos de Seguridad de la Información

- Nuestros servicios en la nube han sido diseñados e implementados con controles de seguridad integrados desde su concepción (seguridad por diseño).
- Se realizan evaluaciones de riesgo periódicas para identificar y mitigar amenazas potenciales.
- Los datos del cliente son protegidos mediante cifrado en tránsito y en reposo.

Riesgos de Personas Autorizadas con Información Privilegiada

- El acceso a los sistemas críticos por parte de personal autorizado es monitoreado y auditado constantemente.
- Se implementan controles de segregación de tareas para minimizar el riesgo de uso indebido de información privilegiada y todo el personal con acceso privilegiado se ha sometido a la correspondiente capacitación en seguridad.

Multi-Tenencia y Aislamiento de Clientes

- Los entornos virtualizados están diseñados para garantizar el aislamiento lógico y físico de los datos de los clientes.
- Cada cliente tiene su propio espacio de almacenamiento y cálculo, con controles para prevenir accesos no autorizados entre inquilinos.
- Se utilizan hipervisores seguros y actualizados para mitigar riesgos relacionados con la virtualización.

Acceso a los activos del cliente por parte del personal de Grupo Castilla

- El acceso a los activos de los clientes esta estrictamente restringido a personal autorizado y limitado al mínimo necesario para realizar tareas operativas.
- Todos los accesos son registrados y revisados periódicamente.

Procedimientos de Control de Acceso

- Se ha implementado una autenticación robusta mediante el uso de autenticación multifactorial (MFA).
- Los privilegios de acceso son revisados regularmente para garantizar que estén alineados con las necesidades del puesto de trabajo.

Comunicaciones durante la Gestión del Cambio

- Los cambios de versión y actualizaciones serán comunicados con antelación a los clientes, proporcionando detalles sobre el impacto y la fecha de ejecución de la misma.

Desarrollo Seguro

- Incorporación de prácticas de desarrollo seguro en todo el ciclo de vida del software.
- Las prácticas de desarrollo seguro están alineadas con la ISO 27017 y con otros estándares reconocidos globalmente como OWASP y NIST
- Se sigue el principio de "seguridad por diseño", asegurando que la arquitectura de nuestras aplicaciones está concebida para mitigar posibles amenazas desde el inicio.
- Se han implementado medidas de seguridad en relación con la validación y sanitización estricta de entradas para prevenir ataques de inyección.
- Se realiza análisis pruebas de penetración para identificar posibles vulnerabilidades de seguridad

Seguridad de la plataforma

- Los sistemas están configurados para minimizar las superficies de ataque.
- Se realizarán pruebas de penetración periódicas para identificar y mitigar vulnerabilidades en la infraestructura.
- Una referencia horaria coherente y precisa resulta crucial para muchas tareas y procesos del servicio. Las marcas de tiempo en los registros del sistema desempeñan un papel esencial a la hora de identificar cuándo se produjeron los problemas y el orden cronológico de los eventos. Lo sistemas se sincronizan con el host time.windows.com.

Comunicación de incidentes de seguridad

- Cualquier incidente o evento con impacto en materia de seguridad será notificada de inmediato a los clientes afectados, proporcionando detalles del incidente y las medidas tomadas.
- Se cooperará con los clientes para facilitar investigaciones y análisis forenses, asegurando la protección de la evidencia.

Esta política se encuentra alineada con las políticas generales de la compañía, es revisada anualmente o cuando se produzcan cambios significativos en el entorno tecnológico o de seguridad. Nuestro compromiso es garantizar la seguridad de la información y la confianza de nuestros clientes.

En Riudoms, a 29 de enero de 2025

Carles Castilla
Consejero delegado