Cardinal
Paperless experts

Manifiesto de Seguridad de accesos

Cardinal Systems se compromete a otorgar al cliente una auditoría total de los registros consultados, así como monitoreo en tiempo real de nuestras bases de datos.

Además, nos comprometemos a eliminar de forma segura aquellos documentos o archivos que ya no sean útiles para la empresa al ofrecer la descarga previa del contenido. La eliminación de datos innecesarios se garantiza en un periodo de 90 dias conforme a la normativa vigente.

Estamos en un proceso de mejora continua con estándares compatibles con la norma GDPR, por esta razón ofrecemos al cliente control total y auditoría sobre sus archivos además de cifrar los archivos de todas las bases de datos.

Además, en nuestra base relacional, todas las contraseñas están encriptadas.

Desde Azure, la administración de contraseñas está centralizada en los administradores que acceden a la plataforma solo con token.

Las credenciales para acceder a las bases de datos y otros entornos son administradas por los administradores asignados y el cambio de contraseña es obligatorio cada 15 días, respetando políticas de longitud, complejidad e identificación de dispositivo desde donde se realiza el SSO.

Todos los errores al ingresar la contraseña o los intentos de inicio de sesión se registran en la auditoría de las aplicaciones web y en Azure, de este modo se pueden prevenir ataques por fuerza bruta reiterada.

Usamos Microsoft Azure para alojar y monitorear nuestros entornos y aplicaciones, pero el control y la ejecución de los procesos no se tercerizan, somos responsables y los únicos que accedemos a los datos.

Además, los usuarios que pueden ingresar son auditados, registrados y acceden al sistema solo con doble autenticación utilizando un dispositivo previamente registrado en sincronización con Azure AD.

Si alguien logra acceder a la base de datos, no podrá ver un archivo completo sin conocer la ubicación, la contraseña y el nombre de código de todas las réplicas y particiones que conforman todo el sistema de datos que no son SQL.

Todas las auditorías de nuestras aplicaciones, servidores y entornos están automatizadas. Tenemos control del nivel de registro y realizamos copias de seguridad de todos los registros dentro del proceso BK de las máquinas virtuales.

Los clientes no pueden ver los Ips, pero podemos rastrear el origen de la solicitud desde el firewall de Azure.

También tenemos registros de auditoría segmentados por cada API, entorno y sitio.

Utilizamos la conexión a través del protocolo RDP con seguridad de "" acceso justo a tiempo "".

El acceso a través de RDP solo es posible desde el portal y de forma segura por Token; Solo los usuarios registrados con permisos suficientes pueden ingresar a través de RDP con doble validación de dispositivo de PC.

Además, implementamos Azure Key Vault, con lo cual no necesitamos aprovisionar, configurar, parchear y mantener HSM y software de administración de claves sensibles a ataques externos.