SISTEMA INTEGRADO PIMS – CT8016

La solución CT8016-PIMS fue diseñada teniendo en cuenta la sensibilidad de la información que almacena e intercambia y con el fin de garantizar esta premisa fue sometida a auditorias de empresas consultoras quienes realizaron varios test para verificar su seguridad. En todos los casos se obtuvieron las aprobaciones correspondientes.

Acceso web seguro:

- Inicio de sesión usando nombre de usuario y clave. Las claves tienen que cumplir con las políticas de seguridad especificados por las herramientas administrativas de PIMS.
- Las claves son almacenadas en la Base de datos usando encriptación MD5.
- Teclado virtual para iniciar sesión en el sitio web cuando los usuarios utilizan PC's de acceso público.
- Acceso via HTTPS usando certificado.
- las aplicaciones web sólo tienen acceso de sólo lectura a la base de datos.

Seguridad en equipos CT8016:

- Sistema operativo Linux embedded.
- Bloqueo de todos los puertos entrantes en el sistema operativo, salvo requerimiento de específico del cliente; lo que impide el acceso externo a los datos almacenados en el equipo CT8016.

Transmisión de información:

La información que se intercambia entre el cliente y el servidor viaja encriptada y provee un alto grado de confidencialidad. Es importante la confidencialidad en todo tipo de transacciones ya que todos los datos enviados por un canal encriptado con SSL se encuentran protegidas por medio de un mecanismo para detectar la manipulación o alteración de alguno de los datos de la información.

- Los datos intercambiados entre el equipo CT8016 y la plataforma PIMS se envían encriptados a través de SSL (Secure Socket Layer).
- Cifrado de datos utilizado es el AES con 256 bits.
- Clave pública de 1024bits.
- Sistema de login cruzado entre el equipo CT8016 y la plataforma PIMS. Ambos deben loguearse al otro sistema al comienzo de la supervisión, con el objetivo de prevenir falsas identidades.
- las direcciones MAC de los equipos CT8016 son almacenadas y se utilizan para asegurar un método único de login de cada equipo. Si la dirección MAC no coincide con la registrada el equipo CT8016 no puede establecer la comunicación.

Confidencialidad de información:

- La PIMS está compuesta por "*entidades*" (empresas), y organizada por una estructura jerárquica en forma de árbol, donde se van agregando los "*puntos de venta"* (negocios minoristas) y dentro de cada punto de venta están las "*Terminales remotas"* (equipos CT8016)
- Nivel de Acceso por profundidad: cada entidad tiene acceso sólo a su propia información y la información relativa a las entidades de su hijo.
- Los usuarios sólo pueden ver los reportes correspondientes a su perfil de usuario.
- Entidades y usuarios son relacionados con el objetivo de filtrar sólo los puntos de venta a los cuales cada usuario tiene permiso.
- El protocolo de intercambio de información es **nativo** de DELSATGROUP. El protocolo se denomina PTSD y la versión actual es la v1.2

Mecanismos de autenticación, validación e intercambio de información

1. El equipo CT8016, su MAC, el correspondiente punto de venta y la entidad deben ser creados en la plataforma PIMS Administrativa. Para esto se utiliza un escritorio remoto al cual se accede previo establecimiento de la VPN.
2. Luego de instalados los equipos, se deben configurar para que permitan la conexión a la dirección IP de la plataforma web PIMS.
3. SIEMPRE el inicio de la comunicación procede del equipo CT8016. Esto puede deberse a que tiene que enviar alguna información (depósitos, extracciones, alarmas, etc) o bien puede deberse a tareas prefijadas de reporte de status.
4. Antes de cualquier intercambio, se verifica la MAC del equipo, usuario, contraseña. Recién luego de pasado el proceso de autenticación y validación cruzada, puede comenzar el intercambio de información.

Seguridad en aplicación PIMS:

- Prevención de SQL Injection y scripts maliciosos.
- Protección contra XSS (Cross-site Scripting).
- Prevención contra Ataques por fuerza bruta.
- Implementacion de politicas de passwords.
    - Configuración de aging de passwords: Se configura el tiempo de vencimiento de los passwords, el tiempo mínimo para poder realizar cambio de password, y la cantidad de passwords a utilizar como históricos para evitar repeticiones.
    - Configuración de longitud mínima de password: Se puede podrá establecer cuál es la mínima longitud permitida para un password de usuario.
    - Configuración de nivel de complejidad de password requerido: Se permite especificar el nivel de complejidad requerido al introducir los passwords de los usuarios. Esta configuración obliga al usuario a utilizar contraseñas con mayor grado de complejidad, combinando números, letras y caracteres en

función del nivel seleccionado. Según los valores seleccionados para el password, se evalúa la fortaleza de la contraseña.

- Session Aging: Cierre de Sesión durante cierto tiempo de inactividad: La plataforma PIMS cierra la sesión automáticamente luego de cierto tiempo sin detectar actividad por parte del usuario.

Infraestructura:

- Los servidores están alojados en un Data Center contratado especialmente (collocation service). Esto permite una arquitectura que brinda mayor potencia, mayor redundancia y mejores prestaciones.
- El servidor de base de datos y las aplicaciones de la PIMS son accedidas via Remote Desktop dentro de una VPN.
- Sistema de alimentación ininterrumpida 24/7.
- Paneles de control para monitorear el estado del servidor.
- Posibilidad de notificaciones de sistema via email o sms.
- Protección por medio de un Firewall.
- Servicio de internet dedicado y redundante.