



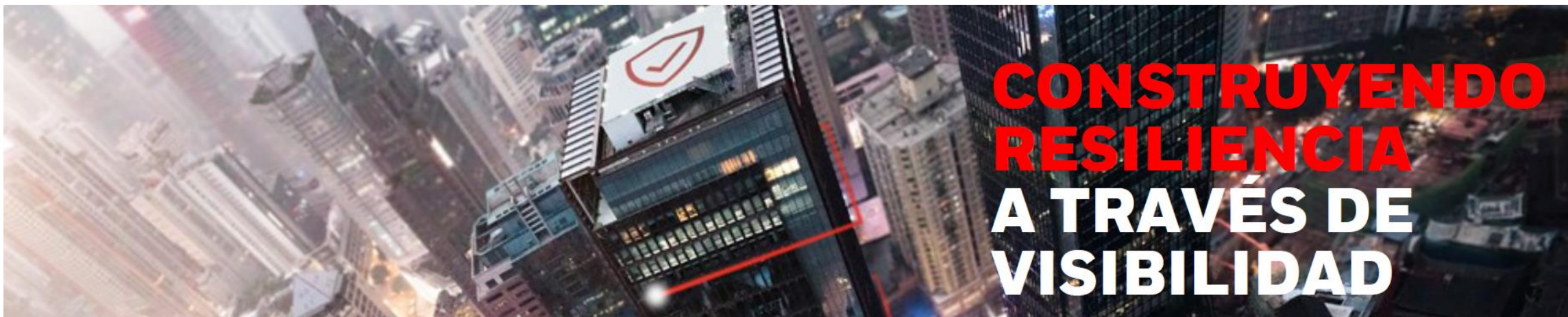
COMISIÓN DE SEGURIDAD PRIVADA DE EXTREMADURA
JORNADAS DE CIBERSEGURIDAD

Diciembre 2022

CUESTIONES SOBRE CIBERSEGURIDAD
APLICACIÓN PRÁCTICA DE LA CIBERSEGURIDAD A LOS
EQUIPOS DE SEGURIDAD ELECTRÓNICA

Honeywell

Santiago García Naranjo
santiago.garcia@honeywell.com
616 761 419



La importancia de la ciberseguridad

A medida que los edificios se vuelven más y más digitales, las organizaciones están abrazando cada vez más la demanda de ambientes conectados y reconociendo su exposición a las amenazas de ciberseguridad. Para ayudar a defenderse de posibles pérdidas financieras o daños a la imagen causados por los ciberataques, se debe implementar una estrategia fuerte de ciberseguridad, que comience con la comprensión de los motivos del atacante y los escenarios de riesgo cibernético.

AGENDA

- General
 - Amenazas de Ciberseguridad
 - Buenos prácticas y costumbres
- Intrusión
 - Cambio de contraseñas de fábrica
 - Actualización de los sistemas a las últimas versiones
- Control de Accesos:
 - Cambio de contraseñas de fábrica
 - Actualización de los sistemas a las últimas versiones
- CCTV:
 - Cambio de contraseñas de fábrica de forma regular
 - Actualización de los sistemas a las últimas versiones
- Softwares de Gestión
 - Tipos de equipos
 - Usuarios y Contraseñas
 - Actualización a la últimas versiones (Acuerdos de Software)
 - Respaldo de la información
 - Soluciones en la nube

POSIBLES AMENAZAS SOBRE LOS SISTEMAS DE SEGURIDAD

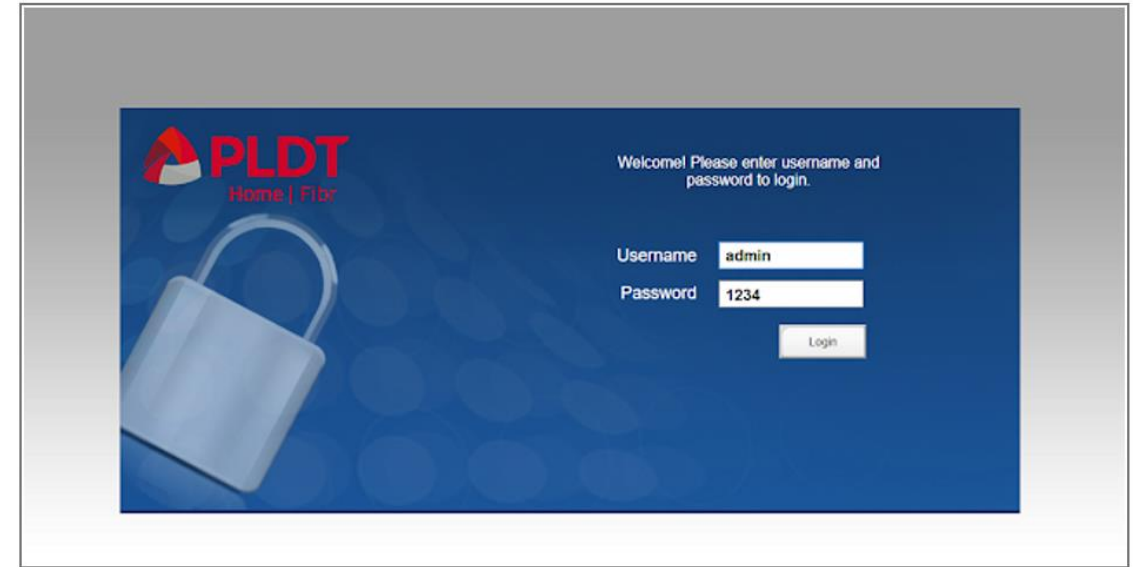
- Acceso no autorizado
 - Modificación de la configuración
 - Modificación de la información:
 - Cambio de contraseñas
 - Interceptación de la información y modificación (MitM)
 - Parada total del sistema
 - Física
 - Lógica
- Acceso no autorizado y/o Infección por Malware, Virus o Ransomware
 - Robo de la Información o extracción no autorizada
 - Secuestro de la información o del sistema
 - Conversión de nuestro sistema en un “Zombie”

APLICANDO LA CIBERSEGURIDAD

BUENAS PRÁCTICAS GENERALES

EQUIPOS DE CAMPO

- El mayor problema de ciberseguridad en nuestro sector, son los equipos instalados con los parámetros por defecto.
 - Cambiar inmediatamente las contraseñas de administrador, no más Admin + 1234
 - Tratar de elegir equipos que obliguen al técnico al cambio de dicha contraseña cuando los arrancan por primera vez, evitara olvidos
 - Que esas contraseñas sean robustas (se puede usar una tipología dependiendo de cada cliente), y que se cambien de acuerdo a un plan preestablecido, de forma regular
 - Asociar cada usuario del equipo a los diversos roles que este admita (Administrador, Supervisor, Operador...etc)
 - Si no dispone de roles predefinidos, crear usuarios para cada acceso necesario al equipo (Cliente, Administrador, Usuario Local, Software Integración...etc)
 - Permite controlar quien accede y que hace
 - Y permite delimitar las capacidades de cada usuario



Please change password.

New Password

Weak Medium Strong

Confirm Password

☐ Don't show this again.

OK Cancel

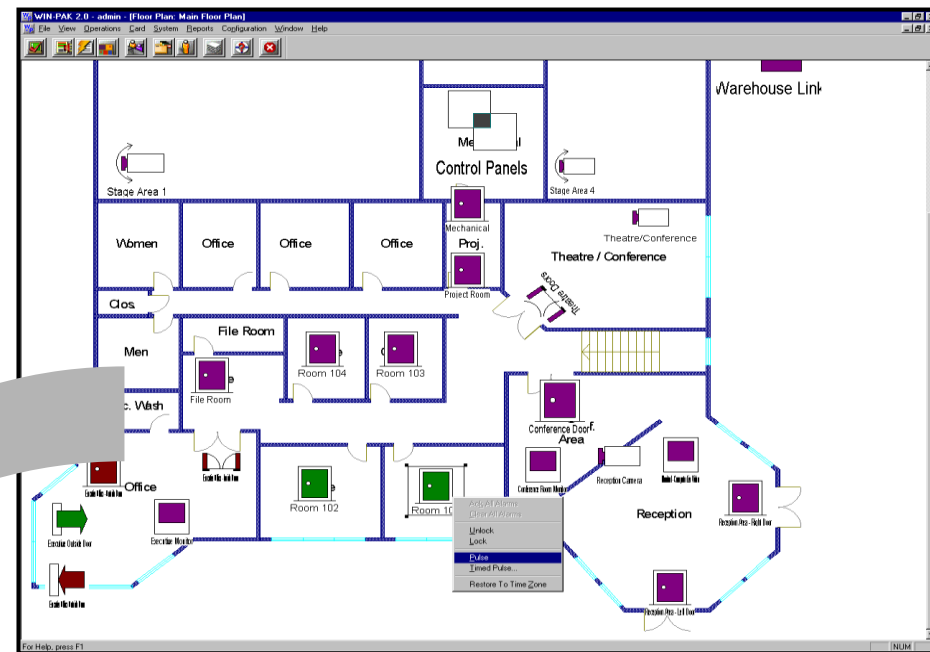
EQUIPOS DE CAMPO

- El segundo mayor problema de ciberseguridad en nuestro sector, son los equipos instalados tal y como venían, con los firmwares de fábrica.
 - Todos los sistemas de origen tienen pequeños bugs, fallas o carencias, que ponen en riesgo la operativa de dichos sistemas
- Los fabricantes invierten una gran suma de dinero en lanzar actualizaciones para cubrir esos problemas o incluso para añadir nuevas funcionalidades.
- Desgraciadamente en nuestro sector, no se acostumbra a mantener los sistemas al día, excepto los de Software
- Por sistema debemos añadir como una rutina más, el revisar todos los firmwares de los equipos de campo, al menos una vez al año (en la visita física de la revisión...), y en el caso de equipos más tecnológicos, como los sistemas de Vídeo IP



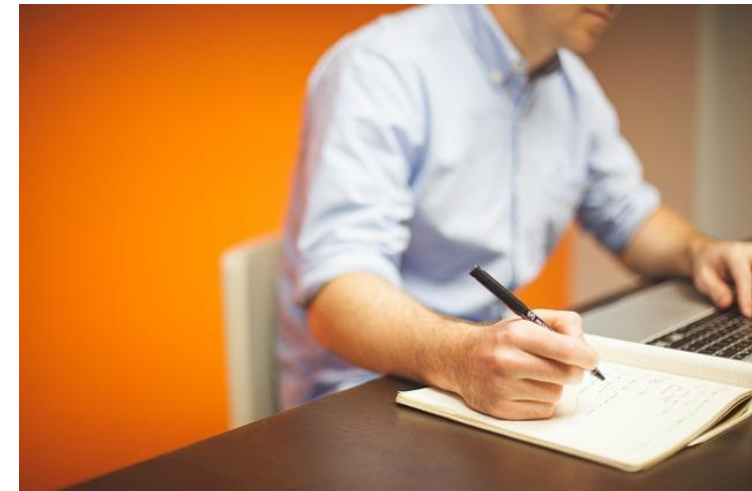
SOFTWARE DE GESTIÓN

- Son el punto más expuesto respecto a la Ciberseguridad en nuestras instalaciones, son la parte más visible del sistema, y aparte, si son Sistemas de Integración, cuando la seguridad de estos sistemas se ve comprometida, puede afectar a todos los equipos de campo.
- Pueden ser solo el software de programación de un equipo de campo, o bien pueden ser sistemas de gestión integral
- A ser posible, utilizar PCs dedicados para los Sistemas de Seguridad, y ya como sistema casi perfecto, en nuestras propias redes exclusivas para seguridad.
 - En dichos PCs, bloquear el uso de los dispositivos de Entrada de Datos, como Unidades DVD o USB.
 - Cerrar todos los puertos no necesarios para nuestros sistemas.
 - Crear en la medida de lo posible, usuarios no administradores para los Operadores del Sistema de Seguridad.
- Si no pueden ser dedicados, valorar el uso de sistemas basados en Web Segura HTTPS
- Dentro del propio soft de seguridad, crear usuarios para cada persona que debe usarlos, con sus respectivos roles.
- Hay que mantener dichos softwares actualizados a la última versión



DOCUMENTAR LAS INSTALACIONES

- Otro de los problemas habituales para la falta de Ciberseguridad es la falta de una correcta documentación de las instalaciones
- Es absolutamente imprescindible documentar todas las instalaciones que se hacen.
 - Inicialmente nos parece una tiempo perdido, o al menos no aprovechado como nos gustaría
 - Pero a posteriori, el tiempo invertido en documentar cada equipo instalado, nos lo ahorraremos con creces cuando nos sea necesario el acceder a estas instalaciones, recuperarlas, darles servicio, o por ejemplo, cuando el técnico que lo monto ha dejado nuestra compañía.
 - Guardar como mínimo los siguientes datos de cada equipo de cada instalación:
 - Fabricante
 - Tipo de equipo
 - Modelo y Accesorios
 - Versión de Firmware
 - Configuración (si se puede salvaguardar)
 - Si no, al menos usuarios y contraseñas
 - Fecha de instalación
 - Técnico que lo instaló

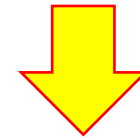


APLICANDO LA CIBERSEGURIDAD

SISTEMAS ANTI INTRUSIÓN

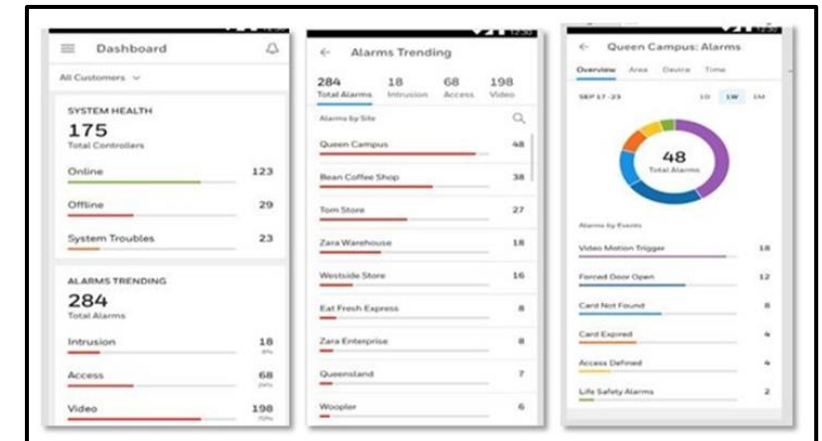
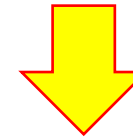
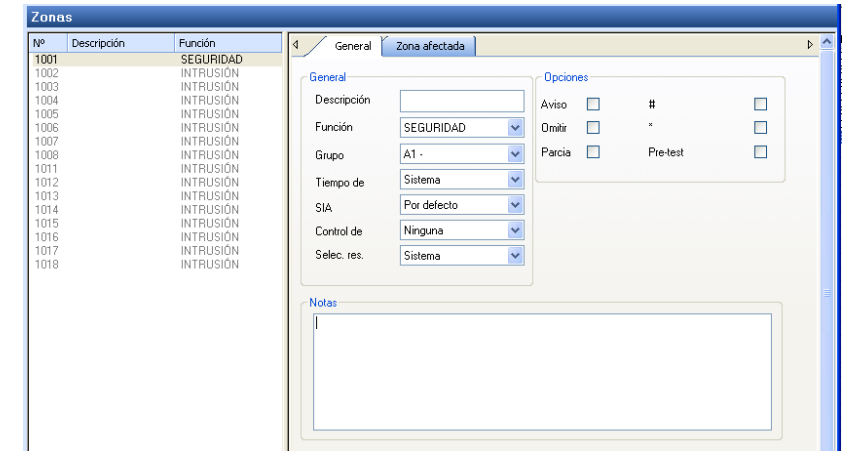
CIBERSEGURIDAD EN LOS SISTEMAS DE INTRUSIÓN

- Los sistemas de Intrusión, son hoy por hoy los más sencillos de los que instalamos en nuestros proyectos, dado que solo se identifican los usuarios por un PIN o en el mejor de los casos, una tarjeta de accesos
- Las vulnerabilidades se dividen en tres:
 - Acceso físico al equipo:
 - Desarmado
 - Modificación de la Configuración
 - Acceso remoto al equipo
 - Desarmado
 - Modificación de la Configuración
 - Acceso a las comunicaciones del equipo
 - Ataque “Man in the Midle”, o sustitución de la información.
- Para evitar en lo posible los ataques a los Sistemas de Intrusión, es absolutamente imprescindible:
 - Identificar (crear) a cada usuario con su propio PIN, nada de usuarios generalizados (como “oficina”, o “vigilantes”)
 - Cambiar todas las contraseñas de fábrica (Ingeniero, usuario remoto...etc)
 - Actualizar regularmente las centrales con el último firmware.
 - Si es posible, seleccionar sistemas con identificación por certificados, y que tengan encriptados tanto comunicaciones internas como externas.



CIBERSEGURIDAD EN LOS SOFTWARES DE INTRUSIÓN

- Aparte de la sencillez de los sistemas de intrusión electrónicos,, debemos tener en cuenta que en la mayoría de marcas ya contamos con softwares de configuración y/o gestión.
- Igual que todos los softwares, esto posiblemente son la puerta más fácil a acceder a los equipos de campo, y por ese motivo debemos protegerlos de la misma forma que a cualquier otro software:
 - Crear usuarios específicos para cada técnico que utiliza el sistema
 - Cambiar las claves por defecto
 - Mantener el software actualizado.
- Siempre que sea posible, pasar a soluciones de gestión encriptadas y con respaldo en servidores externos.

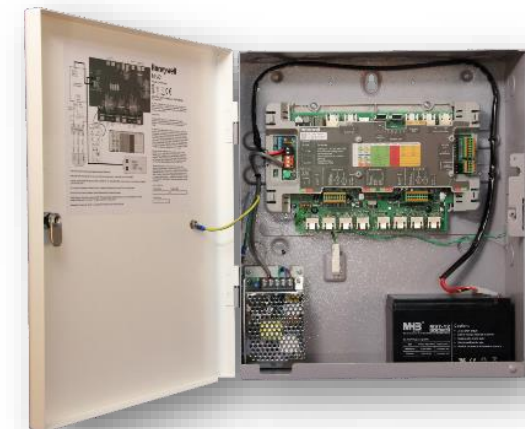
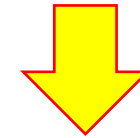


APLICANDO LA CIBERSEGURIDAD

**SISTEMAS DE CONTROL DE
ACCESOS**

CIBERSEGURIDAD EN LOS SISTEMAS DE CONTROL DE ACCESOS

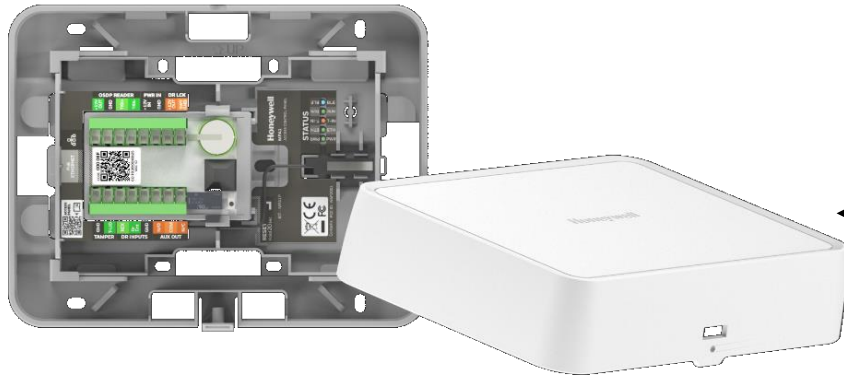
- Los sistemas de Control de Accesos, son los primeros que tuvieron software, por lo que debemos dividir nuestros esfuerzos en dos frentes, el hardware y el software:
- En el caso del hardware tenemos las siguientes vulnerabilidades:
 - Accesos físico al equipo:
 - Poco habitual dado que los equipos no tienen una consola de acceso como las centrales de intrusión.
 - Acceso remoto al equipo
 - Modificación de la Configuración
 - Detención de servicios
 - Acceso a las comunicaciones del equipo
 - Ataque “Man in the Midle”, o sustitución de la información.
- Para evitar en lo posible los ataques a los Sistemas de Accesos, es absolutamente imprescindible:
 - Identificar (crear) a cada usuario con su propia contraseña, nada de usuarios generalizados (como “oficina”, o “vigilantes”)
 - Cambiar todas las contraseñas de fábrica (Ingeniero, usuario remoto...etc)
 - Actualizar regularmente los paneles con el último firmware.
 - Si es posible, seleccionar sistemas con identificación por certificados, y que tengan encriptados tanto comunicaciones internas como externas.



COMPARATIVA ENTRE WIEGAND Y OSDP

WIEGAND

- Comunicación unidireccional (del lector al panel)
- Sin cifrado
- Vulnerable a ataques de hacking man-in-the-middle
- Mínimo 8 hilos y distancia limitada



OSDP

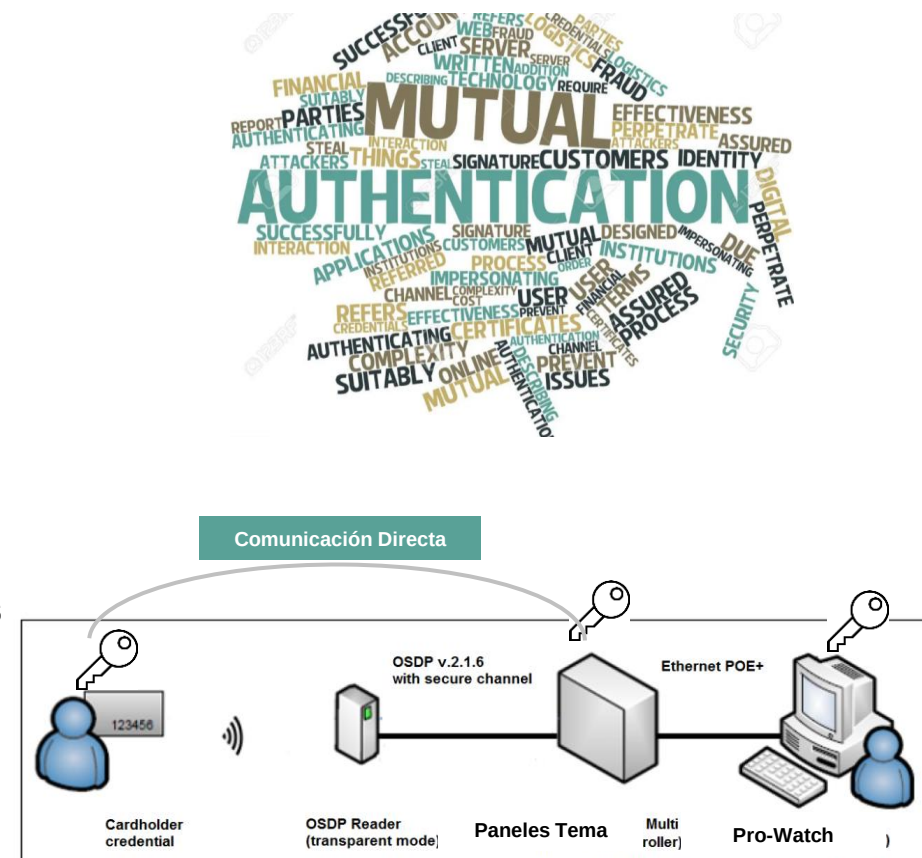
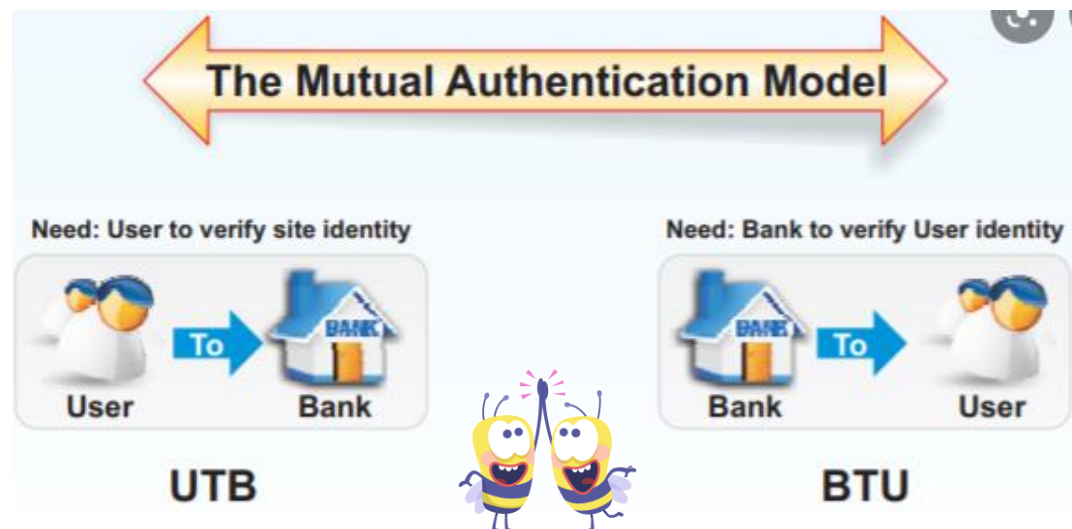
- Comunicación bidireccional entre lector y panel
- Comunicación cifrada (AES128)
- Lazo direccionable RS485 = más lectores, mayor distancia de cableado.
- 4 hilos
- Preparado para el futuro = Características adicionales



AUTENTICACIÓN MUTUA

Los elementos clave de la Autenticación Mutuas son los mismos que le encriptación Punto a Punto:

- **La Tarjeta Smart** (los demás tipos de tarjeta no soportan encriptación)
- El nuevo bus de conexión de lectores **OSDP v2** (Wiegand no soporta encriptación).
- La conexión Ethernet Encriptada **TLS 1.2** Entre el Panel de Accesos y el Software de Gestión
- **Pero eliminamos el riesgo del punto débil en el Lector**
- En la Autenticación Mutua o también llamada “Autenticación de Doble Vía”, las dos partes se autentican entre si al mismo tiempo



En este caso, los lectores son transparentes, no se almacenan claves en los lectores, por lo que eliminamos el único punto de riesgo

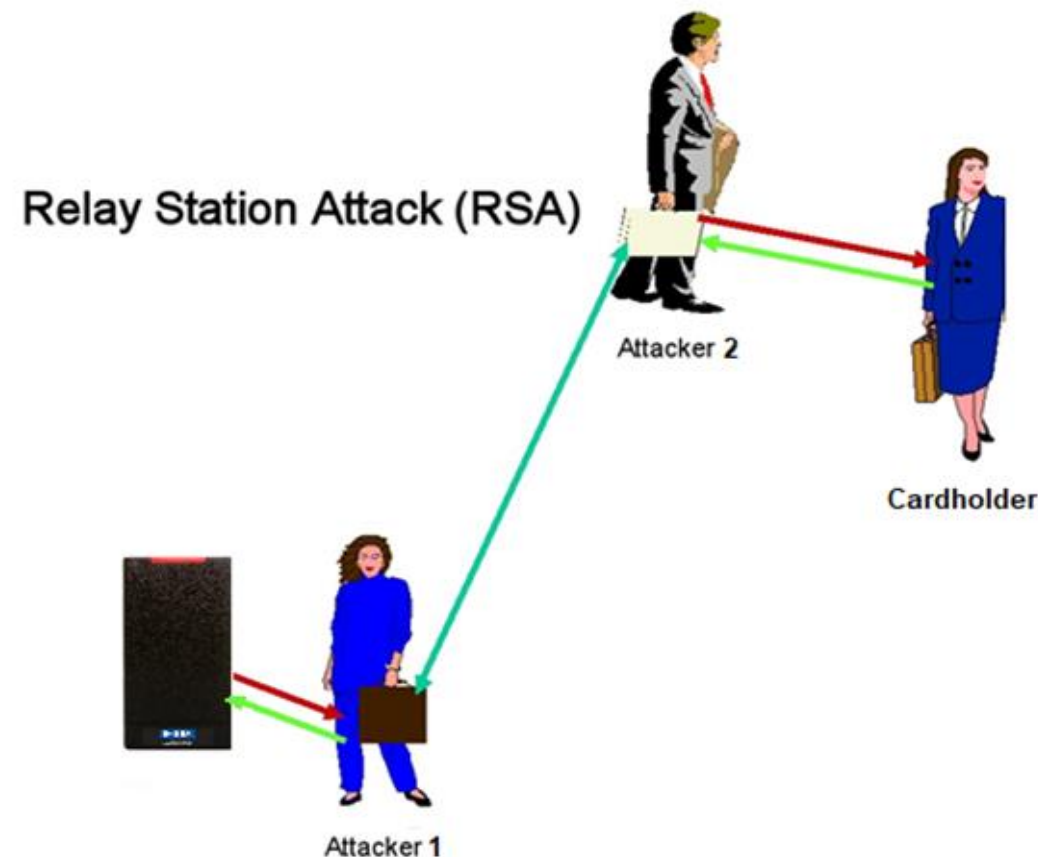
SEGREGACIÓN DE LAS CLAVES POR ZONAS

- Es posible crear varias zonas con diversos niveles de seguridad que usarían distintas claves criptográficas
- Esto asegura que si un área queda comprometida, no afecte al resto de áreas de la instalación



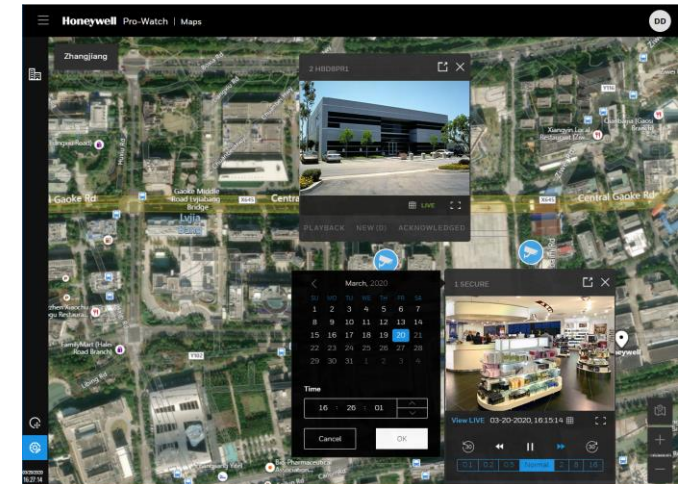
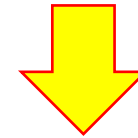
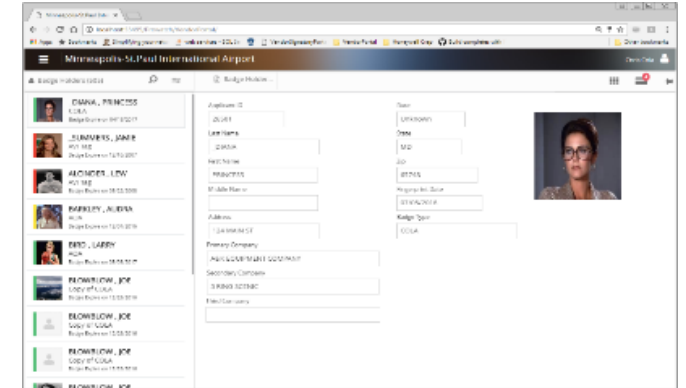
PROTECCIÓN CONTRA “RELAY ATTACK” EN TARJETAS DESFIRE EV.2

- El ataque “Relay Station Attack” se basa en captar la información de la tarjeta del usuario de Control de Accesos sin que se percate, y transmitirla al atacante que quiere utilizarla en una puerta.
- La comprobación de “tarjeta próxima” se utiliza para la detección del intento de “Relay Attack” en el sistema.
- La comprobación de “tarjeta próxima” se basa en la capacidad del sistema para detectar el aumento del tiempo que tarda el sistema en hacer una comprobación contra el panel de accesos.



CIBERSEGURIDAD EN LOS SOFTWARES DE CONTROL DE ACCESOS

- En los softwares de Control de Accesos, debemos seguir las reglas generales que ya hemos comentado anteriormente, porque son la puerta más fácil a acceder a los equipos de campo, y por ese motivo debemos protegerlos de la misma forma que a cualquier otro software:
 - Crear usuarios específicos para cada técnico que utiliza el sistema.
 - Cambiar las claves por defecto.
 - Mantener el software actualizado.
- Siempre que sea posible, pasar a soluciones de gestión encriptadas y con respaldo en servidores externos, como Maxpro Cloud.
- O efectuar copias de seguridad de las Bases de Datos de estos sistemas.



APLICANDO LA CIBERSEGURIDAD

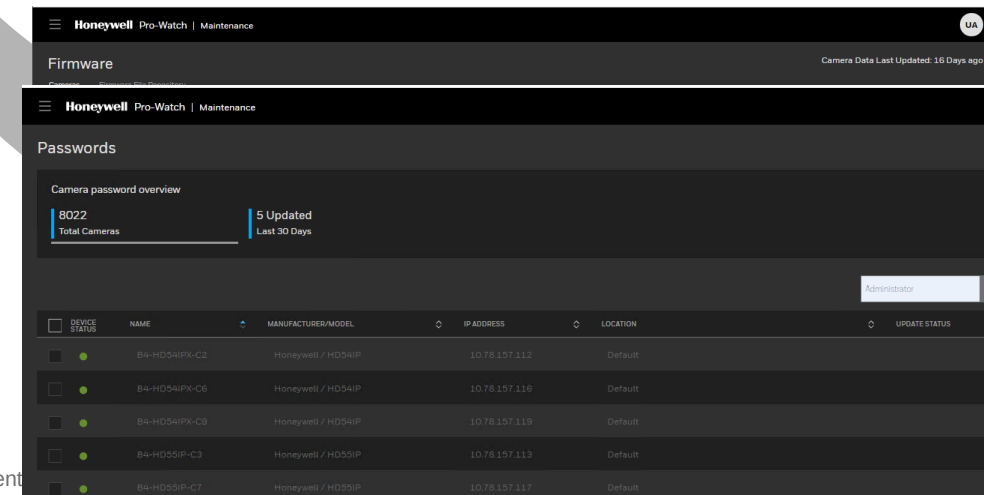
SISTEMAS DE CCTV

CIBERSEGURIDAD EN LOS SISTEMAS DE CCTV

- Los sistemas de CCTV actuales (IP), son probablemente el segundo blanco para los ataques de Ciberseguridad, su complejidad y potencia, permite que se puedan convertir en infiltrados en nuestros sistemas de seguridad.
- Como en el caso del Control de Accesos, debemos dividir nuestros esfuerzos en dos frentes, el hardware y el software, aunque se parecen bastante en cuanto a vulnerabilidades:
- En el caso del hardware tenemos las siguientes vulnerabilidades:
 - Acceso no deseado al equipo:
 - Modificación de la Configuración
 - Detención de servicios
 - Infección del equipo con un Firmware Malicioso, convirtiendo al equipo en un “Zombie” que se puede usar como puente para atacar a otros equipos de la misma red
 - Acceso a las comunicaciones del equipo
 - Ataque “Man in the Midle”, o sustitución de la información.
- Para evitar en lo posible los ataques a los Sistemas de CCTV, es altamente recomendable:
 - Cambiar inmediatamente las contraseña de fábrica para el usuario administrador
 - Identificar (crear) a cada usuario de la cámara (Usuario de conexión desde el grabador, Usuario de Analítica de Vídeo...etc) con su propia contraseña, no utilizar el usuarios “Administrador” para estas funciones
 - Cerrar todos los puertos (FTP...etc) no utilizados de las cámaras
 - Actualizar regularmente las cámaras con el último firmware, semestralmente, o a ser posible trimestralmente.
 - Si es posible, seleccionar sistemas con identificación por certificados, y que encripten los flujos de vídeo así como los metadatos.
 - E igualmente seleccionar sistemas que dispongan de herramientas que permitan automatizar tanto la actualización de firmwares, así como las contraseñas



Honeywell Confidential



CIBERSEGURIDAD EN LOS SISTEMAS DE CCTV

- En el caso de los grabadores, las medidas a tomar, son bastante similares a las de las cámaras:
 - Crear usuarios específicos para cada técnico que utiliza el sistema.
 - Cambiar las claves de “Administrador” por defecto.
 - Crear usuarios con los privilegios adecuados a cada usuario del sistema
 - Cuando añadamos cámaras IP a un grabador NVR, usar un usuario adecuado, a ser posible evitar el “Administrador”, ya que si alguien no deseado accede al grabador, tendrá también las cámaras a su disposición.
 - Mantener el firmware / software actualizado.
- Siempre que sea posible, utilizar equipos que permitan encriptar tanto la configuración y usuarios, así como los flujos de vídeo de las cámaras



CARACTERÍSTICAS DESEADAS DE CIBERSEGURIDAD EN CCTV

NDAA

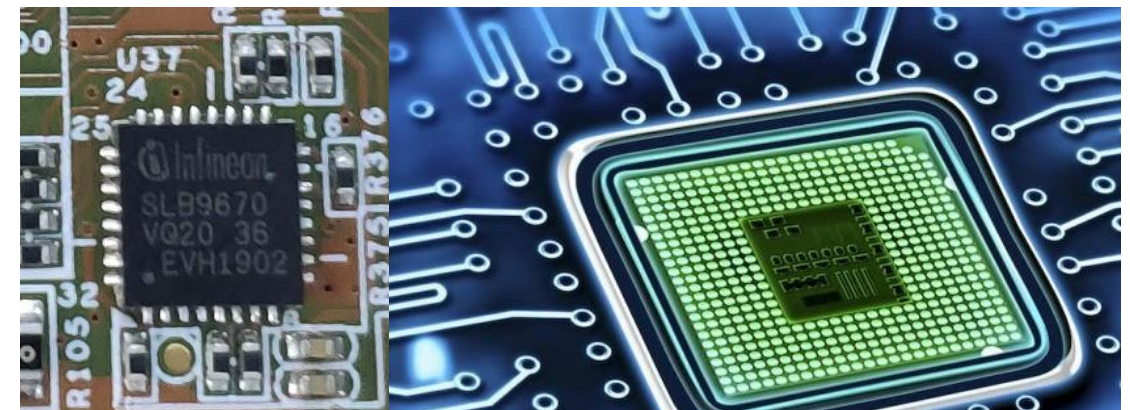
- Cumplimiento de la norma NDAA
- Restringe el material de uso dudoso o bien el que se pueda ver afectado por brechas de seguridad

PCI-DSS

- Incorpora a las cámaras la misma tecnología que usa el segmento del Pago con Tarjeta en sus transacciones

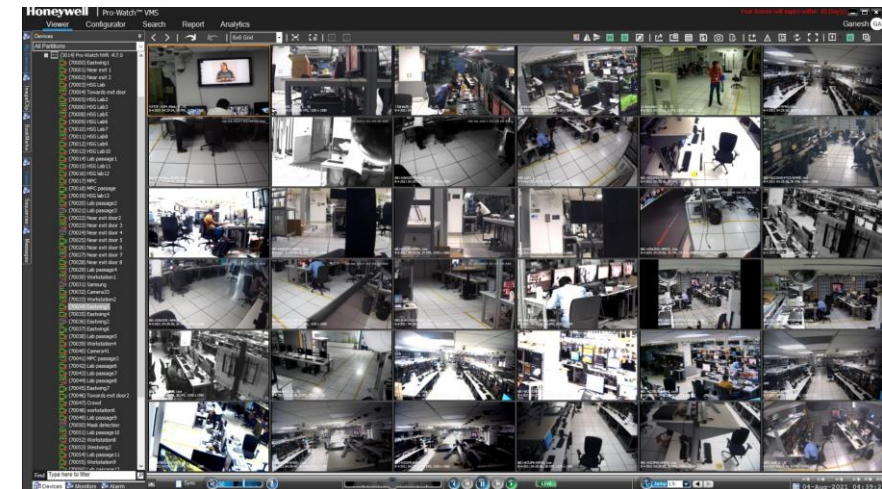
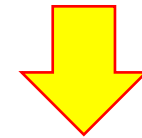
FIPS

- Incorpora en las cámaras chips que efectúan la encriptación de:
- Firmas y firmware
- Encriptación de los flujos de vídeo
- Soporte de encriptación HTTPS en los accesos vía web



CIBERSEGURIDAD EN LOS SOFTWARES DE CCTV

- En los softwares de Control de CCTV, debemos seguir las reglas generales que ya hemos comentado anteriormente, porque son la puerta más fácil a acceder a los equipos de campo, y por ese motivo debemos protegerlos de la misma forma que a cualquier otro software:
 - Crear usuarios específicos para cada técnico que utiliza el sistema
 - Cambiar las claves por defecto
 - Mantener el software actualizado.
- Siempre que sea posible, pasar a soluciones de gestión encriptadas y con respaldo en servidores externos, como Maxpro Cloud.



APLICANDO LA CIBERSEGURIDAD

**SOFTWARES DE PROGRAMACIÓN,
GESTIÓN E INTEGRACIÓN**

SOFTWARE DE PROGRAMACIÓN, GESTIÓN O INTEGRACIÓN

Como ya hemos comentado, son el punto más expuesto respecto a la Ciberseguridad en nuestras instalaciones, son la parte más visible del sistema, y aparte, si son Sistemas de Integración, cuando la seguridad de estos sistemas se ve comprometida, puede afectar a todos los equipos de campo.

En este caso vamos a dividir la protección en 4 partes:

1. Protección del Entorno:

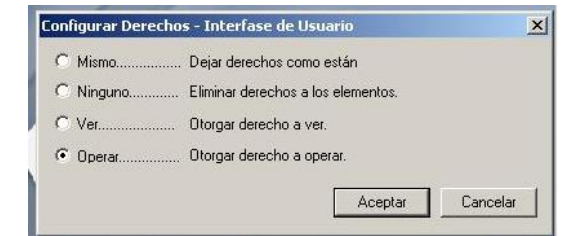
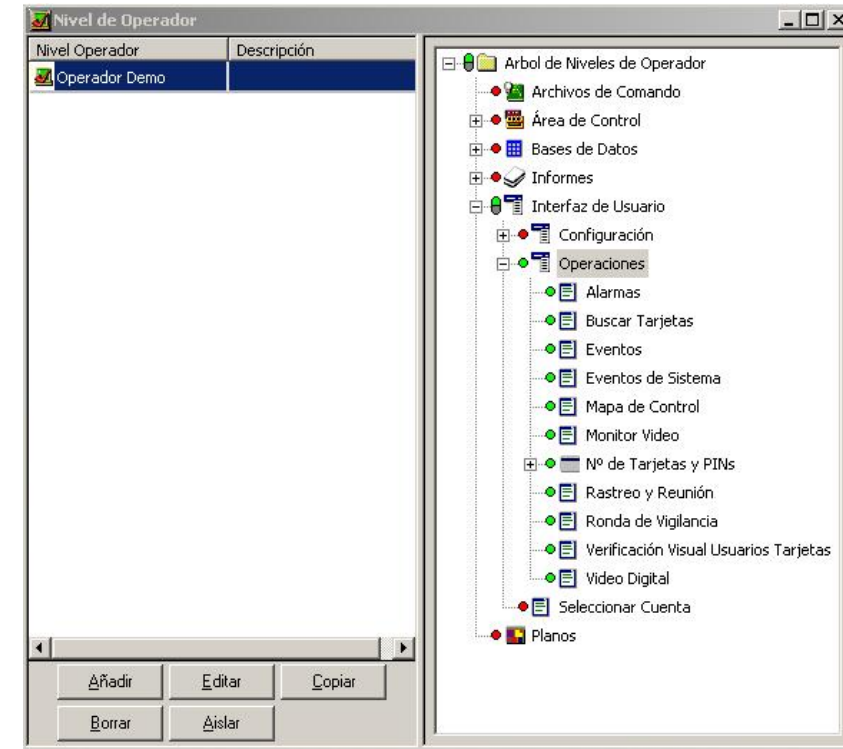
- Siempre trabajar en conjunto con los Responsables de Informática de los clientes finales. Es mas sencillo seguir sus políticas, que crear unas nuevas, o pelear por imponer las nuestras, salvo que sea imprescindible
- Siempre que sea posible, usar redes dedicadas para los sistemas de seguridad.
- Pero puede no se tan sencillo cuando debemos compartir la red con el resto de sistemas de nuestro cliente.
 - Dado es te caso, intentar crear una red Virtual (VPN) para nuestros dispositivos, si es posible, pero esto reducirá la flexibilidad de gestión, desde otros puntos de la red IP
 - En cualquier caso, cuando hablamos de vídeo, como la mayoría de dispositivos de grabación disponen de 2 tarjetas de red, conectar la de Gestión a la red general del cliente, y crear una específica para la de cámaras, de esta manera estarán aisladas del exterior, filtradas por el grabador



SOFTWARE DE PROGRAMACIÓN, GESTIÓN O INTEGRACIÓN

2. Gestión de Usuarios y Contraseñas:

- Como ya hemos insistido, debemos crear un usuario para cada persona que utilice el sistema
- Dichos usuarios deben tener los privilegios acorde con las funciones que desempeñen, por lo que debemos elegir sistemas que permitan definir con detalle dichas funciones
- Debemos crear una política de contraseñas fuertes (mínimo 8 dígitos, incluyendo mayúsculas, minúsculas, números y símbolos, y establecer un plan para su cambio regularmente, p.e. trimestralmente.
- Cerrar todos los puertos no necesarios para nuestros sistemas.
- Crear en la medida de lo posible, usuarios no administradores para los Operadores del Sistema de Seguridad.



SOFTWARE DE PROGRAMACIÓN, GESTIÓN O INTEGRACIÓN

3. Respaldo y recuperación de la Información:

- Las estadísticas nos dicen que los problemas de ciberseguridad nos van a afectar antes o después, por tanto deberemos estar preparados y tener un plan para guardar la información más importante, y preparar la recuperación del sistema.
- Hacer respaldos (Backups) de la información más crítica de cada sistema, normalmente suelen ser las bases de datos de los softwares de gestión, que almacenan toda la información de los usuarios, los equipos de campo y los históricos del sistema.
- Elegir sistemas que permitan hacer estos respaldos de seguridad de forma automática, y programarlos con una frecuencia no superior a la semana.
- Si es posible, que sean incrementales, esto evitara desperdiciar el espacio de almacenamiento. Los sistemas en la nube son una solución sin necesidad de recursos en local
- Preparar un plan para la correcta gestión de estos sucesos, y la recuperación de la operativa en el menor tiempo posible.
- Establecer planes alternativos, si no podemos recuperar el sistema principal, mantener disponibles alternativas de gestión, como los programas individuales de cada equipo de campo, o sus variantes web.

Información de Backup

Nombre de Backup: Copia Curso Básico

Descripción de Backup:

Tipo de Backup

- ☒ Base de Datos-Completa
- ☐ Base de Datos-Diferencial

Destino

Backup en: ☐ Cinta ☒ Disco

Nombre de Fichero: D:\SETTINGS\PRUEBAS IT\ESCRITORIO\Demo.BAK

☒ Añadir

Continuar Cancelar



Restaurar	Nombre del backup	Descripción del backup	Tipo	Fecha	Tamaño
☒	prueba		Completo	12/17/2008 17:31	21705216

Restaurar en...

- ☒ Restaurar la base de datos de WIN-PAK
- ☐ Restaurar el Archivo de Base de Datos de WIN-PAK
- ☐ Restaurar Nueva base de datos

Restaurar Cancelar

SOFTWARE DE PROGRAMACIÓN, GESTIÓN O INTEGRACIÓN

4. Actualización continua:

- Como ya hemos comentado, un sistema actualizado y al día es mas seguro que uno que no lo está.
- Debemos crear un plan de actualizaciones para todos los equipos y softwares que instalamos, aprovechando las visitas regulares de mantenimiento. Todo el personal de campo debe de estar familiarizado con dicho plan, y ejecutarlo automáticamente, como una parte más del mantenimiento.
- Debemos darnos de alta en los servicios de noticias del fabricante, para recibir la información relevante en cuanto actualizaciones, vulnerabilidades o problemas de los sistemas que usamos.
- Apoyarse en los departamentos de informatica de los clientes finales, para que al menos se encarguen de mantener al día los PCs de seguridad, en lo relativo a Sistemas Operativos y sus parches, Políticas de Red e Antivirus
- Internamente se deben crear una librería de actualizaciones para los equipos que se instalan de forma habitual, para evitar problemas in situ.
- Y para finalizar, como cada día es más habitual con los sistemas informáticas, se deben usar y ofrecer los planes de actualización de los sistemas, que ofrecen sus fabricantes, o SSA (Software Service Agreement).
- Normalmente, mediante un pago anual, recibiremos todas las actualizaciones que se lancen durante el año. Esto permite tener controlado el coste de software, y a la vez mantendremos los sistemas permanentemente al día. Ojo, hay que tener en cuenta los costes de mano de obra involucrados en dichas actualizaciones

Honeywell

Honeywell International Inc.
23500 W. 105th Street
Olathe, Kansas 66061-8425
U.S.A.
CAGE: 22373
Telephone: 800-461-3099 (Toll Free U.S.A./Canada)
Telephone: 862-365-3099 (International Direct)
Telephone: 00-800-461-3099 (EMEA Toll Free)
Telephone: 420-234-625-500 (EMEA Direct)

Website: www.myhoneywell.com

SERVICE BULLETIN

NAVIGATION - KGS 200 MERCURY2 WIDE AREA AUGMENTATION SYSTEM (WAAS) GLOBAL NAVIGATION SYSTEM SENSOR UNIT (GNSSU) - Conversion of KGS 200 Mercury2 WAAS GNSSU From PN 066-01201-0101, -0102, or -0104 to PN 066-01201-0105; install new Satellite Based Augmentation System (SBAS) Software

Legal Notice

Export Control

This document contains technical data and is subject to U.S. export regulations. These commodities, technology, or software were exported from the United States in accordance with the export administration regulations. Diversion contrary to U.S. law is prohibited.
ECON: 7E994, NLR Eligible.

Proprietary Information

Honeywell - Confidential

THIS COPYRIGHTED WORK AND ALL INFORMATION ARE THE PROPERTY OF HONEYWELL INTERNATIONAL INC. CONTAIN TRADE SECRETS AND MAY NOT, IN WHOLE OR IN PART, BE USED, DUPLICATED, OR DISCLOSED FOR ANY PURPOSE WITHOUT PRIOR WRITTEN PERMISSION OF HONEYWELL INTERNATIONAL INC. ALL RIGHTS RESERVED.

Honeywell Materials License Agreement

The documents and information contained herein ("the Materials") are the proprietary data of Honeywell International Inc. and Honeywell Intellectual Properties Inc. collectively "Honeywell". These Materials are provided for the exclusive use of Honeywell Service Centers; Honeywell-authorized repair facilities; operators of Honeywell aerospace products subject to an applicable product support agreement; their wholly owned subsidiaries or a formally designated third party service provider; and direct recipients of Materials from Honeywell's Aerospace Technical Publication Distribution. The terms and conditions of this License Agreement govern your use of these Materials, except to the extent that any terms and conditions of another applicable agreement with Honeywell regarding the operation, maintenance, or repair of Honeywell aerospace products conflict with the terms and conditions of this License Agreement, in which case the terms and conditions of the other agreement will govern. However, this License Agreement will govern in the event of a conflict between its terms and conditions and those of a purchase order or acknowledgement.

1. License Grant - If you are a party to an applicable product support agreement, a Honeywell Service Center agreement, or an authorized repair facility agreement, Honeywell hereby grants you a limited, non-exclusive

16 Aug 2012
Revision 0, 16 Aug 2012

KGS 200-34-05

Page 1 of 27

Publication Number 0201207000009
© Honeywell International Inc. Do not copy without express permission of Honeywell.

Stouter Tech Ltd.

SOFTWARE MAINTENANCE AGREEMENT

Parties

This SOFTWARE MAINTENANCE AGREEMENT ("Agreement"), dated July 25, 2022, is made by and between **Danny B. Stouter of Stouter Tech Ltd. ("Contractor")** and **George F. Uyases of Ford & Sons Retail ("Client")**.

In consideration of the mutual promises and covenants in this Agreement, of which the receipt and sufficiency are hereby acknowledged, the Parties further agree to the terms as follows:

Services Provided

The Contractor agrees to perform monthly maintenance services ("Services") of the software purchased from the Contractor within the agreed-upon two-year term. The Services will include inspecting, updating, troubleshooting, and diagnostics. The Services will be primarily conducted at the Client's place of business at 2602 Star Trek Drive, Pensacola, Florida 32507.

Terms and Conditions

HACIENDO LA SEGURIDAD “MÁS SEGURA” HACIA LA ENCRYPTACIÓN TOTAL

TRANSMISIÓN SEGURA DE DATOS



- Paneles encriptados, comunicación TLS 1.2 desde las Cámaras a los NVRs, y desde estos a los Clientes de Vídeo – cubre clientes normales, ligeros y móviles
- Capacidad de usar certificados auto firmados

ASEGURANDO EL RESTO



Exportación de datos encriptada – Los vídeos exportados por el sistema lo son en el formato propietario o mejor, cifrado

MANTENIMIENTO SEGURO DE LOS DISPOSITIVOS



- La actualización del firmware de los dispositivos desde el Intelligent Command se hace de forma segura y encriptada.
- Actualizaciones de firmware en lotes controlada por el usuario

CONTRASEÑAS FORTALECIDAS



- Gestión segura por lotes de los cambios de contraseñas de los usuarios, en línea con las políticas de TI

ENDURECIMIENTO GENERAL DEL SISTEMA



- Parches de seguridad adicionales contra ciber vulnerabilidades
- Vulnerabilidades reducidas mediante mantenimiento al día tanto el S.O como las librerías .NET





NDAA
Compliant



¡Gracias!