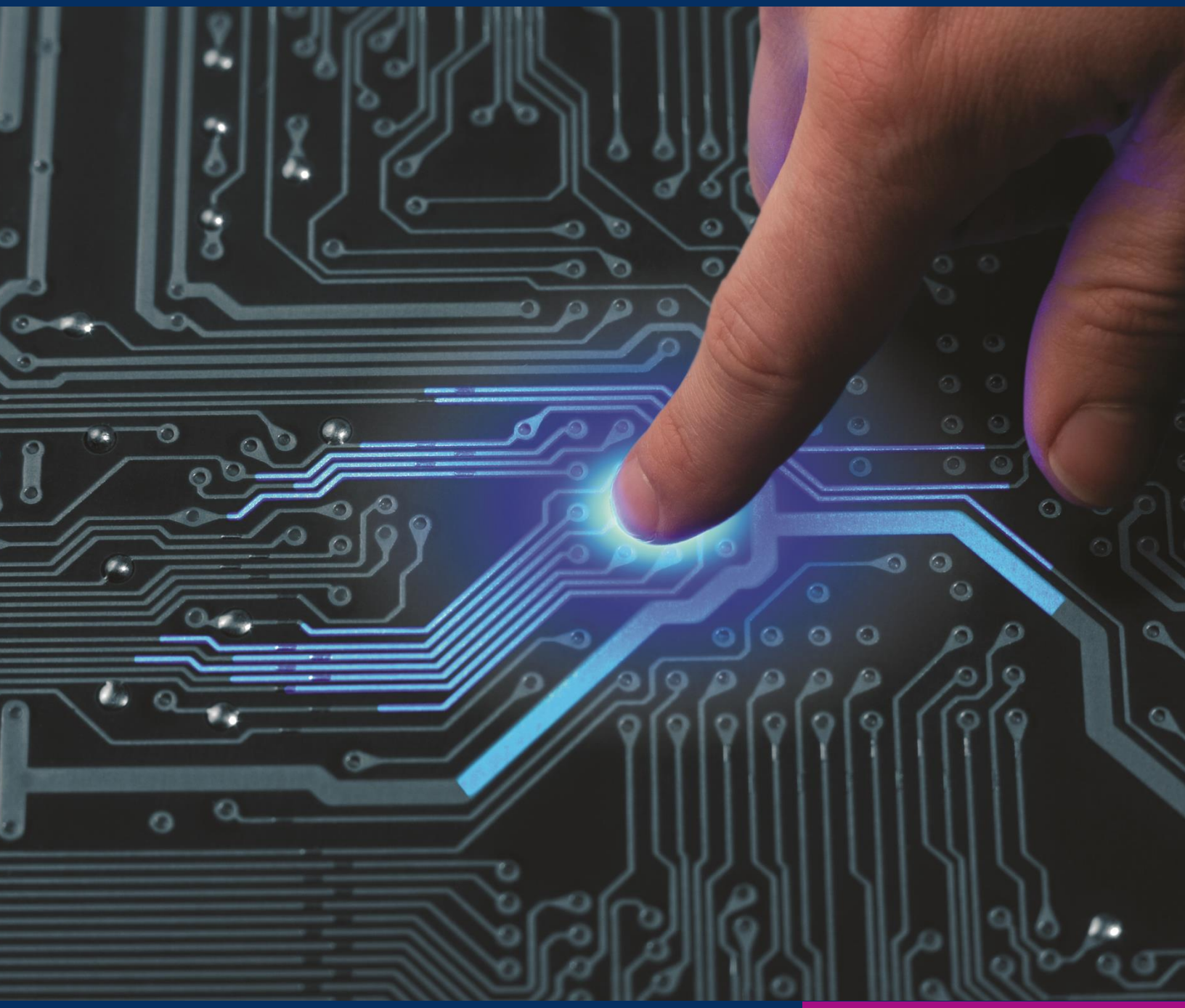
Auditoría de seguridad



Seguridad Informática

Julián B. Sánchez López

SEGURIGAS S.A.

Índice

1. LA EMPRESA

1.1. 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. Dispone de los certificados de calidad ISO 9001 y el certificado ISO 27000 para los sistemas de gestión de la información

1.2. 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.

1.3. 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.

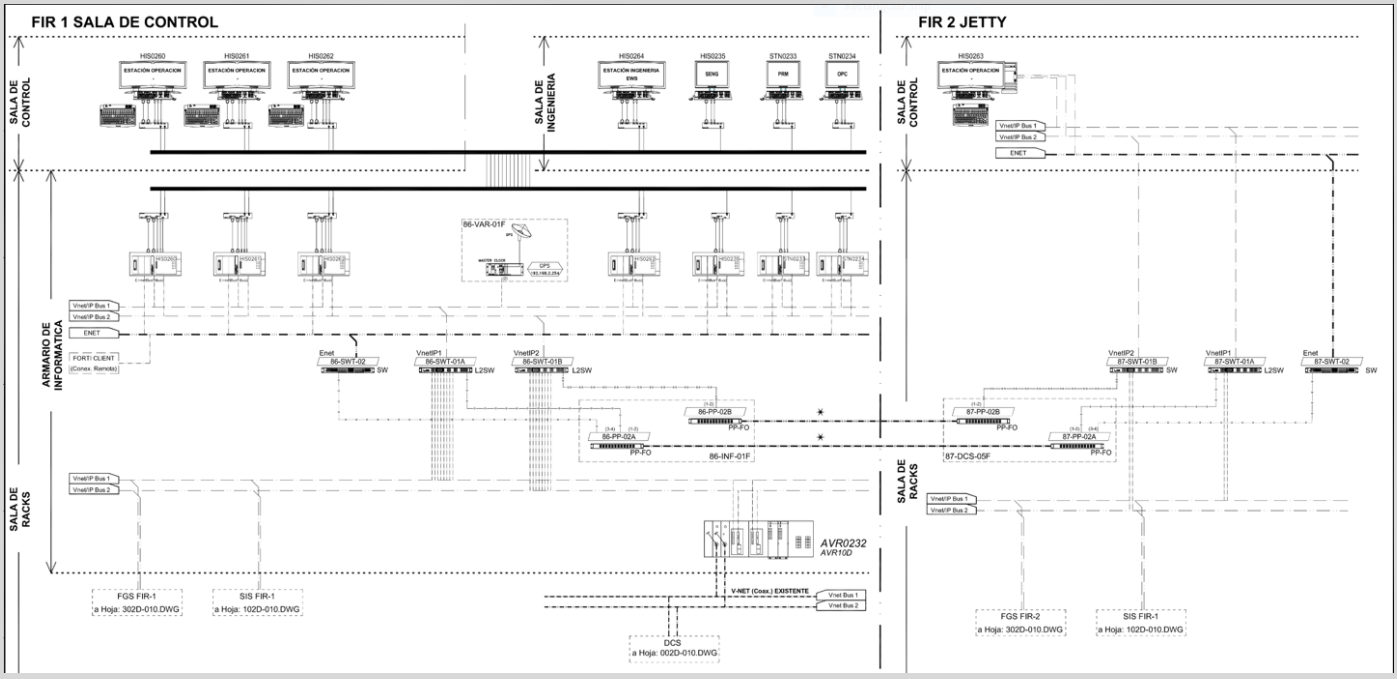
2. SEGURIDAD INTERNA

2.1. INTRODUCCIÓN

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 acceso a las VPNs de la empresa se realizará siempre a través del protocolo SSH el cual permite tunelizar las comunicaciones, cifrando dicho túnel gracias al protocolo RSA que proporciona la PKI de NOEGAS.

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).

2.2. SALA DE CONTROL E INGENIERÍA

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

2.3. CPD

En el corazón de las instalaciones se encuentra el Centro de Procesado de Datos (CPD) el cual está destinado a alojar algunos servidores y sobre todo copias de seguridad de todos los equipos de la empresa. Actualmente la carga del CPD está repartida entre las instalaciones de SEGURIGAS y las instalaciones de NOEGAS, que disponen de un Centro de Respaldo (CR) que en caso de fallo del CPD conmutarán rápidamente para seguir proporcionando un servicio sin sufrir ningún retraso. Ya que tanto la empresa como las empresas cercanas realizan actividades potencialmente peligrosas disponer de un segundo CPD alejado geográficamente es una gran herramienta para salvaguardar la información en caso de accidente.

Gracias a este sistema se puede garantizar una fiabilidad infalible en los servicios del CPD, es decir, se garantiza que el sistema estará disponible un 99,999%, o lo que es lo mismo, solo estará sin servicio un mínimo de una hora al año. Esto es de gran importancia ya que, al estar trabajando con instalaciones críticas, la disponibilidad de la información es uno de los aspectos más importantes a cuidar. Una de las principales herramientas que utiliza la empresa para garantizar esta fiabilidad es un Sistema de Alimentación Ininterrumpida (SAI) on-line, el cual no solo protege ante cortes en el suministro eléctrico, sino también sirve para estabilizar y filtrar la corriente que llega a los servidores. El SAI está monitorizado en todo momento por las salas de control donde se controla en todo momento el nivel de carga y se configuran correctamente para responder ante cualquier fallo en el suministro.

El CPD se encuentra en el primer piso del edificio central de la empresa, en una ubicación no señalizada y alejado de las oficinas. Es una sala de medio tamaño y media altura que no dispone de ventanas y dispone de sistemas de control ambiental para controlar y monitorizar los niveles de temperatura y humedad. Al igual que todas las salas de la empresa, el CPD dispone de un sistema avanzado de detección de humos y un sistema de apagado automático a través de agua nebulizada.

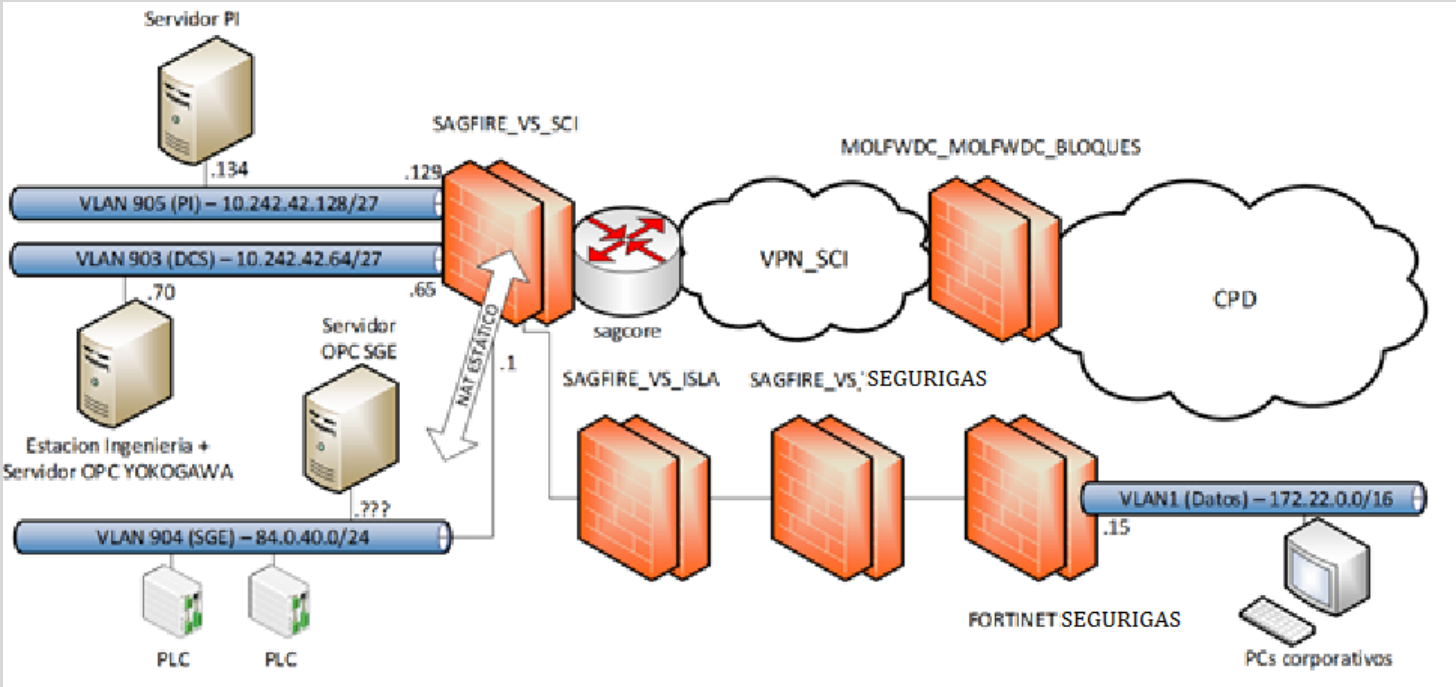
Pese a que el CPD no dispone de muchos equipos sería recomendable realizar una ampliación en la sala o mover el CPD a una sala diferente la cual sea algo más grande, de esta forma se podría instalar un sistema de falso techo y falso suelo que favorezca tanto ventilación como cableado. Además, se podrán organizar los equipos de manera estratégica creando pasillos fríos y pasillos calientes que, una vez más, favorezca en todo lo posible la ventilación y sea más fácil y sostenible para los sistemas de refrigeración mantener los equipos al nivel de temperatura fijado para la sala (22º)

Los servidores que se encuentran en el CPD so, en su mayoría, servidores de almacenamiento ya que las instalaciones de NOEGAS se encargan de la mayoría de los otros servicios que necesita el conjunto de redes que forma el grupo. Estos servidores de almacenamiento disponen de un sistema RAID 5 que evita que el servidor deje de funcionar en caso de fallo en uno de los discos duros. Pese a que el sistema RAID 5 asegura la continuidad del servicio ante una rotura de un disco, sería recomendable utilizar un sistema RAID 0 + 1 en los servidores ya que, pese a que supone un mayor coste, los datos son el activo más importante que la empresa debe proteger y este sistema proporciona fiabilidad absoluta.

El CPD recibe los suministros eléctricos y de comunicaciones de dos proveedores distintos. La alimentación del CPD está separada de la alimentación principal del edificio central y disponen de un generador que utiliza combustible (apto para el entorno de trabajo). La empresa tiene contratado dos líneas con compañías de telecomunicaciones distintitas, la principal utiliza fibra óptica mientras que la secundaria utiliza la tecnología Ethernet.

El objetivo principal del CPD es el almacenamiento y gestión de copias de seguridad las cuales tienen un registro con todas las actividades realizadas en los equipos de la empresa y son de gran utilidad en caso de fallo en algún equipo, ya que permite restaurar el equipo con un bajo tiempo de respuesta y a un bajo coste en comparación a los daños que podría suponer la pérdida de información. Las copias de seguridad se realizan de manera remota desde los equipos de origen hasta los servidores de almacenamiento situados en el CPD y la tecnología para realizarlas está basada en un sistema diferencial con el fin de ahorrar costes de almacenamiento. Las copias se lanzan de manera secuencial todas las noches y se almacenan un total de 14 días naturales en los servidores del CPD. Un ataque ransomware conlleva un enorme riesgo para la empresa debido a la gran importancia de la información y, este sistema de copias de seguridad es una contramedida eficiente ante ellos.

Los servidores de almacenamiento deberán ser accedidos por los usuarios autorizados a través de la red particular de los discos ya que la empresa dispone de una tecnología SAN (Storage Area Network) para acceder a estos. Esta es la manera más segura y eficiente de tener servidores de almacenamiento ya que proporciona la máxima disponibilidad de la información.



2.4. RED CORPORATIVA

La estructura lógica de la red se puede ver en la siguiente imagen, se pueden destacar el acceso a la red corporativa a través de multitud de firewalls y el acceso al CPD a través de la red específica VPN.

La red corporativa está formada por la mayoría de equipos que conforman la red, son los equipos personales que utilizan a diario la mayoría de trabajadores por lo que son el foco principal tanto para atacantes como para la seguridad.

Otro punto a tener en cuenta en la seguridad de estos equipos son las actualizaciones del sistema operativo y las aplicaciones, gracias a ellas se pueden solventar un gran número de vulnerabilidades y brechas de seguridad que contenga el Software, pero deben ser realizadas siempre por el administrador y con una copia de seguridad respaldando la versión más reciente de dicha aplicación o SO. También cabe destacar que todos los equipos utilizan Microsoft Windows 10, el cual cumple con el estándar EAL4 de calidad establecido por Common Criteria.

Todos los equipos disponen de unas políticas muy estrictas de antimalware y antivirus con el fin de controlar todo el Software que tiene cada equipo. Todos los sistemas tienen instalado dos antivirus y antimalware diferentes los cuales utilizan tecnologías de búsqueda distintas lo que proporciona una gran seguridad ante software malicioso de todo tipo (virus, gusanos, troyanos, sniffers, etc…) y, permite detectar que aplicaciones no hacen un uso debido de los recursos

Los usuarios no administradores no disponen de permisos para descargar ningún tipo de aplicación. Estas y muchas otras políticas se aplican a través de una Access Control List (ACL) gestionada directamente por NOEGAS, además todo el grupo de empresas dispone de un software de control de acceso a la red, el cual comprueba si los equipos cumplen con las políticas de seguridad y de esta forma, al tener toda una política común, las diferentes empresas que conforman el grupo pueden compartir información de forma segura.

Como punto de mejora para la seguridad interna de tanto la red corporativa como los servidores del CPD será implantar políticas de seguridad en la BIOS de todos los equipos. Estas políticas deberán aplicar medidas tales como contraseñas para acceder a la BIOS y deshabilitar arranques del sistema por otro medio de almacenamiento que no sea el disco duro para así evitar ataques de denegación de servicio y suplantación de identidad o pérdida de información.

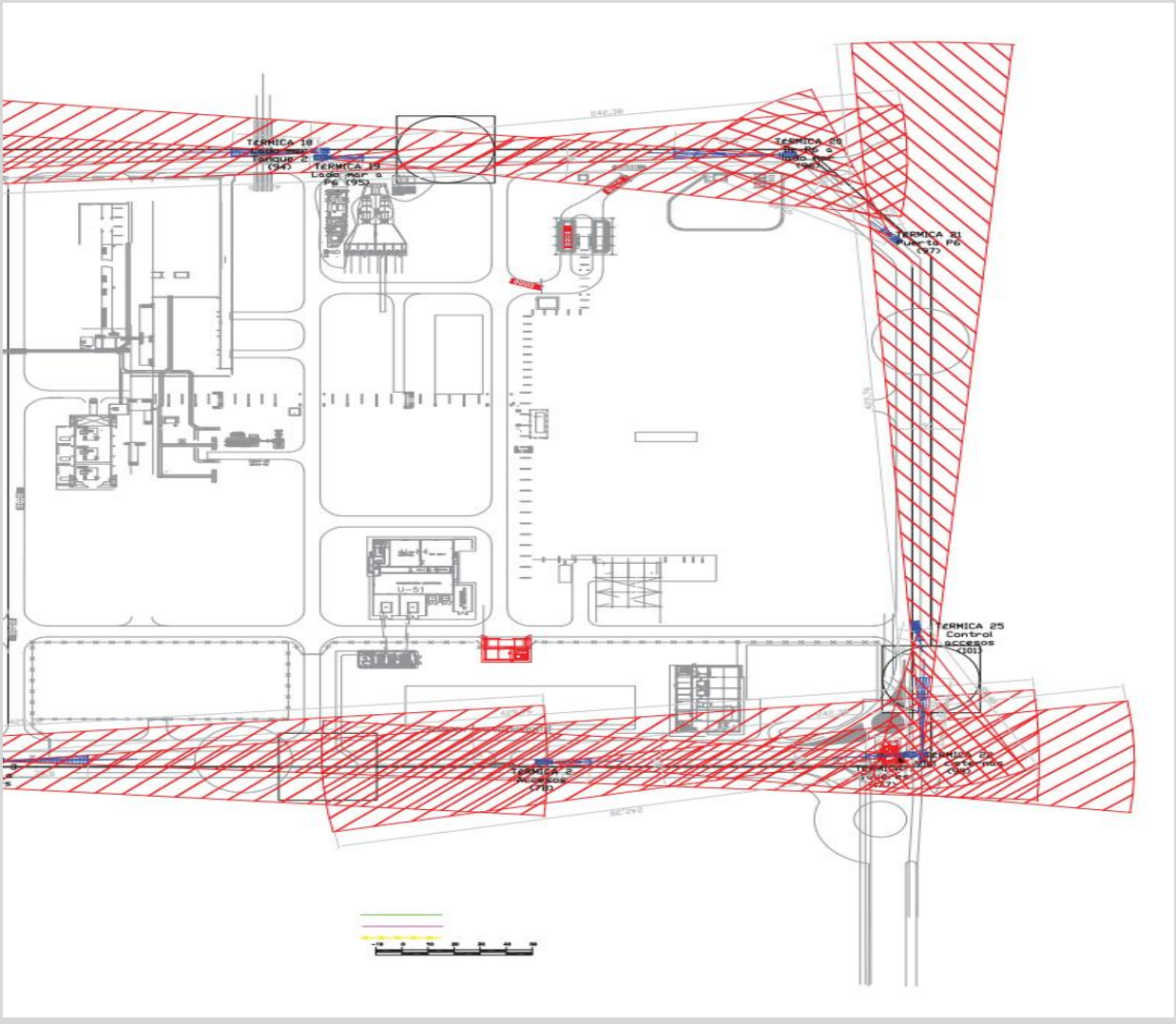
Otro punto a tener en cuenta en la mejora de la seguridad son las múltiples aplicaciones y versiones que existen del mismo programa, es importante que el administrador se decida por una de ella que considere oportuna y realiza la actualización más reciente que se considere segura y esta afecte a todos los equipos ya que por toda la red se encuentran equipos con versiones o aplicaciones desactualizadas que pueden contener vulnerabilidades (véase índice)

3. SEGURIDAD PERIMETRAL

3.1. SEGURIDAD FÍSICA

Las instalaciones de la empresa disponen de un gran extenso circuito cerrado de televisión (CCTV) que controla todo el perímetro para detectar posibles intrusos que quieran acceder de forma no autorizada al recinto. Las cámaras están controladas en todo momento por los vigilantes de seguridad. El servicio de vigilancia supone la primera barrera física para entrar a las instalaciones, deben comprobar la identidad de toda persona que intenta acceder al perímetro y denegar o autorizar el acceso. Las políticas de acceso al recinto y políticas de seguridad en general son conocidas por todo el personal de la empresa.

Toda la planta dispone de sensores de humo y gas los cuales están conectados a la red con el fin de hacer saltar el sistema EDS en caso de emergencia. Además, estos sensores como otros puntos delicados esta vigilados adicionalmente a través de sistemas de alarmas conectadas directamente con el personal de vigilancia.



3.2. SEGURIDAD LÓGICA

La red dispone de un sistema de detección de intrusos, basada en el sistema DIDS, basado en la arquitectura cliente-servidor (el cual se encuentra en NOEGAS) los cuales se encargar de monitorizar la actividad de los equipos y detectan cualesquiera acciones extrañas por parte de los usuarios.

La herramienta principal de la empresa para protegerse ante ataques externos es un complejo sistema de firewalls, cada uno realiza una función específica y están integrados con los antivirus para que en caso de fallo se pueda eliminar el software malicioso antes de que pueda llegar a infectar los equipos. Actualmente la configuración de los cortafuegos la lleva a cabo NOEGAS cuyos administradores se encargan de su correcta configuración

Para transferir información confidencial a través del grupo de empresas, NOEGAS dispone de un PKI y un sistema de firma digital. Siempre que se quiera compartir información sensible a través de las diferentes empresas se deberá seguir el siguiente procedimiento el cual es conocido por todos los empleados y cada uno dispone de su propio par de claves (clave pública y clave privada). A través de técnicas criptográficas y funciones hash logran que toda comunicación cumpla con las políticas de confidencialidad, integridad y no repudio de información.

Como barrera de defensa perimetral lógica, los servidores de almacenamiento de encuentran en una zona desmilitarizada (DMZ) de esta forma se evita que los servidores y la red corporativa tengan contacto directo y toda comunicación sea controlada y gestionada a través de los firewalls. La DMZ utiliza un complejo sistema de firewalls que le permite detectar tanto paquetes maliciosos que intentan entrar a la red y también, escáneres de puertos.

Un punto clave en la seguridad perimetral de la empresa es la red inalámbrica que dispone ya que es un foco ante ataques sniffers, es por ello que para proteger la seguridad de la información a través de este medio de comunicación la empresa utiliza el estándar IEEE 802.11n. A través de este protocolo sólo aquellos dispositivos que tienen su dirección MAC registrada y autorizada por el administrador pueden acceder a esta red.

Un punto a mejorar en la seguridad perimetral por parte de la empresa es el uso de switches en lugar de hubs en las diferentes subredes que conforma la empresa. Pese a que suponen un coste añadido, los switches proporcionan una mayor eficiencia que los hubs y una mayor seguridad ya que solo reenvían los paquetes de información al destinatario en cuestión y no a todos los usuarios de la red, lo que supone una gran herramienta para evitar y reducir el impacto que pueda causar un sniffer.

4. 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 más 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.

5. 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

6. 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

7. 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.

8. ANEXO

8.1. BIBLIOGRAFÍA / DISCLAIMER

He intentado hacer el trabajo sobre una empresa real, de lo cual me he arrepentido bastante a medida que lo iba haciendo. Por temas de confidencialidad no puedo usar los nombres reales ni información muy concreta sobre la empresa que lo he hecho, pero si quieres ver las fuentes de donde he sacado toda la información no tengo ningún problema en mostrarla, pero no me dejan enviarla.

8.2. 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

CÓDIGO	DESCRIPCIÓN	FABRICANTE	VERSIÓN	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* Release: R3.75.00	Estación STN0234
PRM	Gestión Instrumentos HART	Yokogawa	R3.31.00	Estación STN0233
Windows 7 Pro	Sistema Operativo	Microsoft		Estaciones de operación e ingeniería.

8.3. INVENTARIO DE EQUIPOS DE LA RED CORPORATIVA Y CPD

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)

DESCRIPCIÓN	FABRICANTE	MODELO
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