Guía de acceso seguro a los dispositivos de campo

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe cert_

Marzo 2019

INCIBE-CERT_GUIA_ACCESO_SEGURO_DISPOSITIVOS_CAMPO_2019_v1

Índice

Índice de figuras

1. Sobre esta guía

En esta guía se recogen diferentes métodos para mejorar el nivel de seguridad a la hora de acceder a dispositivos de campo en un entorno industrial.

Con el fin de identificar las medidas de seguridad adecuadas, se han clasificado los tipos de accesos: local, red corporativa y remoto. Para cada uno de ellos, se propone una arquitectura de referencia y medidas de seguridad a implantar con el objetivo de proteger el acceso a los dispositivos de campo, a la vez que se permite cubrir las diferentes necesidades que pueden aparecer en una industria.

2. Introducción

En el pasado, las redes industriales se encontraban totalmente aisladas de las redes externas, sin posibilidad alguna de establecer accesos desde fuera de ellas, por lo que cualquier posible acceso fraudulento a la red corporativa no afectaba directamente a la industrial. Además, la única medida de seguridad que se llevaba a cabo en ellas era un control exhaustivo sobre el acceso físico a los dispositivos. Gracias a este control, se pretendía que los dispositivos fueran operados únicamente por usuarios legítimos autorizados y dificultar así a cualquier posible acceso fraudulento.

La creciente necesidad de reducir costes operacionales y de fabricación, junto con la necesidad de acceder a los datos en tiempo real, ha obligado a las empresas a modificar sus arquitecturas de red, conectando la parte industrial con la corporativa de la empresa o incluso con otras externas. Al eliminarse esta separación entre zonas, se pierden las medidas de seguridad implícitas en el uso de segmentación de redes. Con este cambio de infraestructura, las medidas de seguridad llevadas a cabo hasta el momento dejan de ser suficientes.

Por esta razón, surgen nuevas necesidades de seguridad, como la correcta separación de los distintos segmentos de la red industrial para evitar que un incidente de campo pueda afectar a la parte de supervisión o la segregación entre el tráfico corporativo y el industrial de manera que un ataque ocurrido en red corporativa no afecte a la red industrial, sin olvidarnos de la importancia de controlar las actualizaciones y asegurar los accesos provenientes de redes externas a la empresa, principalmente de proveedores, pero también de empresas de mantenimiento.

Una correcta arquitectura de red debería implementar, por tanto, una adecuada separación entre los distintos segmentos de red y proporcionar mecanismos de autenticación lo suficientemente robustos para evitar accesos indebidos.

3. Organización del documento

Este documento consta de un apartado introductorio a los niveles de red, que contiene una explicación de los distintos niveles que componen una red según el estándar ISA-95, así como su correspondencia con las distintas arquitecturas de red propuestas. Tres apartados principales recogen diferentes métodos de acceso a los dispositivos de campo divididos según el tipo de acceso de la siguiente forma:

Acceso local, donde se focaliza en el acceso desde la propia red y el acceso físico a los equipos. El acceso se realiza de manera local a los dispositivos de campo, por lo tanto, el único nivel de red involucrado es el nivel 1, en el que se encuentran dichos dispositivos.

- **Acceso desde red corporativa**, centrado en el acceso a los dispositivos de campo desde la red corporativa, teniendo en cuenta la separación entre las redes y contando con las medidas de seguridad establecidas en el apartado previo. El acceso se realiza desde la red corporativa de la empresa a los dispositivos de campo, por lo tanto, en este caso, intervendrán los niveles de red 4 y 1, además de la red de intercambio de información, por la que se accederá a la red industrial a través de las máquinas de salto.

- **Acceso desde redes externas**, que recoge el modo seguro de acceder hasta los dispositivos de campo desde una red externa a la empresa. El acceso se realiza desde la red externa a los dispositivos de campo, interviniendo los niveles de red 4 y 1, además de la red externa y la de intercambio de información (*Demilitarized Zone*, DMZ), por la que se accederá a la red industrial a través de las máquinas de salto, de la misma manera que en la segunda arquitectura.

Cada una de las arquitecturas propuestas se presenta siguiendo la misma estructura

- Situación inicial de la arquitectura de red y los problemas de seguridad que se pueden dar en la misma.

- Elementos involucrados, activos y agentes, en la arquitectura propuesta.

- Arquitectura de seguridad propuesta como solución para el acceso.

- Otros mecanismos de seguridad adicionales que se pueden implementar para mejorar aún más la seguridad en los accesos.

Por último, se incluyen unas conclusiones que ponen en valor las ventajas que proporciona la adopción de estas arquitecturas y una sección de anexos donde se detallan los mecanismos de seguridad adicionales descritos en cada una de ellas.

4. Niveles de red

En este documento se hacen numerosas referencias a los diferentes niveles de un sistema de control industrial. Para la definición de estos niveles se toma como referencia la arquitectura de red definida en el estándar ISA-95[1], mostrado en la Figura 1, en la que se definen 5 niveles para las redes industriales, divididos según su aplicación principal.

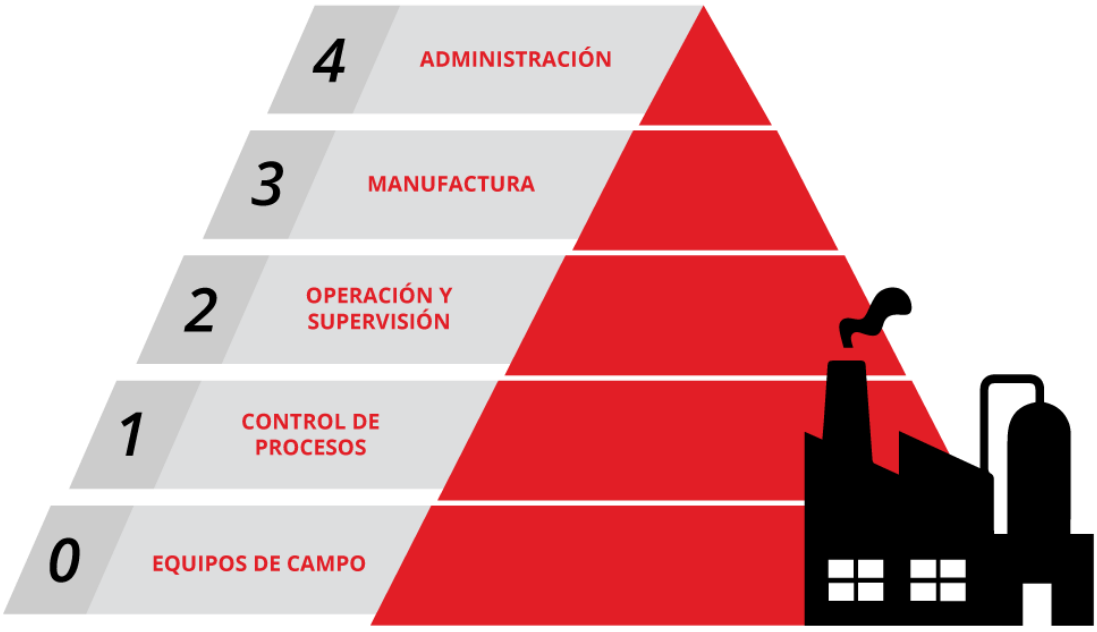

Figura 1.- Pirámide de niveles según ISA-95

- **Nivel 0:** se corresponde con los equipos de campo englobados en el propio proceso productivo, es decir, se compone de los sensores y actuadores que forman parte del proceso industrial.
- **Nivel 1:** correspondiente al control de procesos. Es el nivel en el que se produce la interacción entre la parte física (nivel 0) y los sistemas de control más básicos, los PLC (*Programmable Logic Controller*), DCS (*Distributed Control System*), sensores y actuadores.
- **Nivel 2:** se corresponde con los equipos de operación y supervisión, ya sea de manera local mediante equipos HMI (*Human Machine Interface*) o de una manera centralizada mediante el uso de SCADA (*Supervisory Control And Data Acquisition*).
- **Nivel 3:** se encuentran los equipos de manufacturación. Este nivel controla el flujo de la producción y también el almacenamiento de la información del proceso.
- **Nivel 4:** agrupa las actividades relacionadas con el desarrollo de negocio en una organización industrial, la red corporativa.

[1] https://www.isa.org/isa95/

Estos niveles se pueden trasladar casi directamente a niveles de red, pero se han de tener en cuenta otros dos niveles adicionales:

- **La red de intercambio de datos:** es una red DMZ donde se situarán, entre otras máquinas, las máquinas de salto por las que se accederá a la red industrial desde la red corporativa.
- **La red externa:** incluye todas las comunicaciones con el exterior y conforma la última red de la infraestructura.

5. Arquitectura de acceso seguro a dispositivos de campo (Acceso local)

El acceso típico a los dispositivos de campo se suele realizar desde la propia red de campo o localmente en el dispositivo, aunque hoy en día sea más habitual hacerlo a través de accesos remotos. En este apartado, veremos la problemática que puede surgir al no realizar estos accesos de manera correcta y qué medidas podrían implementarse para que si lo sean.

El tipo de acceso que se detalla en esta sección será el acceso directo al dispositivo físico y el acceso desde la red local.

5.1. Situación inicial de la red

Para este caso concreto de acceso local supondremos que inicialmente todos los equipos de la red de campo se encuentran en el mismo segmento y no se ha realizado ningún tipo de segregación por criticidad. Además, no se ha implementado ningún mecanismo de autenticación en los dispositivos, ni se mantienen medidas de seguridad físicas sobre los mismos.

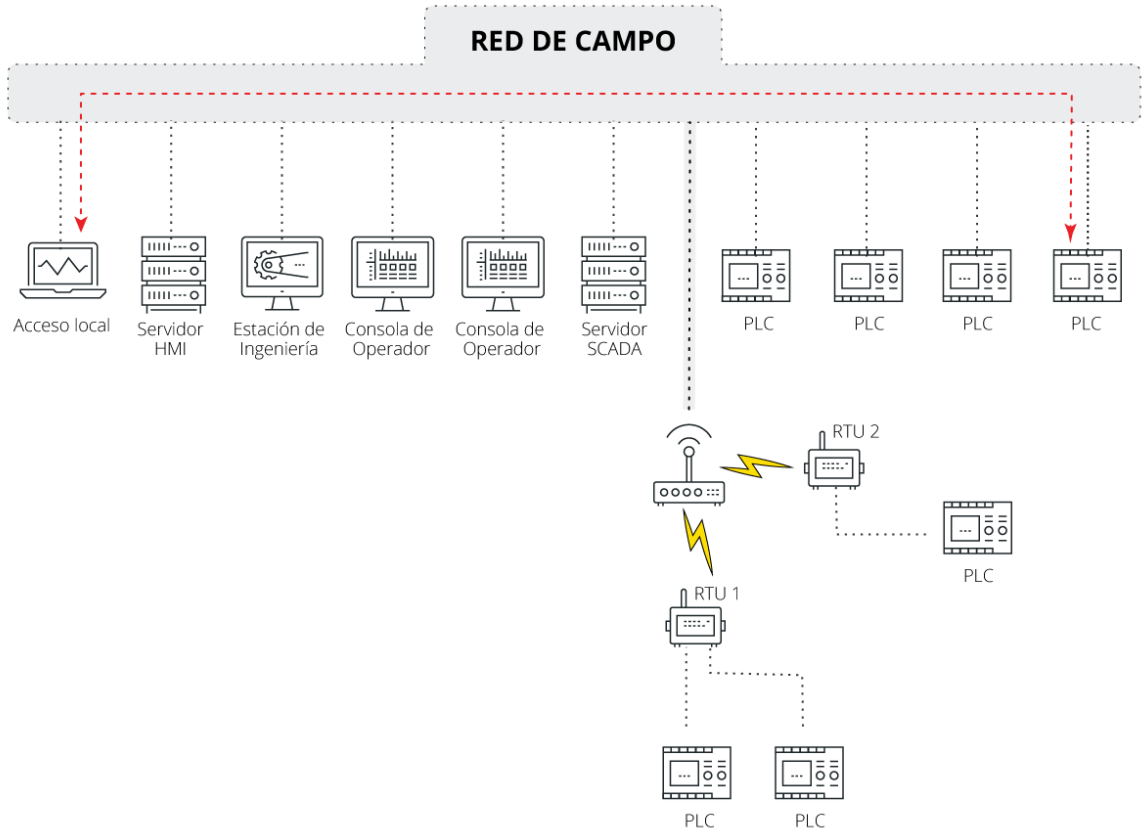

Figura 2.- Estado inicial de la red de campo

5.2. Identificación de los elementos involucrados a nivel de campo

Para realizar el acceso desde la propia red de campo o de manera local a los dispositivos de la red de control es necesaria la participación de diferentes elementos, entre los que se identifican al menos:

- El equipo de la red de campo al que se desea acceder.
- Un operador que realiza el acceso físico.
- Un dispositivo en la misma red para el acceso local.

5.3. Solución propuesta

El principal problema que se plantea en un acceso de tipo físico (acceso directo utilizando un panel de control y pantalla integrados en el propio dispositivo) es la falta de mecanismos de autenticación o el uso de mecanismos poco seguros. Por norma general, los dispositivos suelen disponer de un control de accesos de este tipo poco robusto, basado en un PIN de acceso o similar, si bien es cierto que los dispositivos modernos suelen incluir importantes mejoras en este aspecto, que van desde el uso de contraseñas más complejas hasta el uso de RBAC (control de accesos basado en roles).

Si no se implementa ningún mecanismo de autenticación, o el que se implementa es poco seguro, cualquier usuario con acceso físico al dispositivo podría realizar acciones en él, legítimas o no. Por este motivo, el acceso físico debería contar con el mismo nivel de seguridad que el acceso a cualquier servicio de red, es decir, contar con un sistema de autenticación y autorización seguro. La autenticación local, método utilizado generalmente, puede mejorarse realizando una autenticación delegada, basada en LDAP, por ejemplo, o incluso añadiendo más niveles de seguridad mediante sistemas RADIUS o TACACS/TACACS+. Además de conseguir elevar la seguridad en la autenticación, se descarga al dispositivo de la gestión local de los usuarios, lo que permite una mejora en la trazabilidad de las acciones.

Por otro lado, si no se implementan controles de acceso físico sobre los dispositivos, cualquier dispositivo que dispusiera de interfaz física podría ser susceptible de un uso inadecuado por parte de usuarios sin autorización. Por ello, todos los dispositivos deberían encontrarse en lugares protegidos, como armarios con llave o salas con controles de acceso, basados por ejemplo en tarjetas magnéticas o, identificación de huellas. Se implementarán las medidas necesarias para garantizar que solo los usuarios con acceso legítimo pueden acceder a los equipos de campo. Estas medidas incluyen la identificación de los usuarios que quieran acceder a la planta donde se encuentren los dispositivos, así como controles de vigilancia.

El otro punto de acceso, mediante red local, puede protegerse mediante dos vías. Por un lado, está la propia protección de los servicios publicados por el dispositivo y, por otro, la protección de la red.

La protección de los servicios debería hacerse como se ha indicado anteriormente para el acceso físico, es decir, utilizando sistemas de autenticación y autorización seguros y, en caso de ser posible, delegados.

La falta de segregación de los equipos es una debilidad que puede presentarse en la red, por ello, es importante separar los equipos en la red según parámetros como, por ejemplo,

criticidad, funcionalidad o proceso, de manera que se garantice que los usuarios con acceso a equipos de criticidad baja no pueden tener acceso a los equipos de mayor criticidad. Los dispositivos han de encontrarse separados en diferentes zonas[2] dentro de la red, que deberían estar aisladas y con comunicación limitada, controlada y solo en los casos necesarios. De esta forma, se garantiza que un posible incidente en un equipo de criticidad baja no podrá afectar a un equipo de mayor criticidad.

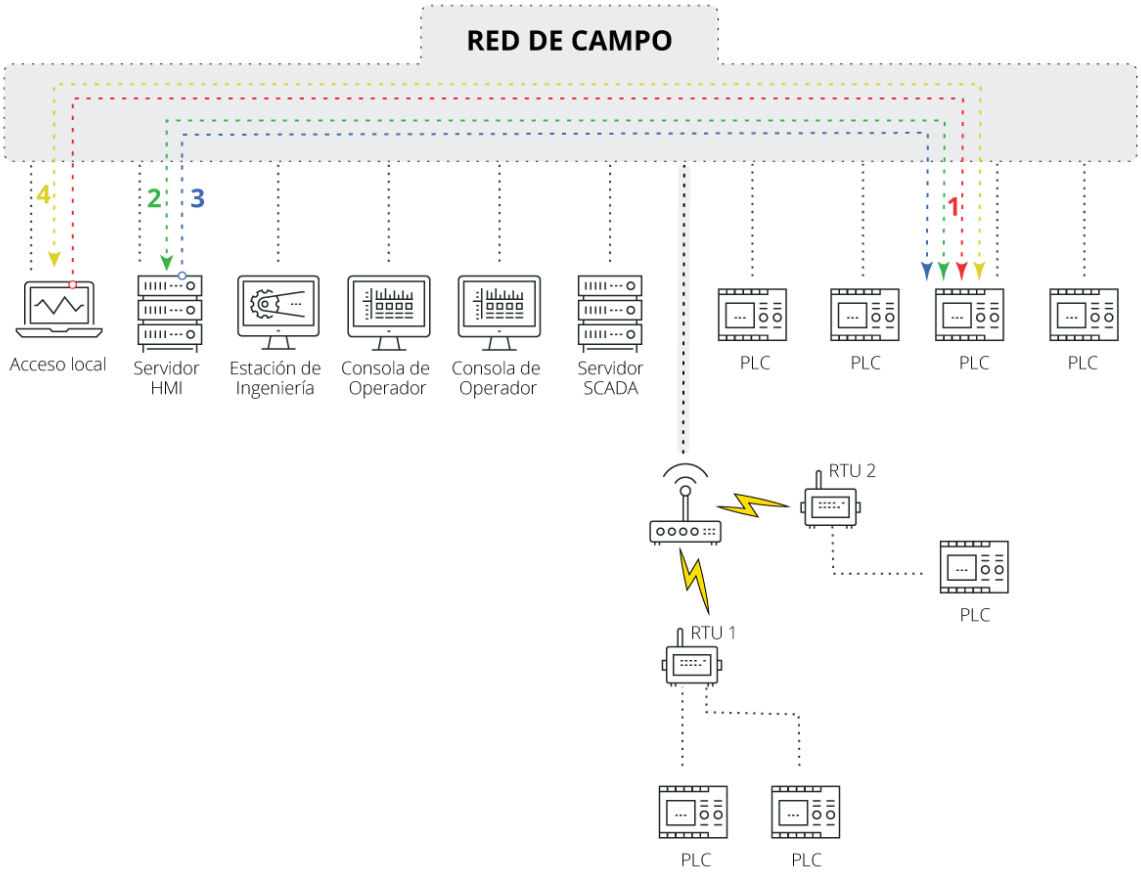

Figura 3.- Estado con mecanismos de seguridad de la red de campo

Siguiendo estos mecanismos de seguridad un operario que quisiera acceder a un equipo de campo desde la red local deberá iniciar sesión en el dispositivo introduciendo su usuario y contraseña. Si el operario desea iniciar sesión de manera física en el dispositivo deberá de tener los permisos para el acceso físico al dispositivo e iniciar sesión utilizando también su usuario y contraseña para el acceso local.

Si los dispositivos finales disponen de mecanismos de log, sería deseable que se implementase un mecanismo de centralización de logs de manera que todos los accesos quedasen registrados y documentados.

[2] Zonas y conductos, protegiendo nuestra red industrial - https://www.incibe-cert.es/blog/zonas-y-conductos-protegiendo-nuestra-red-industrial

5.4. Otros mecanismos de seguridad

Aunque no ayude a incrementar el nivel de seguridad de manera directa, cambiar los banners o mensajes de bienvenida de los equipos, si lo hace de forma indirecta.

Todos los equipos internos que disponen de servicios accesibles deberían estar configurados para mostrar un mensaje de alerta con la información oportuna de la compañía y las condiciones de prestación del servicio que deben ser cubiertas por el usuario. Además, el mensaje debe estar correctamente formado para no incluir datos relevantes de la aplicación, así como versiones o librerías en uso.

6. Arquitectura de acceso seguro desde la red corporativa a la red industrial

Los accesos desde la red corporativa a la red industrial son algo frecuente hoy en día, algo que antiguamente era impensable, al menos de manera directa. En este apartado veremos los problemas que pueden surgir si estos accesos no se realizan de una forma correcta y se propondrá una arquitectura de red que proporcione las medidas de seguridad necesarias para realizar estos accesos de la manera más segura posible.

6.1. Situación inicial de la red

La disposición de las redes industriales y su unión con la red corporativa, en un principio, se hizo pensando en la operativa y no en la seguridad, por lo que se habilitaron los canales de comunicación necesarios.

En esta situación inicial, se permite una conexión directa desde la red corporativa a la red de campo. Esta conexión implica que la red corporativa no se encuentra aislada de la red de campo y no se ha implementado ningún elemento de seguridad intermedio, como un cortafuegos. La Figura 4 refleja este acceso y los elementos involucrados.

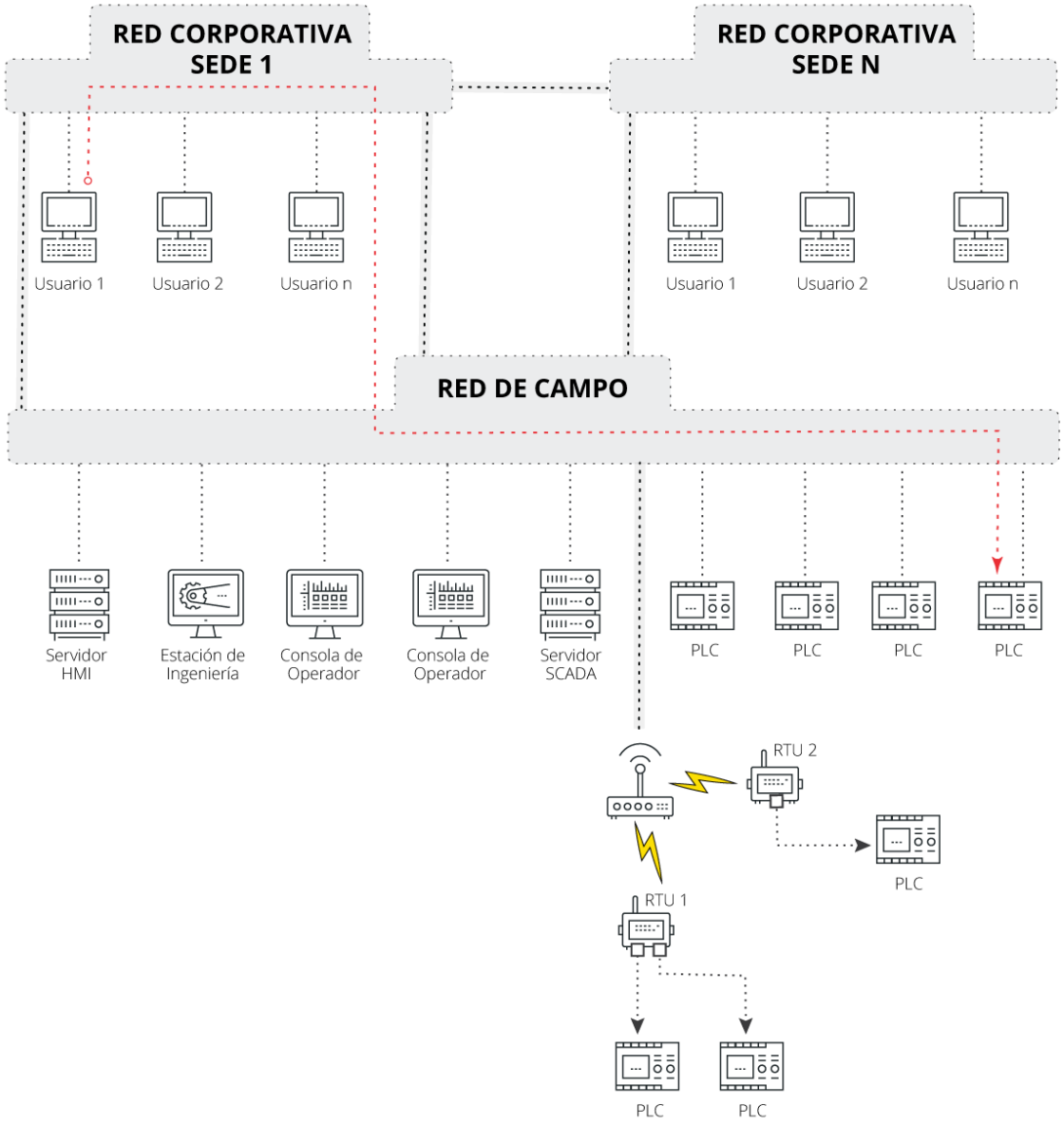

Figura 4.- Arquitectura inicial de acceso desde la red corporativa

Siguiendo esta arquitectura, cualquier equipo de la red corporativa podría acceder a cualquier equipo de la red industrial, lo que supondría tener que controlar numerosos puntos de acceso entre las redes para impedir que un incidente se propague de una red a otra.

6.2. Identificación de los elementos involucrados a nivel de empresa

Para conseguir el acceso desde la red corporativa hasta los dispositivos de la red de control es necesaria la participación de diferentes elementos, entre los que se identifican al menos:

- Un usuario de la red corporativa que realiza el acceso.
- El equipo de la red corporativa desde el que se realiza el acceso.
- El dispositivo final de la red de campo al que se accede.
- Los routers y switches distribuidos a lo largo de toda la red entre el equipo origen y el dispositivo destino.

A estos dispositivos hay que añadir todos aquellos que aportan la seguridad a las comunicaciones, entre los que se pueden identificar:

- Los cortafuegos perimetrales que separan la red industrial de la red corporativa.
- La máquina de salto encargada de establecer la conexión.
- El cortafuegos industrial que separa la red de campo del resto de las redes industriales.

6.3. Solución propuesta

Los problemas de seguridad basados en un acceso desde la red corporativa a la red de campo son numerosos y por esta razón se ha de realizar de una manera que minimice lo máximo posible los riesgos de seguridad.

Permitir una conexión directa entre la red corporativa y la red industrial se saltaría todas las buenas prácticas de defensa en profundidad, como las recogidas en la guía NIST 800-82[3], la cual tomaremos como referencia. Siempre que sea posible, se deben mantener los puntos de entrada a la red industrial al mínimo, de esta manera se reducen los riesgos de un acceso malicioso a la red industrial.

Por este motivo, es preciso mejorar la arquitectura de red para, por un lado, agrupar los posibles puntos de acceso en un único punto, y, por otro, poder incorporar medidas de seguridad que minimicen el riesgo.

Para un acceso seguro a las arquitecturas de red, se recomienda como mínimo, seguir las siguientes medidas:

- **Establecer mecanismos de autenticación robustos:** si no se dispone de unos suficientemente robustos y seguros, cualquier usuario, legítimo o no, con acceso a la red corporativa podría acceder a la red industrial.
- **Implementar una correcta gestión de los usuarios y sus permisos:** es muy importante que se siga una política correcta de gestión de usuarios, roles y permisos. Esta política debe establecer a los usuarios los mínimos permisos que necesiten en su actuación. Además, se debe restringir el acceso de los usuarios únicamente a los equipos desde los cuales estén destinados a operar.
- **Establecer una política de contraseñas segura:** la gestión adecuada de usuarios no sería efectiva si la política de contraseñas utilizada, no es adecuada. Por ello, los usuarios deben seguir una política de contraseñas de manera que sean lo más

[3] NIST 800-82 - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

robustas posible, evitando así posibles ataques de fuerza bruta. Esta política de contraseñas[4], como mínimo, debería cumplir con la política de contraseñas de nuestra guía de políticas de seguridad para la pyme[5].

- Implementar una **segregación y segmentación de la red** según los niveles establecidos en el estándar ISA 95.
- Implementar mecanismos de **monitorización de la red y de centralización de log**.

Siguiendo estas pautas de buenas prácticas, la red industrial se mantendría más protegida en el caso de que un activo de la red corporativa con acceso a ella se viera comprometido, y, además, se minimizaría la exposición frente a posibles ataques a la red industrial, arquitectura que se recoge en la Figura 5.

[4] Uso de patrones en las contraseñas, o como arruinar tu propia seguridad - https://www.incibe-cert.es/blog/uso-patrones-las-contrasenas-o-arruinar-tu-propia-seguridad

[5] Contraseñas, políticas de seguridad para la pyme - https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

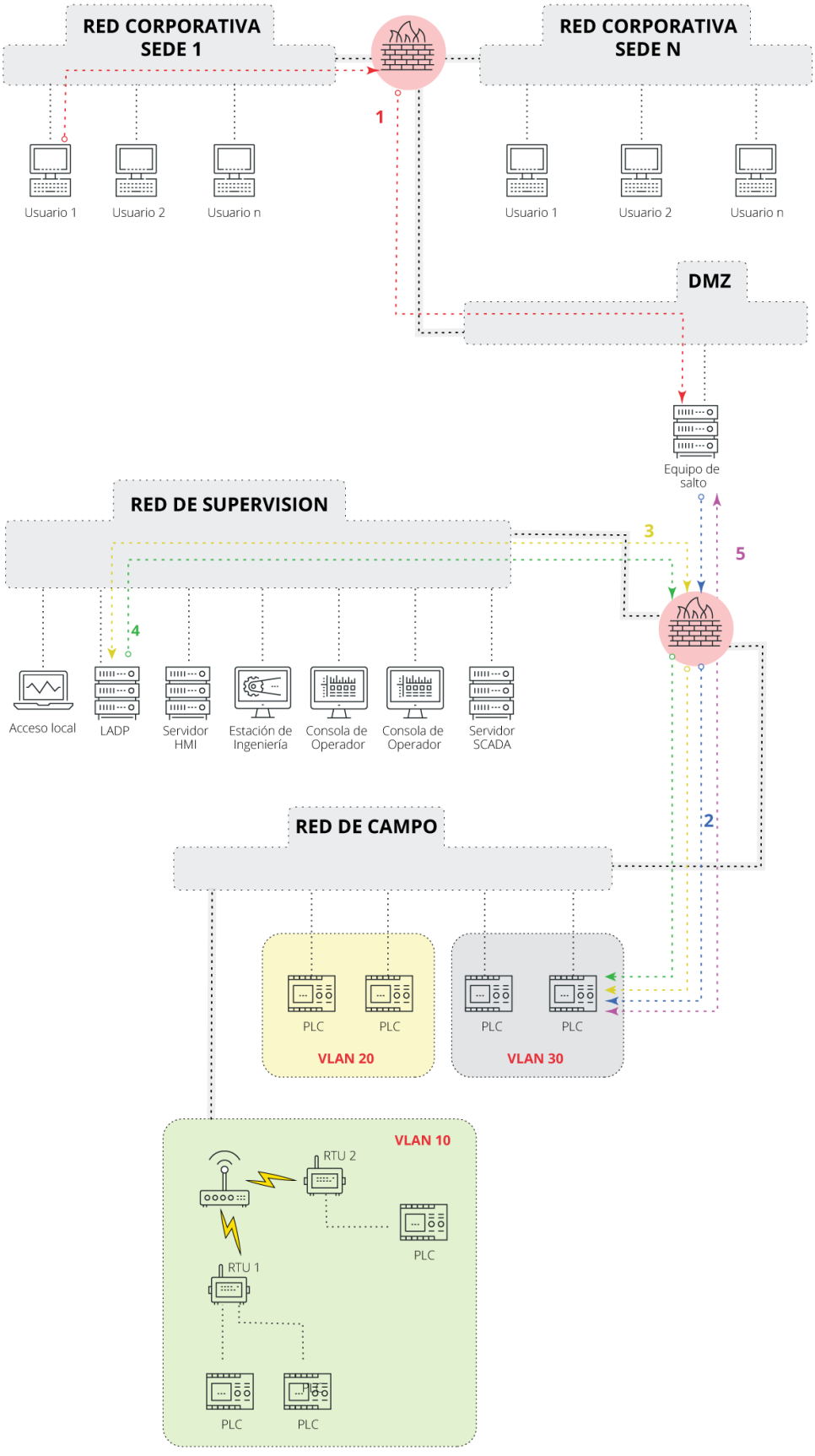

Figura 5.- Arquitectura final con seguridad de acceso desde la red corporativa

La configuración de la red y la segregación de tráfico debe hacerse mediante un cortafuegos. Éste deberá garantizar que el tráfico entre la red corporativa y la red industrial se lleva a cabo únicamente a través de la DMZ. Además, el cortafuegos deberá garantizar que todo el tráfico sin autorizar es denegado.

Como se ve, el acceso debería hacerse mediante un equipo de salto. La solicitud de acceso debe ser dirigida hacia esta máquina de salto, la cual gestionará el acceso en función del usuario que ha realizado la petición. La máquina de salto deberá encontrarse en la red de intercambio de datos (DMZ) y, además, separada del resto de la infraestructura. Si fuera posible, se deberían de tener máquinas de salto, habitualmente en formato virtual, para cada usuario/tipo de acceso perteneciente a la red corporativa que necesite acceder a los equipos de campo. Estas máquinas de salto deberán estar bastionadas con el fin de impedir accesos no autorizados o la ejecución de servicios innecesarios. Una vez se termina la actuación sobre el equipo de la red de campo o el tiempo de sesión expira, es suficiente con que el usuario suspenda o cierre la sesión activa.

El equipo de salto debería disponer de una solución que cuente con un adecuado sistema de autenticación del usuario. Se debe garantizar inequívocamente que el usuario que intente establecer la conexión a los equipos de la red de campo es realmente el usuario legítimo.

Para evitar que un atacante con acceso a la red pudiera capturar el tráfico y obtener las credenciales de acceso, el protocolo utilizado para la comunicación desde la red corporativa debe utilizar métodos de autenticación bien configurados y robustos, como el uso de RADIUS o TACACS+, o incluso disponer de una solución VPN de forma opcional.

Por último, todo el tráfico de la red industrial debería ser monitorizado y registrado en los servidores de log, conjuntamente con los logs de los dispositivos y elementos de red. De esta manera, se podría detectar cualquier anomalía y reducir los efectos de un potencial incidente. Para ello, se recomienda el uso de herramientas SIEM, cuya guía[6] de despliegue y configuración se encuentra disponible también en nuestra página.

La seguridad desde el equipo de salto hasta los dispositivos finales se tomará como un acceso local, y deberá seguir las pautas marcadas en el apartado 5.-Arquitectura de acceso seguro a dispositivos de campo (Acceso local).

6.4. Otros mecanismos de seguridad

Como mecanismo de autenticación adicional se propone el uso del doble factor de autenticación[7] para el acceso al equipo de salto. Implementar el mecanismo de doble factor de autenticación permitiría que, en el caso de haber sufrido un robo de credenciales o un ataque de fuerza bruta, el atacante no podría iniciar sesión, ya que necesitaría superar el segundo factor.

[6] Diseño y configuración de IPS, IDS y SIEM en Sistemas de Control Industrial - https://www.incibe-cert.es/guias-y-estudios/guias/diseno-y-configuracion-ips-ids-y-siem-sistemas-control-industrial

[7] Doble factor de autenticación - https://www.incibe-cert.es/blog/acceso-seguro-los-sci-doble-factor-y-accesos-externos

7. Arquitectura de acceso remoto a la red industrial

Hoy en día son bastante comunes los accesos externos a la red industrial por parte de operadores o incluso de fabricantes que desean aplicar actualizaciones en los dispositivos de campo. En este apartado, veremos los problemas que pueden surgir si estos accesos no se realizan de una forma correcta y se propondrá una arquitectura de red que proporcione las medidas de seguridad necesarias para realizar estos accesos de la manera más segura posible.

Este apartado se centra en un acceso remoto de manera externa a la red de la empresa.

7.1. Situación inicial de la red

En la situación inicial los equipos de la red de campo están conectados directamente a Internet. Esta conexión implica que la red industrial no se encuentra aislada de Internet y no se ha implementado ningún elemento de seguridad intermedio como un cortafuegos. En la siguiente figura se ve reflejado este acceso y los elementos involucrados:

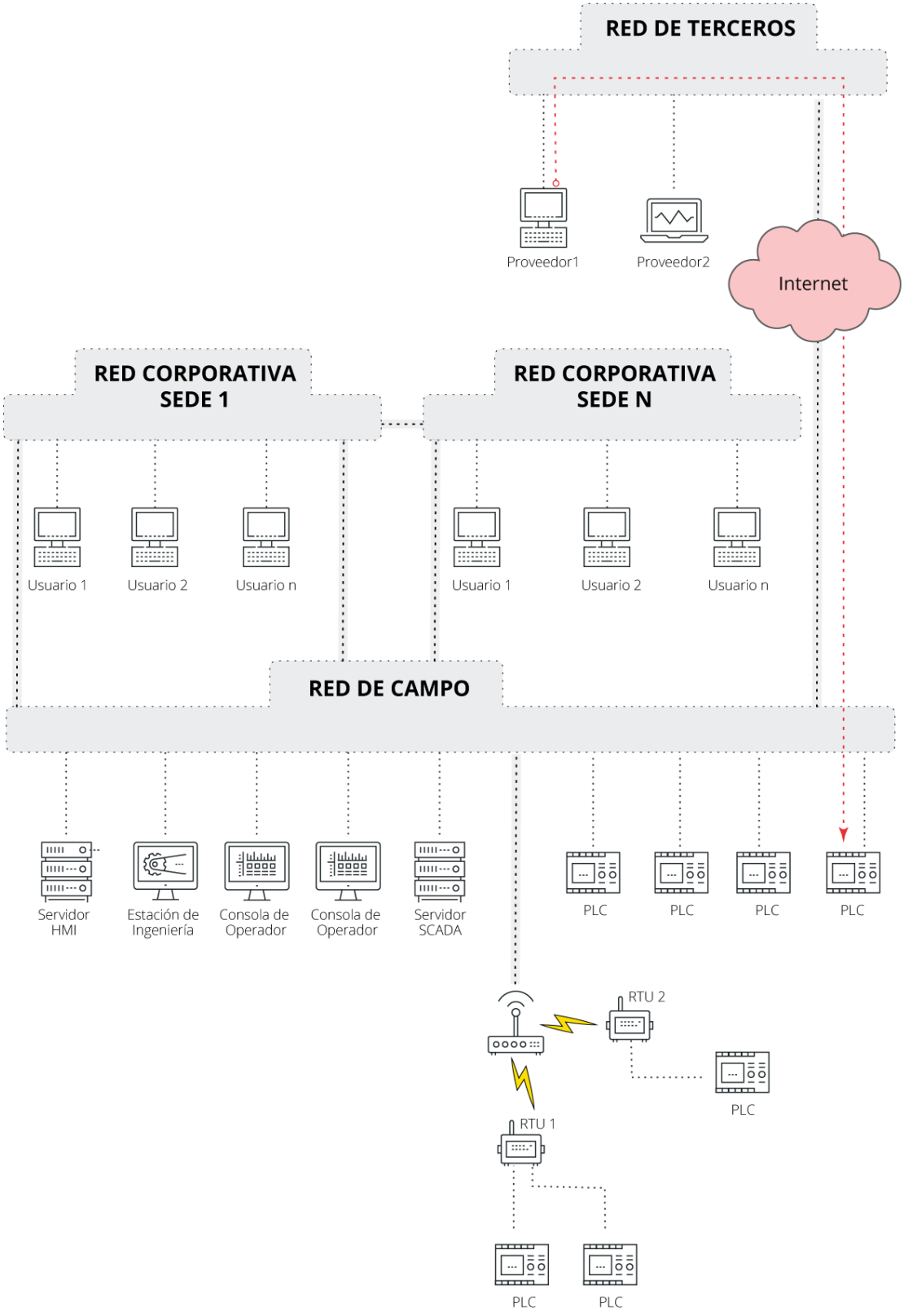

Figura 6.- Arquitectura inicial de acceso a SCI

7.2. Identificación de los elementos involucrados a nivel externo

Para conseguir el acceso desde una red externa hasta los dispositivos de la red de control es necesaria la participación de diferentes elementos, entre los que se identifican al menos:

- El equipo de la red de campo al que se accede.
- El usuario que realiza el acceso desde Internet.
- Los *routers* y *switches* distribuidos a lo largo de toda la red.

A estos dispositivos hay que añadir todos aquellos que aportan la seguridad a las comunicaciones, entre los que se pueden identificar:

- Los cortafuegos que separan la red corporativa de internet.
- Los cortafuegos perimetrales que separan la red industrial de la red corporativa.
- Las máquinas de salto intermedias ubicadas en la red corporativa.
- Las máquinas de salto ubicadas en la red industrial.
- Los cortafuegos industriales que separan la red de campo del resto de las redes industriales.

7.3. Solución propuesta

Un acceso a la red de campo desde una red externa, aunque en ocasiones sea necesario, implica una serie de riesgos que han de ser tenidos en cuenta a la hora de permitir este tipo de accesos. Estos riesgos deberán de ser debidamente mitigados disponiendo de las medidas de seguridad necesarias para garantizar que la actividad realizada es la legítima.

El principal riesgo que surge de la realización de este tipo de accesos es la exposición de la red industrial. Siempre que sea posible, se deben minimizar los puntos de entrada a la red industrial, ya que permitir una conexión directa de un dispositivo de campo a Internet significaría la exposición de la red industrial a cualquier usuario, legítimo o no, de Internet. También hay que tener en cuenta que al realizarse los accesos desde el exterior cualquier incidente que afectase a la red externa, podría propagarse a la red industrial.

La primera buena práctica a seguir a nivel de política interna y antes de realizar ninguna otra acción, es la petición de actuación por parte del usuario externo que desea realizar el acceso. En esta petición se debe reflejar el motivo de la actuación, quien la realiza y los dispositivos sobre los que se va a realizar la actuación. Es recomendable que todas estas peticiones queden registradas de manera que se posea un histórico de actuaciones en los dispositivos teniendo constancia de quién realizó el acceso, cuándo, en qué dispositivo/os y las acciones realizadas. Muchos de los dispositivos no disponen de mecanismos para hacer estos registros, y solo podrá registrarse el acceso a la máquina de salto o en los elementos de red que se atraviesen. Para que el registro sea adecuado, sería ideal disponer de un sistema de centralización de eventos[8].

Aprobada la petición de actuación, el usuario accederá a través del cortafuegos perimetral de la empresa a la red corporativa mediante VPN. La conexión VPN ha de estar configurada para el uso de cifrados robustos y para solicitar doble factor de autenticación[9]. De esta

[8] Registrando eventos en sistemas de control para mejorar la seguridad - https://www.incibe-cert.es/blog/registrando-eventos-sistemas-control-mejorar-seguridad

[9] Acceso seguro a los SCI: doble factor y accesos externos - https://www.incibe-cert.es/blog/acceso-seguro-los-sci-doble-factor-y-accesos-externos

manera, se garantiza la legitimidad del acceso y la protección de datos en las comunicaciones.

Una vez accedido a la red corporativa, el resto del acceso se realizará de manera idéntica a la ya comentada en el apartado 6.-Arquitectura de acceso seguro desde la red corporativa a la red industrial.

La sesión en la máquina de salto deberá suspenderse y la conexión de la VPN cerrarse tan pronto como la actuación sobre el dispositivo implicado haya finalizado, o bien cuando se haya agotado el tiempo establecido para llevarla a cabo. Evidentemente, dependiendo de la criticidad de la actuación, se conocerá de antemano, gracias a la solicitud, la configuración de la máquina de salto para que no finalice de forma abrupta, sino que pregunte y deje extender el tiempo de sesión.

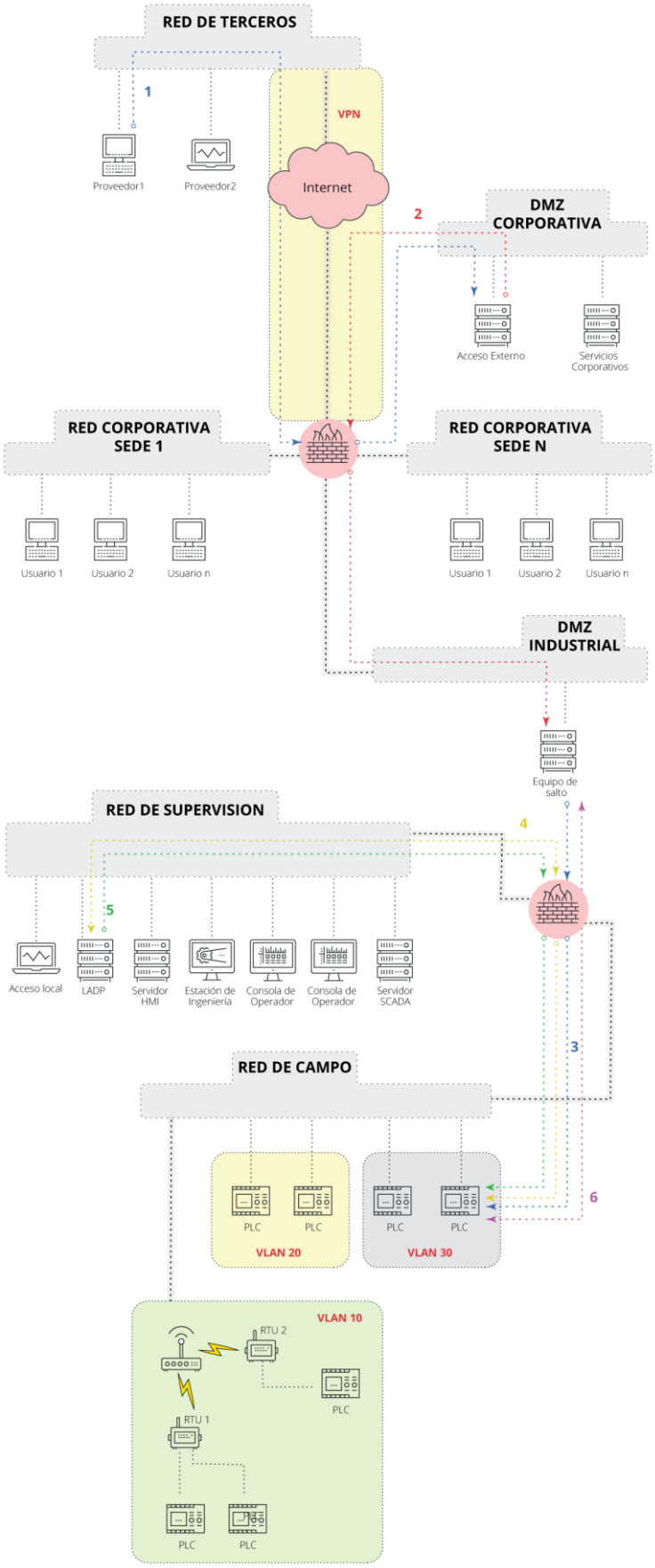

Figura 7.- Arquitectura final de acceso remoto a SCI

7.4. Otros mecanismos de seguridad

Como mecanismo de autenticación adicional se propone el despliegue de un servidor RADIUS[10] el cual va a permitir, de manera segura, realizar una gestión centralizada de los procesos de autenticación, autorización y auditoría de todos los equipos de red. Se recomienda que el listado de usuarios y roles se centralice en el propio servidor RADIUS.

También se recomienda, siempre que sea posible, la implantación de sistemas IDS o IPS[11] en la red. De esta manera se reforzaría la seguridad, ya que cualquier tipo de acceso no deseado sería localizado y bloqueado. Además, se tendría un control más exhaustivo sobre el tráfico de la red.

[10] Protocolos AAA y control de acceso a red: Radius - https://www.incibe-cert.es/blog/protocolos-aaa-radius

[11] IDS e IPS - https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/certsi_diseno_configuracion_ips_ids_siem_en_sci.pdf

8. Conclusiones

Hoy en día, nadie duda que los sistemas industriales deben facilitar información hacia el exterior, lo que obliga a tomar las medidas de control de acceso. No obstante, no solo se trata de proporcionar información, sino también de permitir el acceso para acciones preventivas y de mantenimiento. Todos estos accesos deben hacerse de la manera más segura posible, exponiendo el menor número de equipos posible y siempre de manera controlada por el propietario de éstos, es decir, que nunca debe ser alguien externo a la empresa quien disponga de la capacidad de decidir en qué momento se realiza un acceso y a qué dispositivo.

Las soluciones aportadas en los diferentes apartados que componen este estudio permiten incrementar el nivel de seguridad para cada uno de los distintos tipos de acceso identificados. De forma individual, las empresas industriales deben analizar qué tipo de accesos estarán permitidos a sus dispositivos e implementar las soluciones adecuadas para cada caso.

El futuro tiende a que diferentes servicios de la red industrial se proporcionen desde la nube, pero aún es pronto para vislumbrar cómo se adaptará la normativa a este paradigma y, por tanto, qué soluciones de seguridad se podrán implementar.

9. Anexo I. Mecanismos de seguridad

9.1. Doble factor de autenticación

El mecanismo de doble factor de autenticación es utilizado para reforzar la seguridad en el proceso de autenticación de los usuarios. Su funcionamiento consiste en añadir un elemento extra al, mecanismo habitual de usuario y contraseña. Este elemento extra, puede ser "algo que tenemos", como un *token* USB o tarjeta inteligente, o "algo que somos", como una huella dactilar. El mecanismo de doble factor más extendido es el uso de un código aleatorio generado mediante un *token* hardware o software.

El uso del mecanismo de doble factor permitiría que, en el caso de que se produjera el robo de las credenciales del usuario, el atacante no pudiera acceder al sistema, ya que necesitaría aportar también el segundo factor para poder autenticarse.

9.2. RADIUS

El protocolo RADIUS (*Remote Authentication Dial-In User Service*) pertenece a la familia de protocolos de autenticación, autorización y contabilización (AAA, *Authentication, Authorization and Accounting*), y cuenta con dos elementos principales, el cliente y el servidor:

- El cliente es el encargado de enviar al servidor RADIUS la información proporcionada por los usuarios al servidor y después actuar según la respuesta recibida.

- Los servidores RADIUS reciben la petición del cliente y realizan la autenticación del usuario a partir de los datos recibidos, devolviendo al cliente la información relativa a la conexión del usuario, así como los recursos a los que tiene acceso el mismo. El servidor RADIUS puede realizar de manera complementaria la contabilización de los datos relevantes de la sesión del usuario.

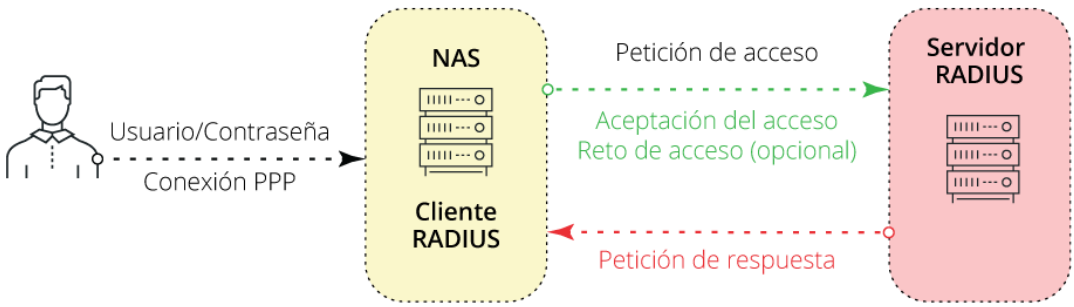

Figura 8.- Flujo de mensajes en un proceso de autenticación/autorización RADIUS

El despliegue de una arquitectura RADIUS en la red permite la gestión de una manera centralizada de la autenticación de los usuarios, así como de la asignación de los recursos a los que tiene acceso y sus permisos.

9.3. IDS/IPS

Un sistema de detección de intrusiones[12] (IDS, *Intrusion Detection System*) permite detectar y monitorizar eventos que ocurren en la red o en un equipo, mediante la detección de anomalías o configuraciones incorrectas en los eventos analizados y la notificación de dichas detecciones.

Un sistema de prevención de intrusiones (IPS, *Intrusion Prevention System*) funciona a grandes rasgos de manera similar a un IDS, sin embargo, una vez detectada una posible intrusión, también es capaz de actuar y bloquearla.

[12] Diseño y configuración de IPS, IDS y SIEM en Sistemas de Control Industrial - https://www.incibe-cert.es/blog/diseno-y-configuracion-ips-ids-y-siem-sistemas-control-industrial

10. Referencias

[1] ISA, ISA95 Enterprise-Control System Integration.

https://www.isa.org/isa95/

[2] NIST, 800-82 Guide to Industrial Control Systems.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf

[3] SANS, Secure Architecture for Industrial Control Systems.

https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

[4] CYBERARK, Next Generation Jump Servers for Industrial Control Systems.

https://lp.cyberark.com/rs/cyberarksoftware/images/wp-CyberArk-NextGenJumpServer-5-28-2014-en.pdf

[5] Homeland Security, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[6] CCI, Estableciendo zonas y conductos

https://www.cci-es.org/documents/10694/613683/Establecimientos+zonas+y+conductos.pdf/a479e3db-81f4-43c1-b5d1-f9e5f7754bcf

[7] Divide y vencerás: Segmentación al rescate

https://www.incibe-cert.es/blog/divide-venceras-segmentacion-rescate

[8] Zonas y conductos, protegiendo nuestra red industrial

https://www.incibe-cert.es/blog/zonas-y-conductos-protegiendo-nuestra-red-industrial

[9] Del Air Gap a la Segmentación en ICS.

https://www.incibe-cert.es/blog/air-gap

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

incibe
cert_