

SEGURIGAS

S.A.

Auditoría de seguridad

**Seguridad Informática**

**Julián B. Sánchez López**

**Índice**

Contenido

[Contenido 2](#_Toc63621280)

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.

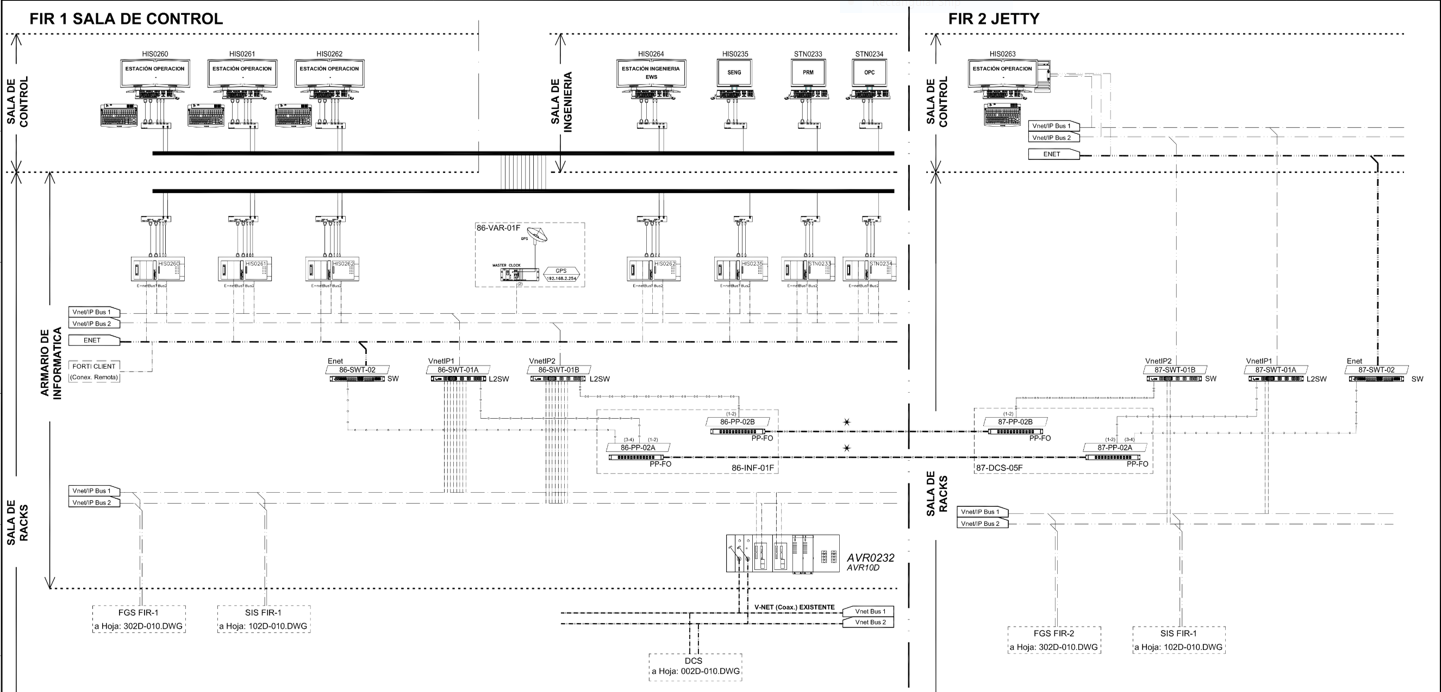
Es por ello la empresa dispone de sistemas de seguridad que le permitan salvaguardar todos los equipamientos y máquinas de las que dispone, así como asegurar la confidencialidad, integridad y disponibilidad de la información.

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

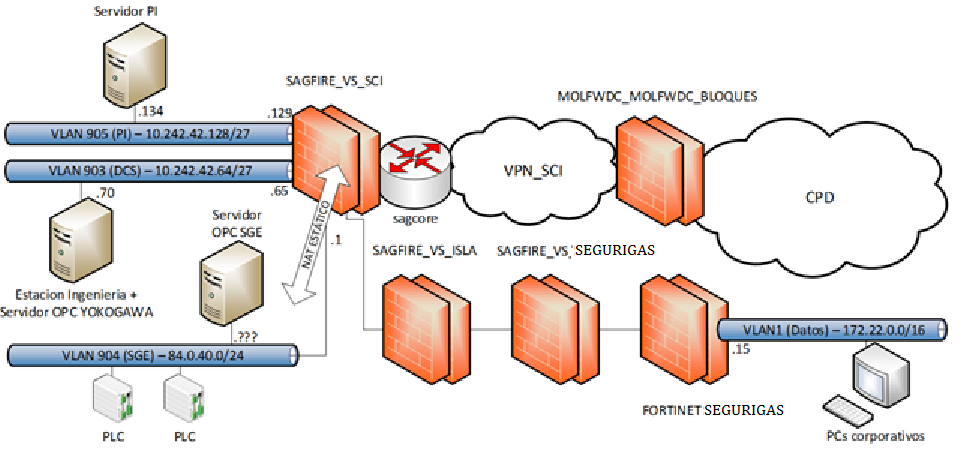
Para entrar en la sala y utilizar los equipos que hay en ella los operarios deben disponer de su tarjeta de identificación y estar debidamente autorizados por el administrador para acceder a los equipos con su usuario de dominio y contraseña particulares.

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 u 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 más 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. Seguridad perimetral
2. Test de intrusión

SEGURIGAS lleva a cabo de forma periódica una serie de simulacros y pruebas con el fin de comprobar la eficiencia de sus sistemas de seguridad, muchas de estas pruebas están organizadas y dirigidas por NOEGAS y se realizan de manera independiente a la empresa.

Es frecuente que se realicen pruebas de personal no autorizado intentando entrar al perímetro, ya sean personas desconocidas, antiguos empleados de la empresa o empleados de una empresa subcontratada. Es por ello que el servicio de administración y seguridad tiene que estar sincronizado en todo momento con el servicio de vigilancia de la empresa, ya que estos son la primera y más importante barrera física para acceder a las instalaciones y deben asegurarse que toda persona que accede está debidamente identificada. Hasta el momento no se ha reportado ninguna intrusión por parte de personal no autorizado lo que indica las estrictas medidas de seguridad física y su adecuada aplicación.

Una vez comprobada la seguridad física, se pasan a realizar test de intrusión al CPD de la empresa. Pese a que la ubicación exacta del CPD no está indicada, es conocida por todos los empleados; es más, la mayoría de empleados tienen acceso a dicha sala con sus credenciales independientemente al departamento que pertenecen. Este debe ser un punto de mejora en la seguridad de la empresa ya que únicamente los administradores o personal específico que vaya a trabajar en el CPD debería tener acceso a la sala.

Por último, cabe destacar un “honeypot” realizado por NOEGAS en el cual se repartieron a los trabajadores de forma gratuita una serie de dispositivos de almacenamiento USB simulando una promoción publicitaria. Muchos de estos trabajadores introdujeron el USB en el ordenador de la empresa para utilizarlo lo cual es un fallo de seguridad muy grave que puede poner en gran peligro la seguridad de la empresa. Cuando un trabajador introduce el USB en el ordenador se pueden ejecutar scripts maliciosos que dañen los sistemas, en este caso simplemente se enviaba un mensaje de advertencia a NOEGAS con la información de equipo host donde se introducía el dispositivo. A través de este test se demostró que los trabajadores siguen siendo el eslabón mas débil en el sistema de seguridad de la empresa y es fundamental invertir en la formación necesaria a todo el personal para evitar que sucedan este tipo de ataques. Una vez NOEGAS notificó a SEGURIGAS un informe detallado con lo sucedido, la empresa llevo a cabo una serie de cursillos sobre seguridad y buenas prácticas a todo el personal. Es importante que este tipo de formación se mantenga y sean de obligatoria atención y cumplimiento tanto para trabajadores actuales como posibles trabajadores futuros que se incorporen.

1. Análisis forense

Una parte muy importante en la seguridad de la empresa es la evaluación de los daños ocasionados ante posibles ataques, como instalación crítica

Durante todos los años se llevan a cabo diferentes simulacros con el objetivo de revisar y evaluar las medidas de defensa de la empresa, pero también sirven como métodos de formación para los trabajadores y conocer el alcance que pueda tener el incidente.

Simulacros como incendios controlados ayudan a la empresa a saber el tiempo necesario que tienen para reaccionar y como salvaguardar la información y los equipos de la mejor manera. Del mismo modo se evalúa como un corte en el suministro eléctrico puede comprometer el sistema de información de la empresa y cómo este se recupera ante una caída.

La empresa dispone de un Plan de Seguridad donde se documenta detalladamente le proceso de análisis forense que lleva a cabo la empresa cuando se ha producido un ataque. El primer paso de este proceso consistirá en realizar una evaluación previa del incidente revisando las políticas de seguridad, notificaciones y autorizaciones de las personas responsables, después se procederá a recoger los datos del incidente custodiando siempre las evidencias originales. Una vez obtenidos los datos originales se deberán analizar los datos de la red, los equipos y los sistemas de almacenamiento para conocer el alcance de los daños ocasionados. Por último, se deberán reportar todos los datos obtenidos y las conclusiones al administrador con el fin de evaluar los daños sufridos y diseñar posibles contramedidas para evitar que vuelva a suceder

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. Con el fin de cumplir con la Ley Orgánica de Protección de Datos (LOPD-GDD) cada vez que un usuario visite por primera vez la página se le informará del uso que hace la página web con sus datos y podrá ajustar sus preferencias con respecto a las cookies siempre y cuando lo desee.

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 ya que dispone de un apartado de contacto donde cualquier persona puede enviar un mensaje a la empresa rellenando un formulario. Este protocolo garantiza que la información entre un cliente que rellene el formulario y la página web estará cifrada asegurando así su confidencialidad e integridad.

A través de una estructura basada en cliente-servidor la página web consigue que solo el servidor web autorizado pueda mostrar el contenido y ofrecer las funcionalidades de la página correctamente. De esta forma se evitan posibles ataques de suplantación de identidad ante atacantes que quieran imitar la estructura de la página a través de técnicas como tabnabbing. Esta estructura también permite a la página tener una mayor resistencia ante ataques de denegación distribuida del servicio (DDoS) ya que el servidor el capaz de gestionar las peticiones de los clientes y rechazar aquellas que detecte como ataques basados en una botnet.

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. Código de la aplicación

La empresa dispone de una aplicación la cual es utilizada diariamente por los empleados y administradores. El acceso a esta aplicación está restringido únicamente a los trabajadores de SEGURIGAS y el personal informático de NOEGAS que controlan el uso de la aplicación.

A través de esta aplicación se pueden realizar las tareas de monitorización de los equipos de toda la instalación y los sistemas informáticos, tareas administrativas como controlar el acceso de empleados y personal subcontratado en los diferentes departamentos de la empresa, acceso y gestión a la información confidencial de la empresa, entre otros servicios.

Por ello, para poder utilizar la aplicación, un administrador debe autorizar específicamente el acceso de un trabajador, habilitando una cuenta propia personal e intransferible, además esta cuenta solo podrá ser utilizada en los equipos a los que el trabajador en cuestión tenga acceso.

Para ingresar en la aplicación será necesario un nombre y una contraseña que solo el trabajador debe conocer y además está sujeta a las siguientes políticas: la contraseña debe tener entre 8 y 32 caracteres, debe contener una minúscula, una mayúscula, un número y un símbolo, tampoco se podrán utilizar palabras del diccionario y la contraseña será renovada automáticamente cada 30 días por otra que no se haya utilizado con anterioridad.

Además, cabe destacar que para acceder a la aplicación es imprescindible hacerlo desde la red de la empresa. Los trabajadores que estén trabajando telemáticamente y quieran utilizarla deberán conectarse a la VPN de la empresa a través de un proceso de doble autenticación con el usuario y contraseña de su cuenta y un código que le llegará al móvil de la empresa.

El código de la aplicación está basado en Windows Froms App y escrito en C# lo que permite tener una aplicación muy robusta en cuanto a eficiencia y seguridad gracias a las herramientas que este lenguaje proporciona. El código está testeado y es mantenido regularmente por los administradores por lo que se puede considerar como una aplicación segura

Un punto importante a destacar en la seguridad de la aplicación es la expiración de cuentas cuando una persona deja de trabajar para la empresa. Este puede seguir accediendo al programa hasta que su contraseña expira, lo cual puede suponer un grave fallo en la seguridad debido a un exempleado descontento que pueda comprometer la confidencialidad de la información. Cuando una persona deja de trabajar para la empresa, el administrador debe denegar el acceso a la aplicación de forma inmediata para evitar este tipo de ataques.

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 |