SEGURIDAD DE LA INFORMACIÓN - NEWSLETTER

Ciberseguridad: Tu mejor defensa comienza aquí

En Kushki, sabemos que la confianza es la base de cada transacción, y por eso, nos comprometemos a mantenerte siempre un paso adelante frente a las amenazas de seguridad.

En un mundo digital que evoluciona constantemente, la ciberseguridad es una práctica diaria que nos involucra a todos. Por eso, hemos creado este boletín de seguridad: para brindarte la información, herramientas y conocimientos necesarios para proteger tu negocio y tus clientes de manera efectiva.

Cada mes, compartiremos contigo las últimas noticias y consejos prácticos para fortalecer tus defensas digitales. Nuestra meta es transformar la seguridad en una parte natural de tu operación, para que puedas enfocarte en lo que mejor sabes hacer: crecer tu negocio.

Newsletters 2026:

Enero:

🔐 Seguridad en cada acceso

La seguridad de nuestras oficinas es responsabilidad de todos.

> 🧍 **Acceso uno por uno:** cada persona debe registrarse individualmente con el biométrico.
>
> 🔐 El **control biométrico es obligatorio** en todas las sedes y accesos habilitados.
>
> 🚫 **No** ingreses en grupo ni permitas el acceso a otros sin registro.
>
> 🚪 **No** dejes la puerta abierta bajo ninguna circunstancia.
>
> 🧍 **Visitas:** regístralas, entrégales gafete y **no permitas que circulen solas**.
>
> 📦 **No entregues documentos u objetos** sin validar identidad y autorización.
>
> 📣 **Reporta** accesos sin registro, personas sin identificación a tu Office Manager, Seguridad de la Información o RR. HH.

👉 Cada control de acceso protege a las personas, la información y los activos de Kushki.

Febrero:

Seguridad de la Información

🔐 La seguridad de nuestras oficinas es responsabilidad de todos.

- **Acceso individual:** cada persona debe registrarse en el biométrico.
- **Control biométrico obligatorio:** aplica en todas las sedes y accesos habilitados.
- **Prohibido ingresar en grupo** o permitir el acceso sin registro.
- **No dejar puertas abiertas** bajo ninguna circunstancia.
- **Visitas:** registrar, entregar gafete y acompañar en todo momento.
- **Documentos u objetos:** validar identidad y autorización antes de entregar.
- **Reportes:** informar accesos sin registro o personas sin identificación al Office Manager, Seguridad de la Información o RR. HH.

Marzo:



Grandes logros

- **Chugchukara Services** y **Kushki Operadora** ya son **ISO/IEC 27001:2022** — con esto, Kushki opera bajo el mismo estándar internacional de seguridad en EC, MX, COL, PE y CL.





- **Renovamos la certificación PCI PIN**, ahora 100% sobre AWS Payment Cryptography. Seguimos cumpliendo los más altos estándares en seguridad criptográfica y protección de PINs.



Abril:

Seguridad de la Información

Es importante saber identificar un correo sospechoso no es opcional.

¿Correo sospechoso? Busca estas señales: urgencia artificial · dominio alterado · enlace dudoso · adjunto inesperado · piden contraseña · tono extraño.

No toques nada — no respondas, no hagas clic, no descargues adjuntos.

Repórtalo usando el botón "Reportar Phishing" o escribe a seguridad@kushkipagos.com.

¿Ya interactuaste?

Clic o datos ingresados → cambia contraseña y revisa MFA.

Adjunto ejecutado → desconéctate de la red y contacta a Seguridad de la Información de Kushki al correo seguridad@kushkipagos.com.

Mayo:



Seguridad de la Información

El acceso a la **IA en Kushki** potencia nuestra productividad, pero también exige responsabilidad. Para aprovecharla al máximo sin correr riesgos, sigamos estas reglas de oro en nuestro día a día:

Comparte únicamente la información necesaria para realizar la tarea. Evita exponer datos sensibles sin justificación.

No ingreses credenciales, tokens o accesos dentro de prompts o conversaciones.

Verifica siempre las respuestas generadas por IA. La IA puede entregar información incorrecta, incompleta o desactualizada.

Revisa el contenido antes de reutilizarlo o compartirlo. Asegúrate de que no incluya información sensible o errores.

No uses herramientas no autorizadas para procesar información corporativa.

Mantén criterio profesional y pensamiento crítico. La IA es un apoyo, no reemplaza validaciones técnicas, legales o de seguridad.

Newsletters 2025:

Enero:

🛡️ Protege tus datos: Pishing



El phishing es una de las formas más comunes de fraude en línea, representando un riesgo significativo para la seguridad de usuarios y empresas. Protege tus datos siguiendo estas recomendaciones:

- ✅ **Verifica la dirección de correo:** Antes de confiar en un mensaje, revisa cuidadosamente la dirección de correo o los enlaces incluidos. Los atacantes suelen usar direcciones que imitan a personas o entidades legítimas.
- 🚫 **Evita abrir enlaces o archivos sospechosos:** Los mensajes de phishing suelen incluir contenido alarmante o tentador para persuadirte a hacer clic en enlaces o descargar archivos maliciosos. Si tienes dudas, no interactúes con el mensaje y repórtalo al equipo de seguridad.
- 🔃 **Mantén tu software actualizado:** Asegúrate de que todos tus dispositivos, como computadoras, teléfonos y tablets, cuenten con las actualizaciones más recientes de su sistema operativo y aplicaciones. Estas actualizaciones incluyen parches de seguridad que corrigen vulnerabilidades.

La prevención y la vigilancia son tus mejores herramientas para evitar caer en estos ataques. Proteger tus datos está en tus manos.

Si recibes un correo sospechoso, **repórtalo inmediatamente** al correo electrónico **seguridad_kushki@kushkipagos.com** 📧.

Febrero:

🛡️ ISO 27001: Seguridad y Confianza

Contar con la certificación **ISO 27001** no sólo refuerza nuestra protección de datos, sino que también nos ayuda a cumplir con las normativas locales y generar confianza con nuestros clientes y aliados.

¿Qué beneficios aporta?

- ✅ **Seguridad reforzada** – Mitigamos riesgos y prevenimos brechas de seguridad.
- ✅ **Cumplimiento normativo** – Aseguramos el cumplimiento de leyes de protección de datos.
- ✅ **Mayor confianza** – Protegemos nuestra reputación y generamos credibilidad.
- ✅ **Ventaja competitiva** – Nos destacamos con estándares de seguridad reconocidos.
- ✅ **Eficiencia interna** – Mejoramos procesos y fomentamos la cultura de seguridad.

Con esta certificación, seguimos fortaleciendo nuestra seguridad y liderazgo en la industria. *¡Sigamos protegiendo nuestra información!.* 🤝

Marzo:

💪 ¡Logramos la Certificación ISO 27001:2022!





Nos enorgullece compartir que logramos la **recertificación en ISO 27001:2022**, el estándar internacional que garantiza la protección de la información. 🌟

Este logro refleja nuestro compromiso continuo con la **seguridad, la confianza y la innovación**, asegurando la **integridad, confidencialidad y disponibilidad** de los datos, tanto nuestros como de nuestros clientes.

SI - CER908618

📅 Certificación vigente hasta 2028

La recertificación ISO 27001:2022 estará vigente hasta **febrero de 2028**, con **auditorías anuales de mantenimiento** para asegurar su cumplimiento continuo. ✅ Estas auditorías podrán realizarse **de forma presencial** en nuestras cinco sedes certificadas: ***México, Colombia, Ecuador, Perú y Chile***.

Para fortalecer nuestro compromiso con la seguridad, el equipo de **Seguridad de la Información** realizará **revisiones periódicas internas** para verificar la correcta implementación de los controles. 🛡

Agradecemos el esfuerzo de todos los equipos involucrados en este proceso, que cada vez exige más y nos impulsa a seguir mejorando 🚀

Abril:

Con esta iniciativa continuamos posicionando a **Kushki como líder en pagos electrónicos en LAC** mostrando nuestra amplia experiencia para:

> 🤝 Mejorar la experiencia de compra del cliente final
>
> ✅ Optimizar las tasas de aceptación
>
> 🛡️ Fortalecer la seguridad y prevenir el fraude
>
> ⚙️ Hacer más eficiente la gestión de contracargos
>
> 📉 Reducir costos operativos

Mayo:

🔒 Certificación PCI DSS lograda



Nos alegra contarles que **Kushki alcanzó la certificación en la versión 4.0.1 del estándar PCI DSS**, el referente global en seguridad para el manejo de datos de tarjetas de pago. 🖤

Este hito refleja nuestro compromiso con la protección de la información, la confianza de nuestros clientes y el cumplimiento de los más altos estándares internacionales. 🚀

Reconocemos al **equipo de Seguridad de la Información** por liderar este proceso con excelencia y dedicación. 👏

Junio:

🔐 Tu rol en la ciberseguridad

Reforcemos juntos estas prácticas clave para proteger nuestra información:

- 🔓 **Activa la biometría** al ingresar a la oficina.
- 💻 **Verifica que tu equipo esté inventariado** (revisa la etiqueta debajo del portátil).
- ☁️ **No guardes archivos en el escritorio local**; usa rutas oficiales o la nube.
- 🔒 **Bloquea tu pantalla** al alejarte de tu puesto.
- 🚫 **No instales software sin autorización de TI**.
- 🔑 **Usa contraseñas seguras y únicas** + activa el doble factor (2FA).
- 📩 **No abras correos ni archivos de remitentes desconocidos**.
- 📶 **Evita el Wi-Fi público**; usa red segura o VPN.
- 🗄️ **Guarda documentos físicos bajo llave**.
- 🛑 **Reporta cualquier incidente o actividad sospechosa**.

Cada pequeña acción suma a la seguridad de todos.
¡Contamos contigo! 🤝

Julio:

🆘 Pérdidas o robos: ¿Qué hacer?

💻 Si perdiste o te robaron tu **computadora o celular con accesos corporativos**, **actúa de inmediato** para proteger la información de la empresa.

1. 📣 Reporta de inmediato a tu líder y a 👉 *serviciosti@kushkipagos.com.*
2. 📝 Denuncia el hecho ante las autoridades en menos de 24 horas.
3. 📄 Envía un informe (máx. 72 horas) a tu líder y a TI

📚 Este proceso se respalda por el documento **STI-FO-0303-KU – Carta Responsiva**. Consulta el manual aquí 👈.

¿Perdiste o robaron tu tarjeta de acceso?

1. 🚪 Informa de inmediato a la Office Manager.
2. 🔒 Se bloqueará la tarjeta para evitar accesos no autorizados.

¡Actuar rápido protege nuestros datos y a todo el equipo!.

Agosto:

🦠 Evita riesgos digitales

Existen muchos tipos de **ataques digitales** que pueden comprometer tu información personal y corporativa 🚨. Estos son algunos de los más comunes y cómo protegerte:

- ⚡ **Día Cero** → Actualiza tu sistema y usa antivirus autorizado.
- 🌐 **DDoS** → Evita redes inseguras y protege tu conexión.
- 🦠 **Ransomware/Malware** → Haz backups y no abras archivos sospechosos.
- 🎣 **Phishing** → No compartas contraseñas ni hagas clic en enlaces dudosos.
- 🕵️ **Man in the Middle** → Evita Wi-Fi públicas y mantén todo actualizado.

❗ **Reglas de oro:**

> ✔️ Contraseñas fuertes + 2FA
> ✔️ No instales software no autorizado
> ✔️ Actualiza tu equipo
> ✔️ Haz respaldos frecuentes

🤝 **Protégete y protege a Kushki: la ciberseguridad está en tus manos.**

Septiembre:

💻 Uso responsable de nuestros equipos

👉 Tu laptop y credenciales son **solo para el trabajo**. Úsalas bien y mantenemos todos la seguridad 💪

🚫 **Evita:**
❌ Usarla para cosas personales
❌ Instalar apps no autorizadas
❌ Repetir tus contraseñas en otros sitios

✅ **Hazlo siempre:**
✔️ Solo uso laboral
✔️ Protege y no compartas tus claves
✔️ Reporta a TI/Seguridad si algo raro pasa

> 🌟 **Tip del mes:** Activa el doble factor de autenticación (2FA), usa contraseñas únicas y olvídate de los papelitos pegados en tu escritorio.

📚 Si quieres más detalles, revisa las **Políticas de Seguridad** y de **Activos Tecnológicos.**

Octubre:

🔐 Cultura Segura en Acción

> 💻 **Tu equipo es tu responsabilidad:** bloquéalo al levantarte, guárdalo si sales, evita cables sueltos o líquidos cerca y mantenlo siempre bajo supervisión.

> 🧍‍♀️ **Si recibes visitantes:** acompáñalos en todo momento, solicita y verifica su gafete y reporta a cualquier persona sin identificación.

> 🏢 **En la oficina:** registra tu ingreso, no dejes puertas abiertas, usa tu gafete visible y comunica cualquier daño o situación sospechosa.

🤝 **Seguridad física y digital van juntas.** Cuidar tu entorno es proteger a todo Kushki.

Noviembre:

🏷️

Etiqueta, protege, previene

Al compartir información o documentos con otras áreas internas o externas (clientes, entes reguladores o auditorías), **asegúrate de etiquetarlos** según su nivel de clasificación *(Confidencial, Restringido, Uso Interno o Público)*. El etiquetado protege la información sensible y evita fugas, accesos no autorizados, sanciones o daños a la reputación de la compañía.

Estas son algunas recomendaciones:

Tipo de Información	Acciones a Seguir de Etiquetado
📄 **Información física**	• Rotula los documentos según su nivel de confidencialidad. • Si los documentos están archivados, rotula la carpeta con la clasificación correspondiente. • Si manejas información confidencial dentro de las oficinas de Kushki, guárdala bajo llave en espacios seguros y visibles por el sistema de CCTV. • Gestiona adecuadamente el uso de las llaves para el resguardo de la información física y garantiza su debido respaldo y control.
💻 **Información digital**	• Antes de compartir cualquier archivo, verifica que esté correctamente etiquetado. • Si un documento no tiene etiqueta, trátalo como confidencial hasta confirmar su clasificación.

📘 **Consulta cómo hacerlo** en el *Instructivo RC-IN-0306-KU* y el *Manual SRC-MA-0303-KU*, disponibles en el **Gestor Documental** de la compañía.

Diciembre:

🏷️ Clasificar la información protege a Kushki

Clasificar la información es clave para proteger a la compañía: **reduce riesgos, previene fugas y evita accesos indebidos**. Todo documento, físico o digital, debe manejarse según su **nivel de sensibilidad**.

Nivel	Significa:	Úsalo para:
🔴 **Confidencial**	Información altamente sensible que requiere máxima protección.	Datos personales o financieros, llaves criptográficas, contratos, información estratégica o de clientes.
🟠 **Restringida**	Información interna crítica cuya exposición afecta la operación.	Procesos del negocio, infraestructura, arquitectura, código fuente, ambientes productivos.
🟡 **Uso Interno**	Información destinada exclusivamente a colaboradores de Kushki.	Políticas internas, manuales, procedimientos, reportes y comunicaciones internas.
🟢 **Pública**	Información apta para compartirse libremente sin restricciones.	Material comercial, sitio web, campañas y contenido informativo externo.

> 🚩 **¿Por qué es clave?:** Evita accesos no autorizados y filtraciones, Permite aplicar controles de seguridad efectivos, Reduce riesgos legales y reputacionales y Garantiza cumplimiento con **ISO 27001, PCI DSS** y **normativas de datos.**

📘 **Conoce cómo hacerlo correctamente:** *SRC-MA-0303-KU – Identificación* y *Clasificación de Activos de Información*
Disponible en el repositorio de políticas de seguridad.