Life Is On | Schneider Electric

Desarrollo y aplicación de la Ciberseguridad en sistemas de monitoreo y control de la energía en el sector del petróleo y gas.

por Roberto Angulo, Adam Gauci y Guillaume Bruandet

Resumen ejecutivo

La industria petrolera, de gas y petroquímica está completamente involucrada en las operaciones de digitalización y tiene una comprensión madura de la ciberseguridad del sistema. Las medidas de reducción de riesgos se han aplicado ampliamente en la parte del proceso de seguridad, pero el control de procesos no es la única vulnerabilidad. Los propietarios de activos también deben enfrentar el Sistema de monitoreo y control de energía (EMCS, por sus siglas en inglés) que administra la energía eléctrica para sistemas de automatización de procesos electro intensivos en los que una fase de digitalización profunda está entrando en vigor durante años.

La metodología de ciberseguridad basada en estándares utilizada en la fase de diseño de un EMCS permite una evaluación de riesgos más completa, un análisis de zonas y conductos más preciso, una especificación de ciberseguridad más detallada y una configuración más precisa del sistema. Las medidas de ciberseguridad específicas del sitio se pueden implementar, probar y validar de manera pragmática durante la construcción para una administración superior de la integridad de los activos

Introducción

A medida que las empresas se enfrentan a las inquietudes de ciberseguridad creadas por una interfaz más amplia entre las plataformas de tecnología de la información (TI) y de tecnología operacional (TO), se ha hecho evidente que las ciberamenazas no se limitan a los riesgos de seguridad de los datos y que es importante mirar más allá de las soluciones tradicionales que abordan sólo algunos de los desafíos.

Establecer la seguridad del Sistema de Monitoreo y Control Energético (EMCS) para la industria petroquímica, y de gas es vital porque las interrupciones a las operaciones pueden exponer a los trabajadores y las instalaciones a riesgos serios y conducir a pérdidas financieras considerables. Asegurar un EMCS más digital permite operaciones adecuadas, continuas y más confiables, lo que ayuda a asegurar la funcionalidad de actividades críticas como el Sistema de Administración de Generación (GMS, Generation Management System) y el Servicio de Descarga Rápida (FLS, Fast Load Shedding), y a proteger a los trabajadores e instalaciones contra daños.

En las operaciones de OT donde las interrupciones pueden tener consecuencias enormes, la seguridad sigue siendo de primordial importancia, pero el concepto tradicional de TI (confidencialidad, integridad y disponibilidad) se ha reordenado para priorizar la disponibilidad por sobre la integridad y la confidencialidad (AIC). Aunque nadie cuestiona la importancia de proteger la integridad de los datos, en el entorno OT, esta preocupación se traslada para ayudar a garantizar la continuidad y la seguridad.

Las empresas del sector del petróleo y gas han estado desarrollando durante años protocolos y procedimientos de ciberseguridad basados en estándares internacionales conocidos, y en la actualidad incluyen requerimientos de seguridad como parte de las especificaciones generales de los subsistemas. El sector se ha vuelto cómodo aplicando estándares de seguridad intersectoriales internacionales, que incluyen estándares de información de seguridad como ISO 27001 para aplicaciones informáticas y en la nube, e IEC 62443 para infraestructura de distribución eléctrica, automatización industrial y EMCS, que la Comisión Electrotécnica Internacional (IEC) define como una "colección de procesos, personal, hardware y software que pueden afectar o influir en la operación segura, segura y confiable de un proceso industrial".

La ciberseguridad es un proceso continuo de evaluación, implementación y mantenimiento en un ciclo cerrado, donde una fase activa la siguiente durante todo el ciclo de vida del proyecto.

Las empresas que desean el mayor nivel de protección para sus activos deben priorizar la seguridad de EMC en la etapa de FEED de una nueva construcción para asegurar que se minimicen todos los riesgos. Para lograr una configuración de EMCS sólida y efectiva, las empresas deben emplear una metodología probada con un enfoque estructurado que incluya una evaluación exhaustiva y sistemática de riesgos y un análisis de zonas y conductos a fin de reunir la información necesaria para que los expertos desarrollen una especificación de ciberseguridad detallada.

Figura 1

Las empresas del sector del petróleo y gas han estado desarrollando durante años protocolos y procedimientos de ciberseguridad basados en estándares internacionales bien conocidos.

La ciberseguridad del ciclo de vida completo ofrece una seguridad superior para los sistemas de monitoreo y control de energía en el sector del petróleo y gas

Trabajar con estándares OT

Una de las primeras acciones que deben realizarse antes de que comience la construcción en una refinería, una planta petroquímica o una unidad de perforación o producción es una evaluación completa del riesgo. Un análisis detallado identifica los riesgos y permite a los propietarios tomar decisiones sobre el nivel de ciberseguridad que se debe aplicar para proteger el EMCS. Con el nivel de seguridad acordado, es posible definir una solución bien estructurada que se pueda desarrollar desde el principio y diseñar de manera que sea fácil de implementar, operar y mantener.

IEC 62443 es el estándar de seguridad global para las redes del Sistema de Control de Automatización Industrial. Desarrollado por la International Society of Automation (ISA), IEC 62443 fue adoptado por la IEC para un desarrollo continuo. El marco de este estándar guía a los operadores de redes de sistemas de control de automatización industrial a través de los requerimientos, controles y mejores prácticas necesarias para crear una red industrial más segura que reduzca el riesgo de tiempos caídos y minimice la exposición a amenazas cibernéticas.

El estándar se basa en el performance, en lugar de ser prescriptivo, y está diseñado para permitir la implementación usando una amplia gama de productos. Por ejemplo, si bien el estándar requiere que se implemente un enfoque de autorización basado en funciones, no determina el uso de un producto, como Windows Active Directory. .

En cada fase del proyecto se debe incorporar orientación del modelo de referencia IEC 62443 y un concepto de defensa en profundidad para lograr la máxima ciberseguridad.

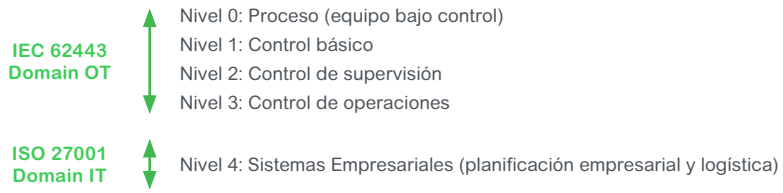


Figura 2
La disponibilidad de repuestos se ve afectada por la programación paulatina de los fabricantes de equipos.

IEC 62443 y diseño de ciberseguridad

Para la mayoría de las empresas, la ciberseguridad se lleva a cabo de una de dos maneras. Las organizaciones que tienen suficiente experiencia en ciberseguridad internamente a menudo aplican sus propias metodologías para que los proveedores las sigan para enfrentar la ciberseguridad de los componentes que proporcionan para su inclusión en el sistema. Por lo general, los líderes de ciberseguridad dentro de la empresa determinan el nivel adecuado de riesgo y especifican el nivel de seguridad adecuado para el proyecto, en algunos casos, con el apoyo de consultores de ciberseguridad de TI.

Otras empresas buscan fuera de la organización la experiencia en ciberseguridad para desarrollar medidas de ciberseguridad específicas de proyectos. Se contrata a una empresa externa de seguridad de TI para llevar a cabo una evaluación de riesgos de alto nivel a fin de establecer el nivel de seguridad que se impondrá a los proveedores. El auditor de TI es responsable del monitoreo continuo y de asegurar las medidas de seguridad de TO propuestas durante el diseño del sistema, mientras enfrenta los riesgos detectados durante la evaluación inicial.

En algunos casos, las empresas no requieren seguridad en la etapa inicial del proyecto y en cambio comienzan a enfrentar los problemas de ciberseguridad cuando el proyecto comienza y el sistema ha sido validado. Este mismo enfoque se aplica a sistemas integrados en proyectos de campo de navegación. Cabe destacar que si bien es posible abordar la ciberseguridad en estas condiciones, a menudo no es posible abordar todos los riesgos potenciales debido a las limitaciones de recursos y disponibilidad, y el tiempo y costo asociados con la remodelación de la ciberseguridad puede ser significativo.

En ambas situaciones, IEC 62443 es la base común para las especificaciones de ciberseguridad, con IEC 62443-2-4 que define cómo se debe manejar y entregar el sistema. El uso de IEC 62443 como base para el desarrollo del sistema asegura que los componentes adecuados estén diseñados en el sistema de seguridad desde el principio, cuando el propietario del activo define los requisitos de seguridad. Esto permite a los expertos diseñar un sistema que responda a las necesidades específicas de las instalaciones y garantizar que se incorporen directrices estándar en cada fase del proyecto.

A pesar de que los sistemas de ciberseguridad se pueden reajustar y las mejores soluciones se diseñan en el proyecto desde el principio.

Comprensión y aplicación del IEC 62443

Los 14 componentes que comprenden el IEC 62443 se dividen en cuatro grupos:

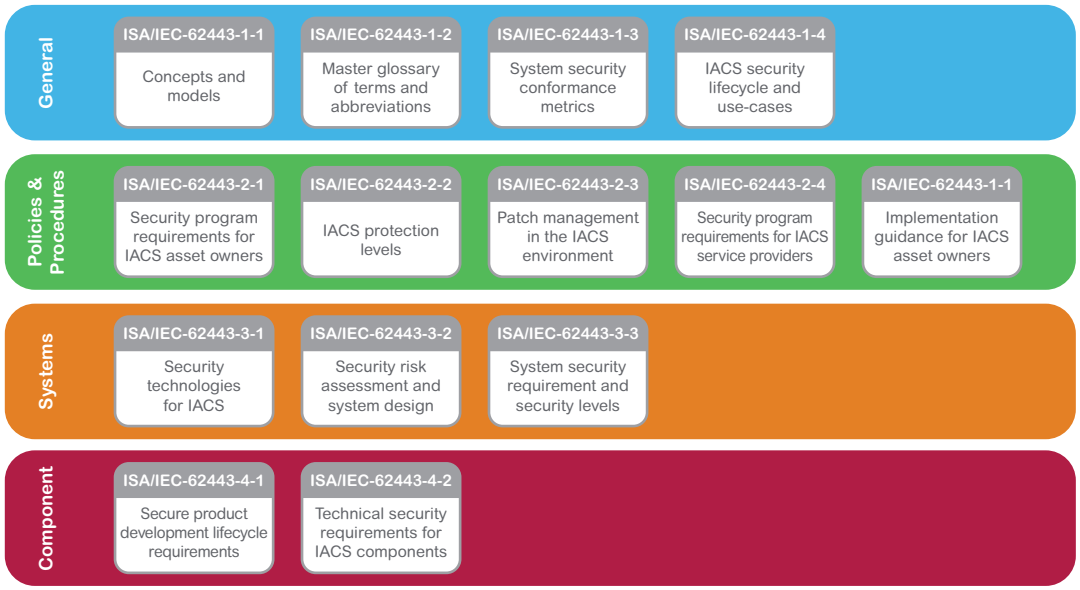
1. General
2. Políticas y procedimientos
3. Sistema
4. Componente

Los dos primeros grupos describen conceptos, políticas y procedimientos aplicados para controlar la seguridad del sistema. Los dos últimos definen los requerimientos técnicos de las redes y los componentes.

La estructura del IEC 62443 facilita el diseño de la seguridad para los sistemas OT, ya que proporciona orientación para la implementación e identifica a la parte responsable para cada requisito y proceso.

Figura 3

Tipos de componentes del tablero de distribución en los que se pueden realizar diagnósticos



Source: isa.org/isa99

Las dos secciones del estándar que más afectan la forma en que se aplica la seguridad al sistema se concentran en identificar los requerimientos fundamentales y definir cómo se administrará la seguridad durante el ciclo de vida de EMC. Dentro de estas secciones se encuentran dos consejos para diseñar y ofrecer un sistema seguro:

- IEC 62243-2-4 incluye un conjunto integral de requerimientos de capacidad de seguridad para proveedores de sistemas.
- IEC 62443-3-3 delinea los requisitos fundamentales que se deben considerar para la seguridad mejorada del sistema de control de automatización. Este estándar está dividido en siete categorías de Requerimientos Fundamentales (FR1-FR7). Debido a que las referencias FR se utilizan en toda la documentación de requisitos técnicos, es recomendable familiarizarse con estas categorías.

Otra sección importante, IEC 62443-3-2, proporciona pautas para el desarrollo de riesgos de seguridad durante la vida del proyecto. Estas pautas ayudan a identificar el alcance de la evaluación de riesgos para el sistema en consideración (SUC) al dividir en zonas y conductos para identificar el peor de los incidentes no mitigados, de manera que se pueden desarrollar y clasificar escenarios para enfrentar los riesgos usando la escala de "consecuencias".

IEC 62443-3-2 también proporciona un enfoque estructurado para llevar a cabo evaluaciones detalladas de riesgos siguiendo estos pasos:

- Identificar amenazas por zonas/conductos (modelo de amenaza)
- Vulnerabilidades puntuales
- Determinar las consecuencias y el impacto
- Calcular la probabilidad de cada incidente potencial
- Calcular el riesgo
- Determinar el objetivo de nivel de seguridad
- Evaluar las contramedidas existentes
- Volver a evaluar la probabilidad y el impacto de incidentes
- Calcular el riesgo residual
- Comparar el riesgo tolerable con el riesgo residual

Presentación de una nueva solución

EcoStruxure™ Power for Oil and Gas de Schneider Electric™, basado en IEC 62443, es una solución industrializada rentable para los desafíos del sector del petróleo y gas, que incluye seguridad, confiabilidad y disponibilidad del sistema, y es apropiada para plataformas sobre la costa y fuera de ella, almacenamiento de producción flotante y descargas (FPSO), refinerías y plantas petroquímicas. Este enfoque estructurado, que es llevado a cabo y revisado por el equipo del sistema, proporciona una gama de soluciones para:

- Sistemas de protección y control de alta y media tensión
- Protección inteligente de carga rápida
- Sistema de monitoreo del generador
- Sistma de protección de baja tensión

EcoStruxure está diseñado para ofrecer resultados en todos los ámbitos, abordando:

- Requerimientos de la organización: Contacto de seguridad, ciclo de vida de desarrollo de software (SDLC), auditorías de terceros, respuesta ante incidentes
- Soluciones técnicas: Endurecimiento, planificación de continuidad del negocio, planificación de recuperación ante desastres, acceso remoto seguro
- Ingeniería y puesta en servicio: Configuración segura, funciones de seguridad y procedimientos y normas de seguridad

Evaluación de las necesidades del proyecto

El ciclo de vida del proyecto abarca tres fases que se definen libremente como evaluación, diseño/ejecución y mantenimiento. La fase inicial del proyecto es una evaluación completa de las necesidades del sistema. Los resultados se utilizan para desarrollar soluciones recomendadas, las cuales se evalúan en un estudio de factibilidad para evaluar la adecuación de cada solución y su eficacia en el cumplimiento de los objetivos del proyecto. Esto lleva a una recomendación final. Una vez que se aprueban las recomendaciones, se define el alcance del trabajo y se inicia el proyecto, con los requerimientos de seguridad definidos según la evaluación de riesgos.

Estos requerimientos son críticos dado que determinan la fase de selección, consultas y consultas.

Esta fase inicial de evaluación, dirigida por el especificador del cliente, incluye como mínimo:

- Revisión de alto nivel de riesgos cibernéticos para identificar las restricciones de seguridad y los obstáculos
- Identificación de requerimientos fundamentales y determinación del objetivo de nivel de seguridad
- Definición de una metodología de arquitectura de sistema de alto nivel

Identificar estos hitos permite prediseñar los requerimientos del cliente y las especificaciones del proyecto, de manera que los requerimientos de seguridad se puedan incorporar desde las primeras fases del proyecto.

Once the information is reviewed by the assessment team, the final step is to develop an in-
detallada para asignar activos a fin de implementar la solución de Sistema de Control de Automatización para alcanzar el nivel de seguridad deseado. En este punto, todos los activos físicos o lógicos que comparten requerimientos de seguridad comunes se agrupan según factores como criticidad y consecuencias, y se identifican las comunicaciones entre límites (conductos).

Tabla 1

Ejemplo de Escalamiento de Objetivos de Ciberseguridad

		Criterios			
Nivel		Disponibilidad(A)	Integridad (I)	Confidencialidad (C)	Autenticación (A)
4	Muy alto	Critico	Certificación a priori	Estrictamente confidencial	No rechazo
3	Alto	Alto	Certificación a posteriori	Difusión restringida	Seguimiento controlado
2	Moderado	Estándar	Detección y corrección	Interno	Seguimiento simple

Tabla 2

Niveles de ciberseguridad para el sistema EMCS

Objetivos (A,I,C,A)	Cyber SL	Recursos	Conocimiento	Motivacion
4	CSL 4	Crítico	Violación intencional por parte de expertos en ACS con recursos sofisticados y ampliados	Estrictamente confidencial
3	CSL 3	Alto	Violación intencional por parte de expertos en ACS con recursos sofisticados y ampliados	Difusión restringida
2	CSL 2	Estándar	Violación intencional usando medios/recursos simples	Interno
1	CSL 1	Mejor esfuerzo	Protección contra violaciones casuales	Público

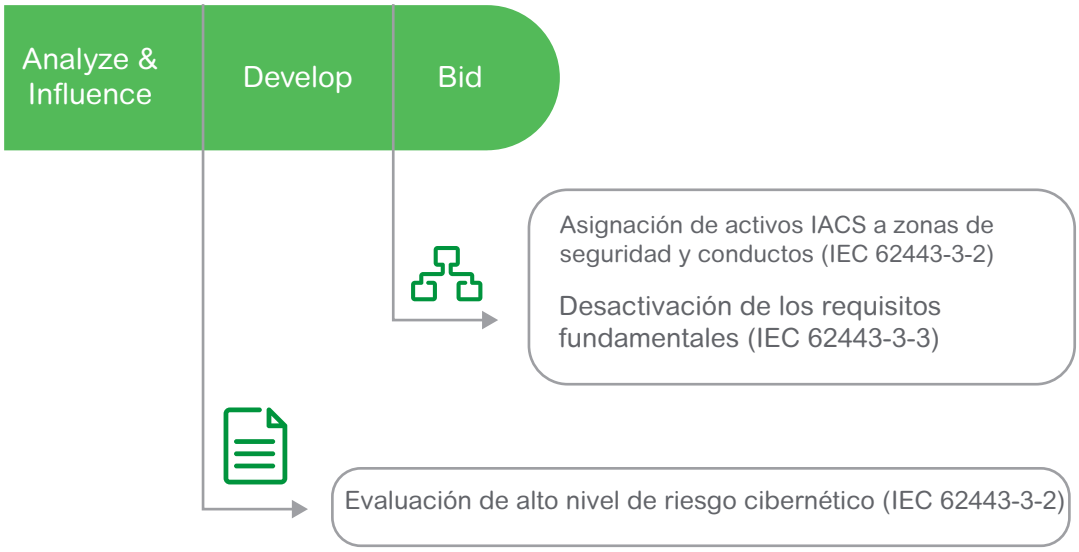


Figura 4
Hitos de Seguridad de Fases de Evaluación

La arquitectura personalizada de EcoStruxure Power for Oil and Gas tiene en cuenta las conclusiones del especificador de la evaluación de alto nivel de riesgos cibernéticos y considera la configuración de zonas y conductos de seguridad basados en funciones de activos, roles, ubicación y necesidades de comunicación. En la primera etapa del proyecto, los expertos de Schneider Electric crean una matriz de cumplimiento, un documento del proyecto que se utiliza como herramienta para determinar cómo se asegurará la seguridad para cada requisito. La matriz de cumplimiento de normas se revisa a medida que el proyecto avanza para monitorear el desempeño del sistema y se ajusta y rediseña según sea necesario durante el ciclo de vida del proyecto para ayudar a asegurar que se cumplan todos los requerimientos fundamentales.

Ejecución: Construcción de la arquitectura

Cuando se aprueba el proyecto, comienza la fase de ejecución. Esta es la fase durante la cual se acuerdan las especificaciones para el proyecto, se definen los requerimientos de arquitectura y proyecto, se llevan a cabo pruebas de validación y se completa la puesta en marcha del sitio, lo que lleva al traspaso del proyecto.

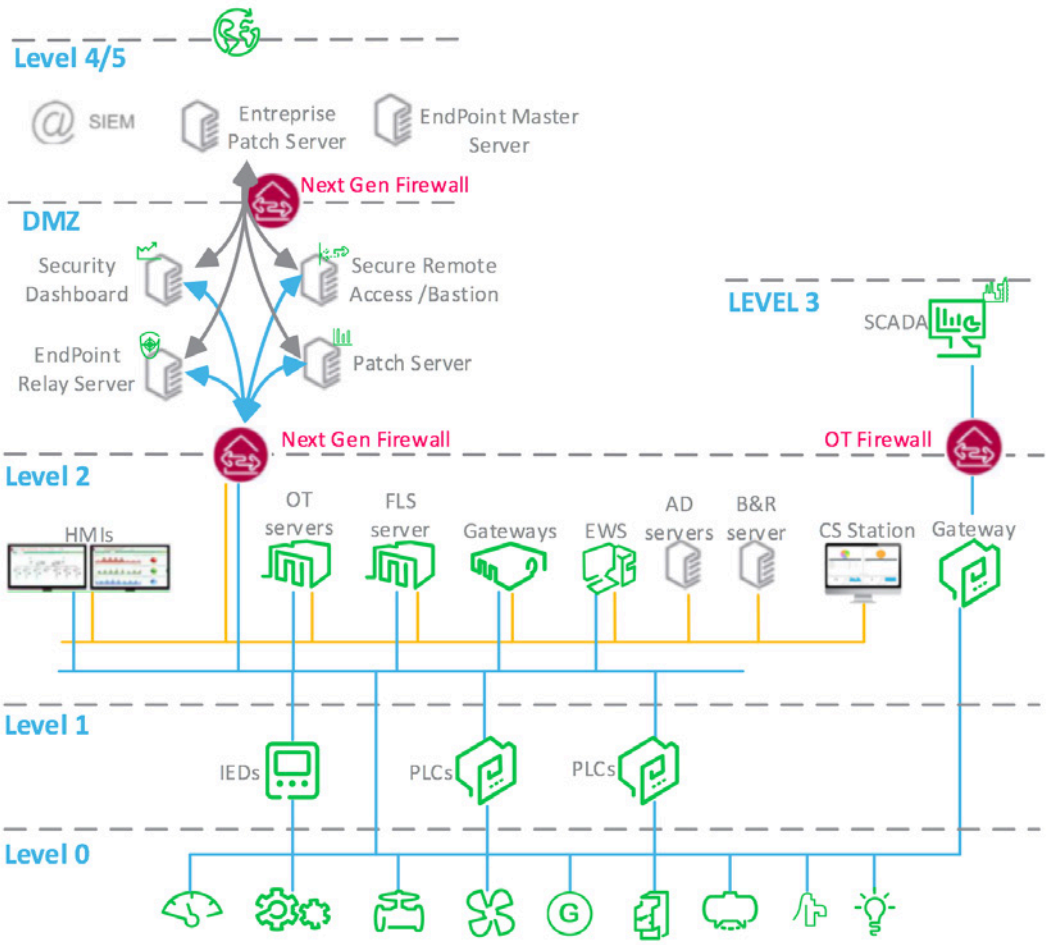


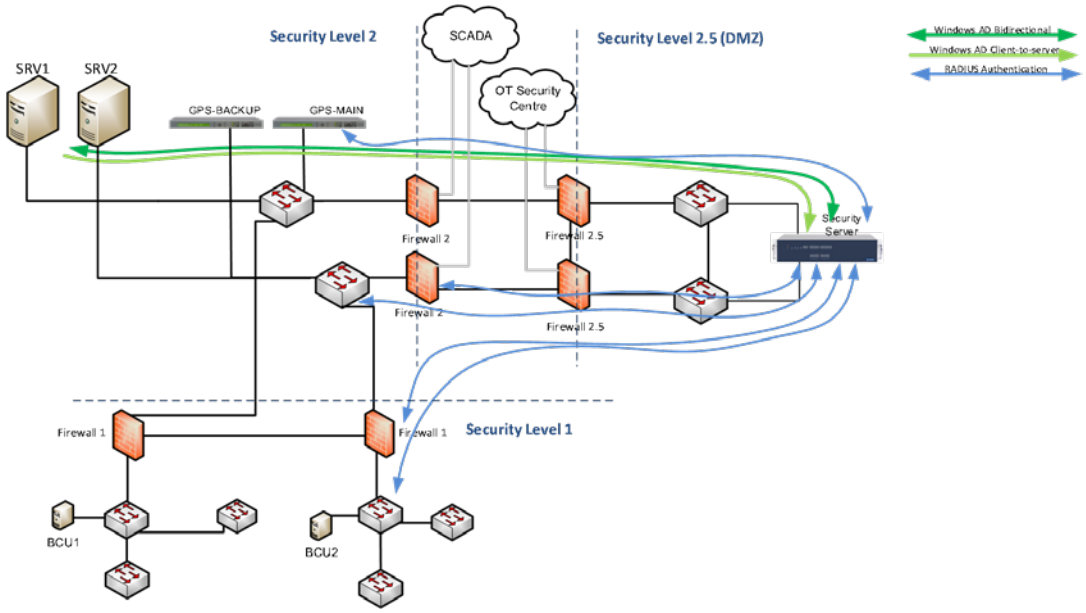
Figura 5

EcoStruxure Power Principio de Arquitectura de Seguridad

Desde el punto de vista de la seguridad, esta fase se basa en el informe de evaluación de riesgos, con requerimientos de seguridad del proyecto derivados de los requerimientos fundamentales y de las zonas y conductos identificados.

Figura 6

El trabajo de crear zonas y conductos se basa en la arquitectura del sistema, con expertos que identifican activos con el mismo propósito y preocupaciones de seguridad. En este ejemplo, los activos de nivel 1 de seguridad tenían diferentes preocupaciones de seguridad física que los servidores de nivel 2. Por lo tanto, se colocaron firewalls entre Nivel 1 y Nivel 2. Debido a que la disponibilidad es indispensable en los sistemas eléctricos, se incorporó un segundo firewall en modo cluster, con el incendio paredes que soportan la capacidad de derivación en caso de falla eléctrica en ambos firewalls.



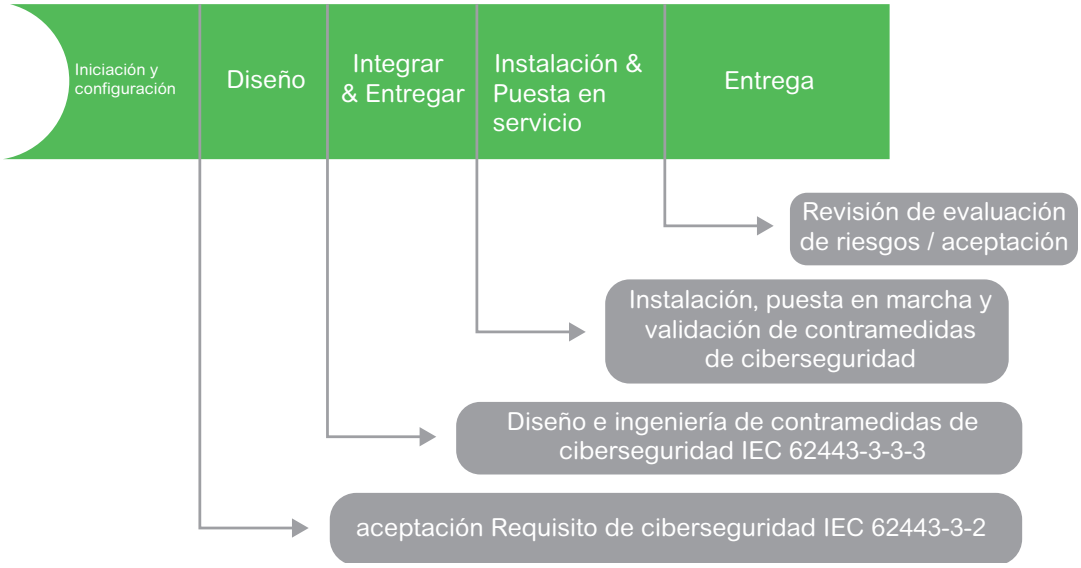


Figura 7

Fase de ejecución
Hitos de Seguridad

La implementación de seguridad se encuentra dentro de tres áreas de focalización principales: organización, aspectos técnicos y procedimientos.

La organización comienza con la formación de un equipo de proyecto que revisa las políticas y los procedimientos teniendo muy presente la conciencia de la ciberseguridad. La administración de documentos es una parte importante de esta fase, en la que el equipo define cómo se administrarán los documentos internamente, incluida la manera en que se compartirán los documentos y qué política de confidencialidad se aplicará a cada tipo de documento. El principio de mínimo privilegio se aplica a la documentación del proyecto, permitiendo el acceso sólo a los miembros del proyecto. Dentro del equipo, el acceso se restringe a la información relevante para el trabajo del miembro del equipo. Por ejemplo, un ingeniero eléctrico que no necesita tener acceso a información de compras o contratos no puede ver estos documentos.

Los aspectos técnicos incluyen especificaciones de proyectos como la arquitectura EcoStruxure, la especificación funcional de ciberseguridad, el flujo de datos dentro de la red, los procedimientos de validación de seguridad y las pautas operacionales.

De acuerdo con el IEC 62443, la arquitectura se concibe considerando zonas de seguridad y conductos, aplicando los principios de Defensa en Profundidad (DiD). DiD protege datos e información valiosos usando una serie de mecanismos defensivos en capas. Si un mecanismo falla, el siguiente en la línea inmediatamente entra en escena para provocar un ataque. Un proceso de múltiples capas que utiliza redundancias intencionales aumenta la seguridad del sistema y pone defensas para muchos vectores de ataque diferentes.

La especificación funcional de ciberseguridad define las contramedidas de ciberseguridad. Este documento detallado describe la seguridad funcional, incluida la manera en que se protegen los requerimientos fundamentales del proyecto, identificando la solución de seguridad elegida, que incluye:

- Un servidor AAA central que maneja las solicitudes de acceso de los usuarios a recursos computacionales y proporciona servicios de autenticación, autorización y contabilidad (AAA, Authentication and Accounting).
- Soluciones para asegurar terminales como computadoras de escritorio, portátiles, dispositivos móviles, PLC, IED y otros activos eléctricos y de procesos
- Políticas de administración de correcciones y consolidación
- Recuperación ante desastres
- Soluciones de monitoreo de seguridad, que incluyen logs de seguridad y sistemas de monitoreo de redes
- Inventario
- Separación de redes

El documento de flujo de datos de red es otro elemento del componente técnico. Este documento detalla todo el tráfico esperado de Interconexión de Sistemas Abiertos (OSI) que cruzará el Sistema de Control de Automatización Industrial. Esta información se basa en las zonas y los conductos de este sistema y se utiliza para configurar los dispositivos de firewall albergados y físicos. Un Plan de Segmentación de Red separado define cómo se aplica el sistema y permite, entre otras cosas, el desarrollo de reglas de firewall.

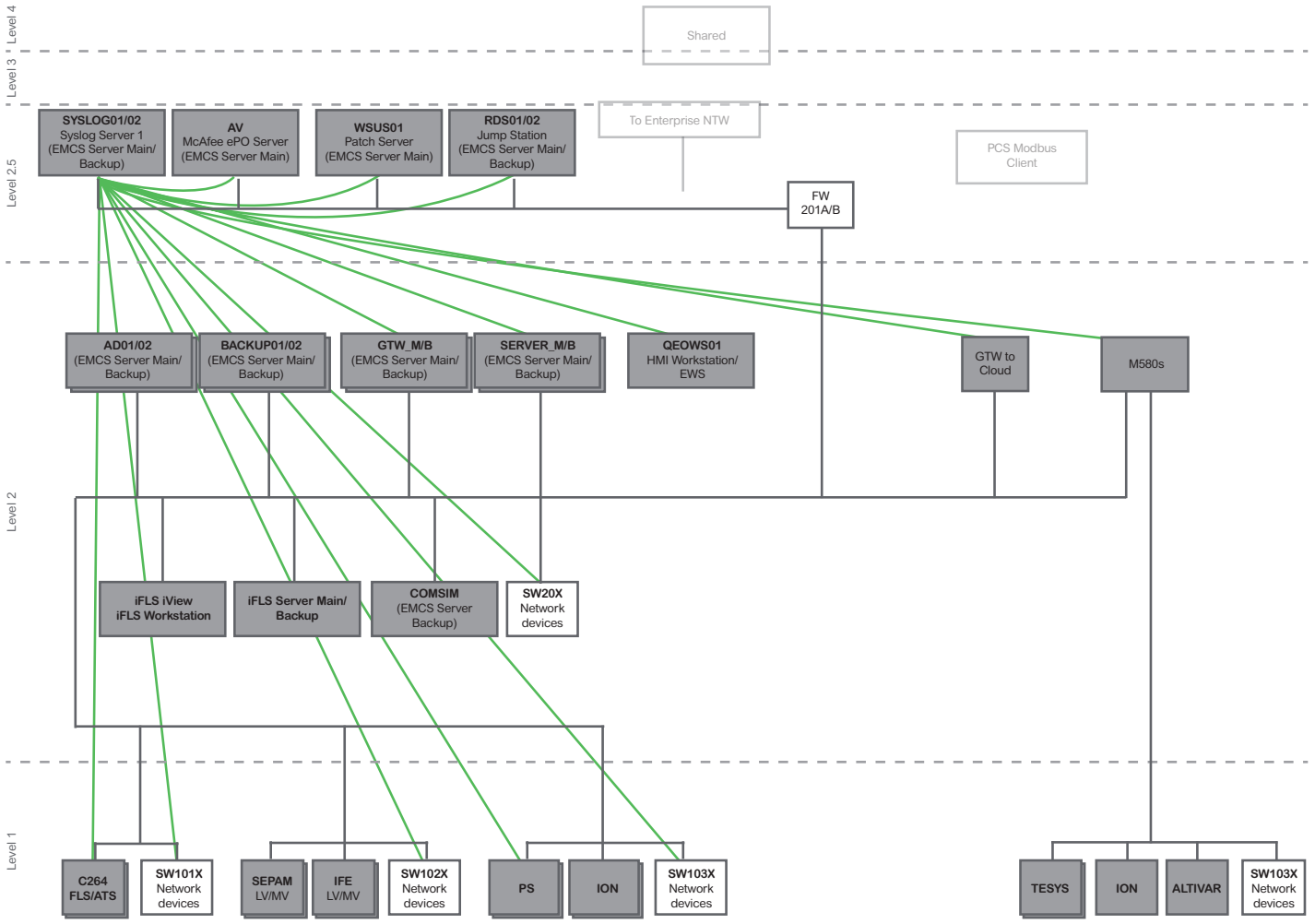


Figura 8

Esta ilustración muestra un diagrama típico de flujo de datos donde se identifican los flujos entre todos los componentes de la arquitectura. Por lo general, los firewalls se colocan entre zonas y este diagrama se utiliza para auditar y validar la configuración de las reglas del firewall.

Los procedimientos son el tercer área de enfoque principal y están cubiertos por la Especificación del proyecto de administración de seguridad. Este documento se refiere a un Plan clásico de calidad de proyecto (PQP, Project Quality Plan), que describe las actividades, estándares, herramientas y procesos necesarios para ofrecer un proyecto de calidad. La Especificación del proyecto de administración de seguridad define los planes para administrar la ciberseguridad en el proyecto. Describe la jerarquía del proyecto, identifica un punto de contacto de seguridad para el proyecto y explica desde una perspectiva de seguridad cómo se organiza el proyecto. Este documento se comparte con el cliente para su aprobación.

La pieza final de la seguridad técnica son las pautas operacionales que documentan cómo operar y administrar el sistema desde una perspectiva de seguridad y cómo se aplican reglas de endurecimiento en el sistema de automatización.

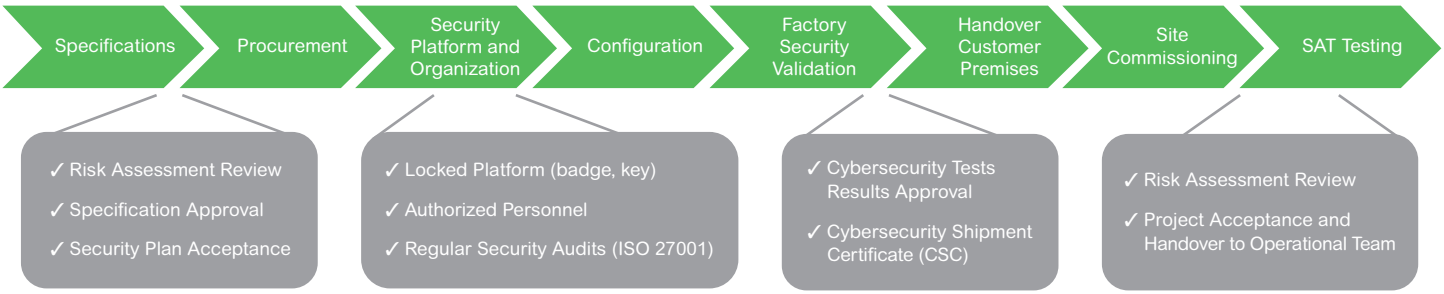


Figura 9

Ejecución del proyecto sigue un proceso bien definido

Ejecución: Prueba del sistema

Los procedimientos y herramientas que son integrales para EcoStruxure proporcionan un marco para garantizar la ciberseguridad del sistema. Entre ellos se encuentra un inventario del proyecto que identifica el material, así como el firmware y el software para que se puedan monitorear los cambios que indican vulnerabilidades. El inventario se crea a medida que se conceptualiza el proyecto, con un inventario base creado en la etapa de prueba de aceptación de fábrica y actualizaciones realizadas cuando se realizan cambios en cualquier hardware o software del sistema.

Los procedimientos de validación de seguridad también forman parte de la seguridad técnica. Estos procedimientos establecen un conjunto de pruebas mediante las cuales se verificará el sistema para validar la seguridad y que contendrán al menos:

- Objetivos de seguridad
- Condiciones iniciales
- Herramientas para usar
- Activos objetivo
- Descripci{on de la prueba
- Resultados

Las exploraciones de vulnerabilidad son otro componente crítico del programa de ciberseguridad. Un escaneo de red de todos los activos del sistema permite detectar vulnerabilidades, por ejemplo, cuando el software/firmware no está actualizado, faltan parches de seguridad o cuando hay puertos de comunicación abiertos.

Las herramientas de digitalización empleadas varían según la fase del proyecto. Antes de que se ponga en marcha el sistema, se utilizan herramientas como Nessus o OpenVas para identificar vulnerabilidades y verificar que las configuraciones de seguridad sean adecuadas. Cuando el sistema entra en funcionamiento, la solución EcoStruxure Power for Oil and Gas realiza auditorías pasivas para evaluar el impacto potencial de las herramientas y la criticidad del sistema. Las auditorías de ciberseguridad se llevan a cabo de manera periódica durante toda la vida útil del proyecto, desde la auditoría inicial en la fábrica de Schneider hasta la evaluación en el sitio antes de la entrega del proyecto. El nivel de riesgo se calcula para cada riesgo identificado, tomando en cuenta la vulnerabilidad misma (CVSS) y el posible impacto, y se crea un plan de acción para cada vulnerabilidad.

Test	Name	Description	Tools	Criteria	Type	Result (Executed / Not Executed / NA)	Target of Test	Observations
T12.1	Vulnerability scanning	• Define sets of targets according to their features (servers, databases, operating systems) • Define depth of the tests • Execute tests	• OpenVAS • NESSUS	Entry Criteria: • It is possible to connect remotely to the system Exit Criteria: • The system has been tested for known critical vulnerabilities	Active test		5-Components connected through a Network Interface Card	

Host	High	Medium	Low	Log	False Positive
172.18.4.100	0	14	3	0	0
172.18.4.5 SRV01.EMCS.local	0	11	0	0	0
172.18.4.8 OWS01.EMCS.local	0	11	0	0	0
172.18.4.6 GTW01.EMCS.local	0	1	1	0	0
Total: 4	0	37	4	0	0

Figura 10

Las exploraciones Nessus o OpenVas son útiles para detectar vulnerabilidades del sistema antes de que un sistema esté en producción. Los escaneos proporcionan información valiosa, que asegura que las aplicaciones instaladas estén actualizadas e identifica los riesgos que aún existen. Este informe de pruebas de OpenVas se ejecutó en un ecosistema EcoStruxure en las instalaciones de Schneider Electric durante la fase de configuración antes de completar la validación interna.

Las estrategias de backup se aplican en función de los tipos de activos instalados en el sistema. Se implementan soluciones de backup automático para activos basados en PC y herramientas de administración de redes, mientras que los backups manuales se utilizan para IED, PLC y otros activos para los cuales los backups automáticos regulares no son adecuados. En ambos casos, los procedimientos de backup siguen el Objetivo de tiempo de recuperación (RTO, Recovery Time Objective) y el Objetivo de punto de recuperación (RPO, Recovery Point Objective), que normalmente se especifican en el Plan de continuidad del negocio del propietario del sistema.

Administración de riesgos

Las revisiones de evaluación de riesgos que examinan cómo se administra el riesgo y cómo se trata se llevan a cabo durante todo el ciclo de vida del proyecto.

La administración de riesgos identifica los riesgos de seguridad en términos de los cuatro términos y condiciones:

- Tolerar: Cuando el cliente conoce y acepta el riesgo y no se toma ninguna otra medida
- Transferencia: Cuando se conoce el riesgo y se transfiere a un tercero para su administración, es decir, el equipo de operaciones y mantenimiento se hace cargo del riesgo y lo administra.
- Terminar: El riesgo se elimina al hacer las cosas de manera diferente
- Tratamiento: El riesgo se resuelve mediante la aplicación de procedimientos técnicos u organizativos. El objetivo de tratar el riesgo es reducir la probabilidad de amenaza hasta que se pueda tolerar, transferir o terminar.

El riesgo se trata mediante la aplicación de los principios de la DiD que aprovechan cinco contramedidas de ciberseguridad:

- Detener: Evitar que el atacante intente una violación
- Detectar: Monitoreo de grandes áreas para exponer intrusiones no autorizadas
- Retraso: Lentitud de una intrusión activa para obtener tiempo de respuesta
- Denegar: Evitar que personas no autorizadas accedan al sistema de control de automatización industrial
- Derrota/Responde: El personal de seguridad monitorea el sistema y responde a los intentos de

Resumen

La siguiente tabla muestra el número de problemas identificados en diferentes categorías. Los problemas se clasifican según su gravedad como Alto, Medio, Bajo o Información. Esto refleja el posible impacto de cada problema para una organización típica. Los problemas también se clasifican de acuerdo con la confianza como Ciertos, Firmes o Provisional. Esto refleja la confiabilidad inherente de la técnica utilizada para identificar el problema.

		Confianza			
		Cierto	Empresa	Provisional	Total
Severidad	Alto	0	0	0	0
	Medio	1	0	0	1
	Bajo	1	0	0	1
	Información	4	0	1	5

El siguiente cuadro muestra el número agregado de problemas identificados en cada categoría. Las barras de color sólido representan problemas con un nivel de confianza de Cierto, y las barras desaparecen a medida que el nivel de confianza disminuye.

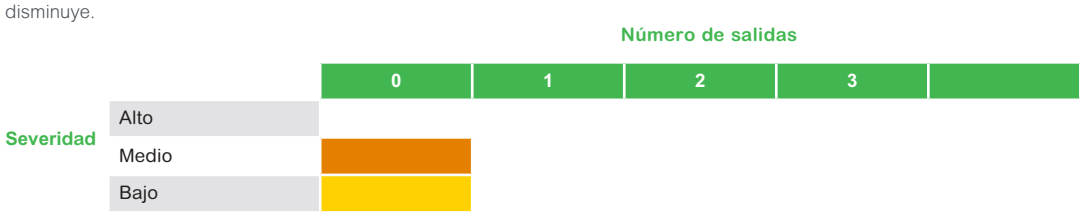


Figura 11

Ejecutar pruebas de penetración en las aplicaciones es común en esta etapa para verificar, por ejemplo, el nivel de seguridad de las aplicaciones Web. El uso del software de pruebas de seguridad de la aplicación Burp Suite permite evaluar los riesgos en función de las vulnerabilidades encontradas.

Mantenimiento del sistema

Una vez que el proyecto ha sido entregado oficialmente al propietario del activo, el equipo operativo es responsable de operar y mantener el sistema. Un error común en esta etapa es considerar la ciberseguridad sólo en términos de soluciones antivirus, listas blancas y endurecimiento y pensar que estas herramientas son adecuadas para la protección del sistema. Es fundamental considerar la ciberseguridad en su totalidad y hacer de la ciberseguridad una consideración cotidiana que se incorpora en las tareas del equipo operativo.

Emplear EcoStruxure Power de Schneider Electric no sólo ayuda a asegurar la integridad de los activos, sino que también ayuda a los propietarios a desarrollar planes que se puedan usar con rapidez en caso de violación cibernética. Este programa proporciona recuperación ante desastres y procedimientos operacionales de seguridad, incluida la recuperación ante desastres para EcoStruxure Power for Oil and Gas, dentro del plan de continuidad del negocio para el sitio.

La capacitación es un componente vital de esta oferta. El alcance de la capacitación abarca no sólo la educación del equipo operativo local para operaciones seguras y eficientes en la planta, sino también el monitoreo de la seguridad y la familiaridad con los procedimientos, de modo que se puedan seguir rápidamente en caso de un evento cibernético. Personal clave renueva periódicamente su capacitación en ciberseguridad para asegurarse de que esté familiarizado con los cambios en las políticas y procedimientos de ciberseguridad.

Las auditorías periódicas y las evaluaciones de riesgos también forman parte del plan de servicio de mantenimiento preventivo de EcoStruxure Power for Oil and Gas. Las auditorías y evaluaciones ayudan a diagnosticar problemas inusuales de tiempo de ejecución e identificar riesgos nuevos potenciales que el equipo de operaciones no cubre rutinariamente. Un componente obligatorio de este programa son las revisiones periódicas de los registros de ciberseguridad que permiten identificar posibles riesgos para que se tomen medidas antes de que ocurra una violación cibernética.

Por lo general, las funcionalidades de seguridad incluyen un Sistema de Detección de Intrusión en Red Industrial, que monitorea toda la red para detectar un comportamiento anómalo o un servidor de Información de Seguridad y Administrador de Eventos (SIEM, Security Information and Event Manager). Al igual que un servidor syslog, SIEM recopila datos de eventos de toda la empresa, pero también realiza un análisis continuo de todos los datos recopilados y emite alertas cuando ocurren anomalías. Para un rendimiento adecuado, la comunicación entre los sistemas y el SIEM debe verificarse periódicamente a fin de garantizar que todos los sistemas que deben conectarse al SIEM se comuniquen correctamente de modo que el SIEM pueda correlacionar, monitorear y controlar eventos de seguridad.

A medida que se realizan mejoras en el sistema de seguridad con el tiempo, los propietarios reciben actualizaciones que les permiten proteger el sistema. Debido a que pueden ocurrir nuevas vulnerabilidades para el firmware, los sistemas operativos y las aplicaciones en cualquier momento, el inventario periódico del proyecto debe incluirse en el protocolo de ciberseguridad. Se debe realizar una evaluación de riesgos para cada vulnerabilidad conocida a fin de determinar la probabilidad, el impacto y la importancia de una violación de seguridad. Involucrar al equipo de respuesta e incidentes del proveedor es clave para garantizar una respuesta adecuada a los incidentes identificados en el sistema.

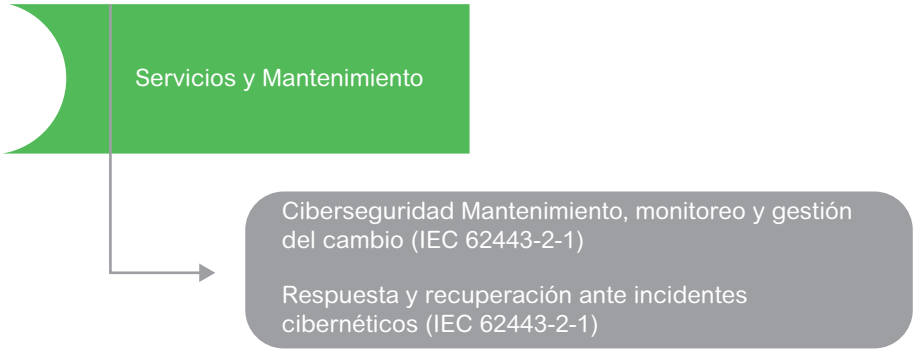


Figura 12
Fase de ejecución
Hitos de Seguridad

El valor del ciclo de vida de la ciberseguridad de EMC

La economía del proyecto siempre es importante, pero en el mercado actual es más importante que nunca optimizar las operaciones. La mejor manera de asegurar la instalación de una solución exitosa y escalable es seguir un enfoque sistemático basado en reglas para instalar e implementar sistemas de ciberseguridad de EMC basados en estándares establecidos de la industria.

Trabajar con el partner adecuado puede ser la diferencia entre el éxito y el fracaso.

El profundo conocimiento de las tecnologías de TI y OT que el equipo de Schneider Electric pone a disposición de los clientes les permite brindar orientación especializada para diseñar, implementar y mantener un sistema de ciberseguridad de EMC que mejore el tiempo de funcionamiento y la rentabilidad.

Acerca de los autores

Roberto Angulo actualmente trabaja para Schneider Electric en Montpellier, Francia, como Líder en Ingeniería de Ciberseguridad, administrando la implementación de ciberseguridad en sistemas de automatización de subestaciones. Nació en Tenerife, Islas Canarias, España y recibió su licenciatura en telecomunicaciones de la Universidad de Sevilla. Angulo también completó la capacitación industrial en ciberseguridad y obtuvo la certificación de GIAC e ISA. Anteriormente trabajó como ingeniero de redes diseñando e implementando una amplia gama de redes de comunicación (fijas y radiofónicas), incluidos sistemas seguros de troncalización digital end-to-end, en Australia, Sudamérica y Medio Oriente.

Adam Gauci nació en Toronto, Ontario, Canadá y recibió una Licenciatura en Ingeniería Informática de Queen's University en Kingston, Ontario. Su experiencia de trabajo anterior incluye Hydro One Networks como Ingeniero de Protección y Control y Cooper Power Systems como Ingeniero de Aplicaciones en Terreno. Actualmente trabaja con Schneider Electric como líder de mercadeo de ciberseguridad para EcoStruxure Power, con sede en Montpellier, Francia. El Sr. Gauci es un Ingeniero Profesional registrado en la provincia de Ontario.

Guillaume Bruandet es el arquitecto digital de soluciones globales para sistemas de energía y energía de petróleo y gas. Nació en Grenoble, Francia y se graduó de University of Grenoble con un grado de honores en ciencias de la computación. La experiencia previa fue Ingeniero de Sistemas y gerente de sitio de puesta en servicio, con muchos años de experiencia en las plantas de gas y petróleo más grandes. Con base en estas experiencias, pasó a la posición de Gerente de proyecto de I+D para digitalizar el sistema de energía..

Schneider Electric

998-21125448 _GMA