Hungry-UP  
Políticas de Sistemas de la Información

**Política de Seguridad de Datos:**

1. Acceso a la Base de Datos: Solo el personal autorizado tendrá acceso a la base de datos de Django. Se deben establecer niveles de acceso y autenticación segura para proteger los datos sensibles.
2. Cifrado de Datos: Todos los datos sensibles almacenados en la base de datos deben cifrarse tanto en reposo como en tránsito utilizando protocolos seguros.
3. Política de Contraseñas: Se deben implementar políticas de contraseñas sólidas que requieran contraseñas complejas, cambios periódicos de contraseña y la prohibición de compartir contraseñas.

**Política de Respaldo y Recuperación:**

1. Frecuencia de Respaldos: Los datos críticos del sistema, incluyendo la base de datos, deben respaldarse regularmente de acuerdo con la frecuencia establecida en el plan de respaldo.
2. Almacenamiento de Respaldos: Los respaldos deben almacenarse en ubicaciones seguras, preferiblemente en servicios de almacenamiento en la nube con cifrado de datos.
3. Pruebas de Restauración: Se deben realizar pruebas periódicas de restauración para garantizar que los respaldos sean funcionales y los datos se puedan recuperar correctamente.

**Política de Acceso y Control de Usuarios:**

1. Roles y Permisos: Los usuarios del sistema deben tener roles y permisos asignados adecuadamente para limitar el acceso solo a las funciones y datos necesarios para sus responsabilidades.
2. Monitoreo de Acceso: Se debe implementar un sistema de registro y monitoreo de acceso para detectar y registrar cualquier actividad inusual o no autorizada.

**Política de Desarrollo y Mantenimiento:**

1. Control de Versiones: Todo el código fuente del proyecto Django debe gestionarse utilizando un sistema de control de versiones como Git.
2. Pruebas de Seguridad: Antes de implementar nuevas funcionalidades o cambios en el sistema, se deben realizar pruebas exhaustivas de seguridad para identificar y corregir vulnerabilidades.

**Política de Cumplimiento Normativo:**

1. Cumplimiento Legal: El proyecto debe cumplir con todas las leyes y regulaciones aplicables, como las relacionadas con la protección de datos y la privacidad del cliente.
2. Documentación y Auditoría: Debe llevarse un registro de todas las políticas, procedimientos y auditorías de seguridad realizadas para garantizar el cumplimiento continuo.