POLÍTICA INTEGRAL DE SEGURIDAD DE LA INFORMACIÓN

JHARDSYSTEX SAC | RUC: 20605917421

I. DECLARACIÓN DE GOBERNANZA

JHARDSYSTEX SAC, en su compromiso con la excelencia tecnológica y la protección de los activos digitales de sus clientes, establece la presente política basada en los estándares internacionales **ISO/IEC 27001** y **NIST**. Reconocemos que la información es el activo más crítico y, por tanto, su protección es una responsabilidad principal por toda la organización.

II. DESARROLLO DE LOS PILARES ESTRATÉGICOS

01. Gestión de Riesgos y Activos Críticos

Nuestra metodología no es reactiva, sino preventiva.

- **Identificación:** Clasificamos cada activo de información (bases de datos SAP, configuraciones de red, logs de auditoría) según su criticidad.
- **Protección de Propiedad Intelectual:** Aplicamos controles específicos para salvaguardar el conocimiento estratégico y la arquitectura de sistemas de nuestros clientes, garantizando que el acceso sea exclusivo para el cumplimiento de los servicios contratados.
- **Análisis de Impacto:** Evaluamos constantemente las amenazas emergentes (Ransomware, Phishing) para ajustar nuestras defensas de manera proactiva.

02. Seguridad en el Control de Accesos (Acceso Lógico)

El acceso a la información se rige bajo el principio internacional de **"Mínimo Privilegio"**.

- **RBAC (Role-Based Access Control):** El personal técnico solo accede a los recursos estrictamente necesarios para su función técnica.
- **Autenticación Robusta:** Implementamos protocolos de autenticación de múltiples factores (MFA) en todos los nodos de administración de infraestructura local y cloud (AWS, Azure, OCI).
- **Monitoreo Perimetral:** Contamos con sistemas de detección de intrusos que monitorean intentos de acceso no autorizado 24/7, generando alertas inmediatas a la Gerencia de TI.

03. Integridad y Criptografía de Grado Empresarial

Garantizamos que la información no sea alterada desde su creación hasta su disposición final.

- **Cifrado en Reposo y Tránsito:** Utilizamos estándares de cifrado **AES-256** para datos almacenados y protocolos TLS para información en movimiento.
- **Validación de Integridad:** Realizamos auditorías de integridad mediante mecanismos de *hashing* para asegurar que los registros y backups no hayan sufrido modificaciones malintencionadas o accidentales.

04. Marco de Cumplimiento Normativo, Legal y Ético

JHARDSYSTEX SAC opera bajo un modelo de gobernanza que trasciende el servicio TI, integrando controles legales y normativos para blindar la continuidad del negocio y la integridad de la información, las cuales son:

- **Cumplimiento Legal y Privacidad:** Nuestras operaciones se ejecutan bajo el marco estricto de la **Ley N° 29733 (Ley de Protección de Datos Personales)** y su Reglamento, garantizando el tratamiento lícito de la información. Asimismo, nos alineamos a la **Ley N° 30096 (Ley de Delitos Informáticos)** para la prevención de accesos no autorizados y protección de la infraestructura crítica.
- **Gestión de la Continuidad y Resiliencia (ISO 22301):** Implementamos protocolos de recuperación para asegurar la restauración de los servicios en tiempos críticos (**RTO/RPO mínimos**). Este estándar garantiza que, ante eventos disruptivos, el impacto operativo sea mitigado de manera sistemática.
- **Gobernanza de Seguridad de la Información (ISO/IEC 27001):** Utilizamos este marco internacional para la gestión integral de riesgos, asegurando que cada control técnico se audite y actualice conforme a las amenazas emergentes del sector IT.
- **Seguridad en Operaciones de Campo (ISO 45001):** Como parte de nuestra responsabilidad operativa, garantizamos que el despliegue técnico en sedes de clientes cumpla con los estándares de **Seguridad y Salud en el Trabajo**, asegurando una ejecución libre de riesgos laborales y operativos.
- **Cultura de Seguridad y Ética Digital:** El factor humano es gestionado como un activo crítico de seguridad. Todo el personal es capacitado bajo lineamientos de ética profesional y protocolos de respuesta ante incidentes, minimizando el riesgo de vulnerabilidades por ingeniería social.

III. COMPROMISO DEL PERSONAL

Todo colaborador de JHARDSYSTEX SAC suscribe Acuerdos de Confidencialidad (NDA) y se somete a capacitaciones constantes en ciberseguridad defensiva y detección de ingeniería social.

IV. APROBACIÓN Y VIGENCIA

Esta política es de cumplimiento obligatorio para todos los colaboradores de JHARDSYSTEX SAC y terceros vinculados.

BARUC JOAQUIN GARCIA
GERENTE GENERAL JHARDSYSTEX