

SEGURIGAS

S.A.

Auditoría de seguridad

**Seguridad Informática**

**Julián B. Sánchez López**

**Índice**

1. **La empresa**
   1. Introducción de la Empresa

SEGURIGAS S.A. es una planta de regasificación situada en el puerto de Valencia. Pertenece al grupo NOEGAS S.A, encargado de transportar gas a través del territorio nacional. Es una infraestructura clave en el sector energético español ya que aporta una mayor seguridad y eficiencia al sistema de gas nacional ya que está situada en una buena posición estratégica entre los principales productores de gas como África y Oriente Medio y los puntos finales de consumo.

A las instalaciones de SEGURIGAS llega gas natural licuado, el cual se cambia a estado líquido para ser distribuido a través de la red nacional de gaseoductos. Además, también cargan y descargan barcos y camiones cisterna. Todo esto supone que todos los procesos que realizan se lleven a cabo con la última tecnología y bajo las más estrictas medidas de seguridad y calidad.

* 1. Descripción de la planta

La planta cubre un total de 23 hectáreas en el dique del puerto de Valencia, dispone de 4 tanques de almacenamiento de gas natural con una capacidad total de 600.000 metros cúbicos, además de multitud de tecnologías como brazos de descarga, bombas, vaporizadores y gaseoductos. Todo este equipamiento está conectado y controlado a través de la red local de la empresa.

En la plata se realizan las tareas de descarga de buques, almacenamiento de gas natural liquidado, regasificación, carga de camiones cisterna recarga de buques metaneros entre otras actividades. El diseño y construcción de la planta están certificados por el estándar de Gestión de la Seguridad y Salud en el Trabajo OHSAS 18001. Además, antes de entrar a la planta todo trabajador de la empresa o trabajador subcontratado recibirá un curso de formación.

* 1. La visión de la empresa

La empresa está catalogada como actividad esencial y la planta está considerada como instalación crítica ya que debe estar operativa las 24 horas del día, los 365 días del año, no puede cesar su actividad ya que los servicios que proporciona deben estar disponibles en todo momento.

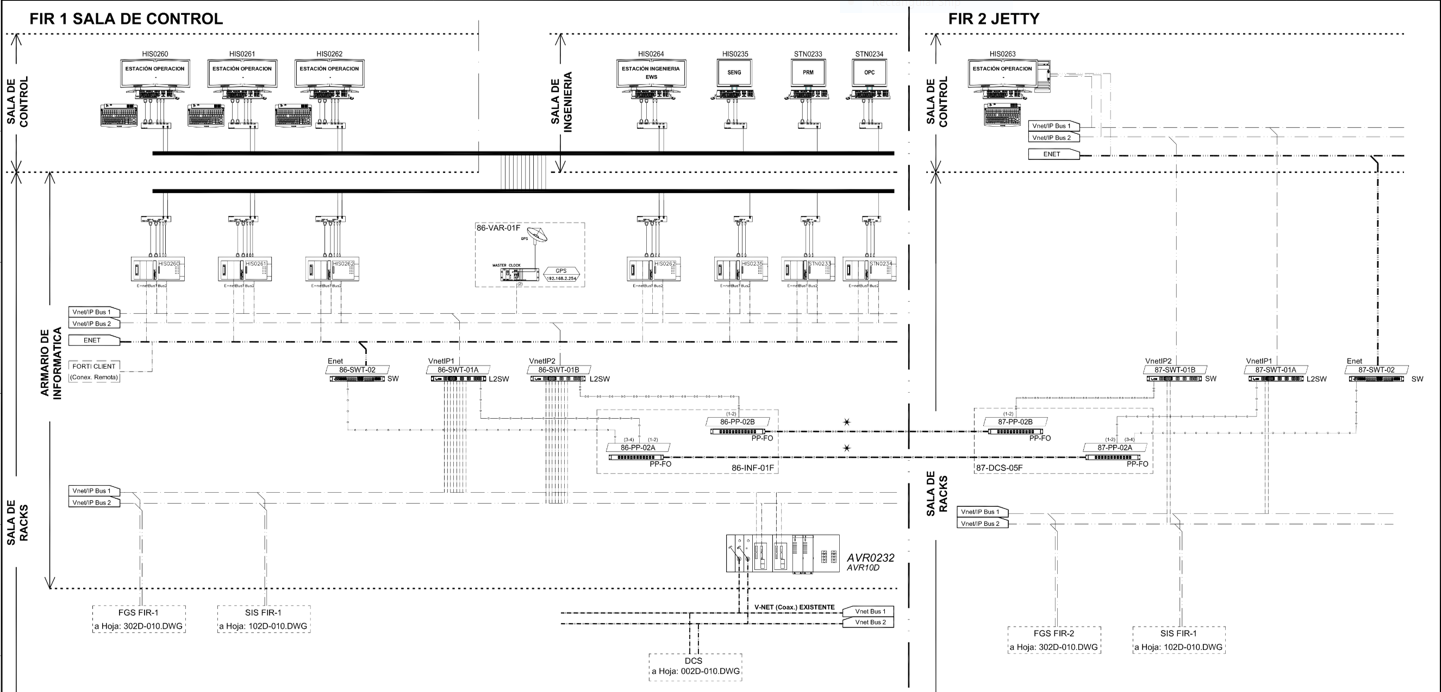
Es por ello la empresa dispone de sistemas de seguridad que le permitan salvaguardar todos los equipamientos y máquinas de las que dispone, así como asegurar la confidencialidad, integridad y disponibilidad de la información.

1. **Seguridad interna**

Debido a la gran infraestructura de la empresa y el elevado número de trabajadores y equipos que requieren conexión a la red, SEGURIGAS tiene una red MAN la cual permite interconectar todos los equipos, donde se incluyen tanto equipos informáticos (PC, servidores, móviles de empresa, etc.…) como la maquinaria la cual también debe conectarse a dicha red.

La red está subdividida a través de VLANs y VPNs con el fin de aislar los diferentes departamentos lo que facilita la gestión, administración y labores de protección de cada subred.

El control y la monitorización de la red se llevan a cabo dese la sala de control de la empresa, la cual tiene la siguiente estructura lógica



En la sala de control principal (FIR 1) se encuentran los tres operarios encargados del control y la monitorización de la red y los sistemas informáticos que la componen. Disponen de un equipo adicional en una sala separada (FIR 2) en caso de fallo en uno de los equipos o necesidad de aislamiento de un operador (como por ejemplo debido a la COVID-19).

En una sala anexa a la sala de control principal se encuentra la sala de ingeniería que contiene los equipos que permiten configurar y monitorizar los parámetros de los sistemas principales de la empresa. Entre estos sistemas destaca el sistema de detección automático que permite detectar alguna anomalía en la red o el suministro y paraliza todo tipo de actividad en esa zona.

Por último, la sala de control también contiene una zona de rack donde se pueden encontrar varios switches, los cuales se utilizan para separar la red corporativa en VLANs

Para entrar en la sala y utilizar los equipos que hay en ella los operarios deben disponer de su tarjeta de identificación y estar debidamente autorizados por el administrador para acceder a los equipos con su usuario de dominio y contraseña particulares.

La red corporativa conforma una topología en árbol o jerárquica donde se definen específicamente los niveles de autoridad de cada sistema que la conforma. En el rango más elevado se encuentra la sala de control. La organización física y estructura lógica de la red son las más adecuadas de acuerdo con las necesidades de la empresa ya que permite a las personas autorizadas actuar inmediatamente en caso de fallo o incidente en alguno de los sistemas.

Para acceder a la sala de control se toman las medidas estrictas necesarias acordes con la importancia de dicha sala, un punto a tener en cuenta y mejorar en un futuro es la incorporación de la biometría como sistema de autenticación en lugar de tarjetas de identificación ya que estas pueden ser robadas o olvidadas. Sin embargo, los rasgos biométricos proporcionan una gran seguridad ya que son intransferibles.

Otro punto a mejorar con respecto a la seguridad de los equipos de control de la sala sería una actualización del Sistema Operativo de las estaciones de operación (véase índice con el listado de componentes HW y SW). Actualmente estos equipos están utilizando Windows 7 cuyo soporté por parte de Microsoft finalizó hace un año aproximadamente, esto supone que, en caso de encontrar una nueva brecha de seguridad en el SO, Microsoft no la va a solucionar por lo que los equipos utilizando dicho SO se encontrarán bajo amenaza. Por ello es recomendable actualizar el SO de los equipos a una versión mas moderna y actualizada como pueda ser Windows 10.

Para finalizar, cabe destacar positivamente el resto de medidas de seguridad tomadas por la empresa para garantizar la seguridad de la sala de control a través de un circuito cerrado de televisión (CCTV) específico para la sala, así como un rack organizado y custodiado bajo llave por el administrador, como los sistemas de repuesto que garantizan la disponibilidad del servicio en todo momento

1. **Página Web**

La empresa dispone de una plataforma web la cual se utiliza principalmente como guía informativa de la actividad que desarrollan y los servicios que ofrecen. Sobre el dominio recaen un total de unas 20 páginas web y, además se puede consultar la web en tres idiomas.

La página hace uso de cookies para su correcto funcionamiento y le ofrece al usuario la posibilidad de aceptar o rechazar ciertas cookies. Por último, dispone de un apartado de contacto donde cualquier persona puede enviar un mensaje a la empresa rellenando un formulario.

Pese a que el objetivo de la página es simplemente informativo y no se llevan a cabo transacciones ni registro de usuarios en ella, es importante que disponga del certificado SSL que garantiza que la información entre un cliente que rellene el formulario y la página web estará cifrada asegurando así su confidencialidad e integridad.

Otro punto a destacar sobre la página web es su extenso código que proporciona seguridad ante todo tipo de ataques externos, ya sean ataques de inyección SQL, inclusiones de archivos locales o remotos y Cross Site Scripting (XSS). Todo este código consigue mantener la página segura pero a su vez dificulta la carga de la página al contar con numerosos scripts de protección que ralentizan el proceso, es por ello, que para mejorar la eficiencia y la seguridad de la página, convendría situar los scripts de los que hace uso la página al final de esta para que se ejecuten una vez la página este completamente cargada y no quede ningún elemento vulnerable y susceptible a un fallo de que pueda originar una brecha de seguridad a consecuencia de una mala estructuración del código

1. **Anexo**

Anexo

Inventario de la sala de control

Equipamiento Hardware

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CÓDIGO | DESCRIPCIÓN | FABRICANTE | MODELO | UBICACIÓN |
| HIS0260 | Estación de operación | HP | Z230 | FIR-1 |
| HIS0261 | Estación de operación | HP | Z230 | FIR-1 |
| HIS0262 | Estación de operación | HP | Z230 | FIR-1 |
| HIS0264 | Estación de ingeniería DCS (EWS) | HP | Z230 | FIR-1 |
| HIS0235 | Estación de ingeniería Prosafe RS (SENG) | HP | Z230 | FIR-1 |
| STN0233 | Estación PRM | HP | Z230 | FIR-1 |
| STN0234 | Estación OPC | HP | Z230 | FIR-1 |
| 86-SWT-02 | Switch red Ethernet | Netgear | GS724T | FIR-1 |
| 86-SWT-01A | Switch red VnetIP 1 | Hirschmann | MACH104-20TX-FR | FIR-1 |
| 86-SWT-01B | Switch red VnetIP 2 | Hirschmann | MACH104-20TX-FR | FIR-1 |
| 87-SWT-02 | Switch red Ethernet | Netgear | GS724T | FIR-2 |
| 87-SWT-01A | Switch red VnetIP 1 | Hirschmann | MACH104-20TX-FR | FIR-2 |
| 87-SWT-01B | Switch red VnetIP 2 | Hirschmann | MACH104-20TX-FR | FIR-2 |
| AVR010D | Router Vnet redundante | Yokogawa | BCVV0232 | FIR-1 |
| MASTER CLOCK | Sincronizador horario vía GPS |  |  | FIR-1 |

Equipamiento Software

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| COGIGO | DESCRIPCIÓN | FABRICANTE | VERSION | USO |
| CENTUM VP | Administración y supervisión del DCS | Yokogawa | R6.03.00 | Estaciones de operación e ingeniería (EWS) |
| Prosafe RS | Administración sistemas SIS y FGS | Yokogawa | R4.02.00 | Estación ingeniera SIS y FGS (SENG) |
| Exa OPC | Interfaz comunicaciones con PI | Yokogawa | NTPKM01-C1\* | Estación STN0234 |
| Release: R3.75.00 |
| PRM | Gestión Instrumentos HART | Yokogawa | R3.31.00 | Estación STN0233 |
| Windows 7 Pro | Sistema Operativo | Microsoft |  | Estaciones de operación e ingeniería. |

Inventario de equipos de la red corporativa

Equipamiento HW

|  |  |  |
| --- | --- | --- |
| **DESCRIPCIÓN** | **FABRICANTE** | **MODELO** |
| Servidor | IBM | System x3650 M4 -[7915E7G] |
| Cabina de almacenamiento | IBM | Storwize v3700 |
| Equipo portátil | Microsoft | Surface Pro 4 |
| Equipo portátil | Microsoft | Surface Pro 3 |
| Equipo portátil | HP | HP ProBook 4540s |
| Equipo sobremesa | Lenovo | 3245B6G |
| Equipo sobremesa | Lenovo | MT-M 10A8-S0HG00 |

Equipamiento SW (No pongo todo porque son 30+ páginas)

|  |  |  |
| --- | --- | --- |
| Adobe Acrobat Reader DC - Español | 18.009.20050 | Adobe Systems Incorporated |
| Adobe Acrobat X Pro - Italiano, Español, Nederlands, Português | 10.0.0 | Adobe Systems |
| Adobe Acrobat XI Pro | 11.0.07 | Adobe Systems |
| Adobe AIR | 3.4.0.2710 | Adobe Systems Incorporated |
| Adobe Flash Player 10 ActiveX | 10.0.32.18 | Adobe Systems, Inc. |
| Adobe Flash Player 10 Plugin | 10.0.32.18 | Adobe Systems, Inc. |
| Adobe Flash Player 11 ActiveX | 11.0.1.152 | Adobe Systems Incorporated |
| Adobe Flash Player 12 ActiveX | 12.0.0.38 | Adobe Systems Incorporated |
| Adobe Flash Player 14 Plugin | 14.0.0.145 | Adobe Systems Incorporated |
| Adobe Flash Player 17 ActiveX | 17.0.0.169 | Adobe Systems Incorporated |
| Adobe Flash Player 18 ActiveX | 18.0.0.261 | Adobe Systems Incorporated |
| Adobe Flash Player 21 ActiveX | 21.0.0.242 | Adobe Systems Incorporated |
| Adobe Flash Player 25 ActiveX | 25.0.0.171 | Adobe Systems Incorporated |