BASQUE INDUSTRY 4.0

Características del diagnóstico

Centro de Ciberseguridad Industrial

Escuela Profesional de Ciberseguridad Industrial

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

BASQUE CYBERSECURITY CENTRE

BASQUE INDUSTRY 4.0

BUENAS PRÁCTICAS PARA EL DIAGNÓSTICO DE CIBERSEGURIDAD EN ENTORNOS INDUSTRIALES

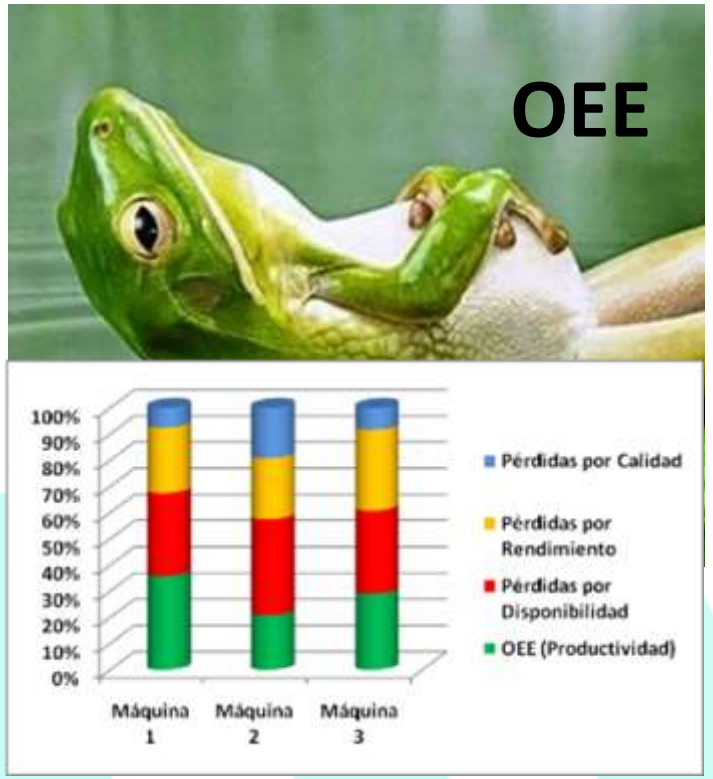
2014

Objetivos

- Conocer el estado de Ciberseguridad de una instalación industrial.
- Identificar puntos débiles.
- **Entender los riesgos que afronta la instalación**.
- Proponer recomendaciones de mejora.

Características

- Servicio de alto valor.
- Muy especializado.
- Oferta reducida en el mercado.
- Complejo y Multidisciplinar.
- Abarca tanto aspectos técnicos como organizativos.
- **Requiere trabajo de campo** (presencial) y remoto.



Características

¿Quién lo solicita?

- Personal con responsabilidades:
  - Responsables de seguridad.
  - Responsables de TI.
  - Responsables de planta.
  - Dirección.

- Interlocución con perfiles variados.
  - **No siempre colaborativos**.

Características

¿Por qué lo solicitan?

- Preocupación:
  - **Han tenido un incidente**.
  - Sensación de inseguridad.
- Requisito:
  - De negocio.
  - De cliente.
  - **Normativo**.
- Por higiene:
  - No han prestado atención a ciertos aspectos.
  - Desconocen la realidad de sus sistemas.

Características

Aptitudes necesarias:

- Conocimientos en Ciberseguridad.
- Conocimientos de comunicaciones y sistemas.
- Conocimiento de los entornos industriales.

Actitudes necesarias:

- **Discurso**.
- **Mano izquierda**.

Características

- **Tener extremo cuidado durante las pruebas técnicas**.
- **Los métodos TI pueden no ser de aplicación.**
- Se accederá a información delicada.
- **Aparecerán cosas incómodas**.
- Transmitir seriedad y profesionalidad.
- **Comunicarse en "*español*"** (*plain Spanish*).

¡¡¡Nunca comenzar sin tener firmados tres documentos!!!

Características

Doc. nº 1: ***Reglas de enfrentamiento*** (*Rules of Engagement*)

- **Establecen el escenario de los trabajos**
  - Sistemas y aplicaciones a revisar
  - Los términos en que se desarrollarán las pruebas
  - La ventana temporal
  - Personas de contacto
  - Alcance de las revisiones
  - Presentación de los resultados

Características

Doc. nº 2: ***Acuerdo de confidencialidad***
(*Non-Disclosure Agreement*, NDA)

- Protege al propietario de la información
- Es probable que durante los trabajos realizados se acceda a información importante sobre la organización auditada
- El auditor se compromete a no divulgar la información recopilada ni aprovecharse de ella.
- Fundamental cuando hay implicaciones legales (LOPD)

Características

Acuerdo de Confidencialidad

D. _____ se compromete a guardar absoluta confidencialidad sobre todos los datos e información a la que tenga acceso como consecuencia de su relación con Mazzallón, cualquiera que sea o haya sido la forma de acceso a tales datos o información y el soporte en el que consten, quedando absolutamente prohibido obtener copias sin previa autorización.

El acceso y tratamiento de datos de carácter confidencial como consecuencia de la relación establecida con la empresa Mazzallón, lo realizará de acuerdo con las finalidades previstas en su colaboración, subsistiendo el deber de secreto, aun después de que finalice dicha colaboración.

Mediante la firma del presente escrito, declaro haber leído y comprendido los derechos y deberes que en él se detallan.

Nombre:

DNI:

Firma del colaborador:

Características

Doc. Nº 3: ***Exención de Responsabilidades*** (Get out of jail card)

- Protege al auditor/evaluador
- Establece que el auditor no será sancionado debido a fallos ocurridos en los sistemas del cliente debidos a los trabajos realizados
- El auditor se compromete a actuar con el cuidado debido y de acuerdo a las reglas de enfrentamiento

Características

- Tiempo
  - Depende del tamaño y la complejidad de la instalación.
  - Estimación (**¡¡¡Ojo, sólo es una estimación!!!**):
    - 2-3 jornadas presenciales por ubicación.
    - 2-3 jornadas de trabajo en remoto.
    - 2-4 jornadas para consolidar documentación.
- Elaboración de la documentación (Informe)
  - **Tan importante como el trabajo de campo**.
  - Implica ordenar **MUCHA** información.

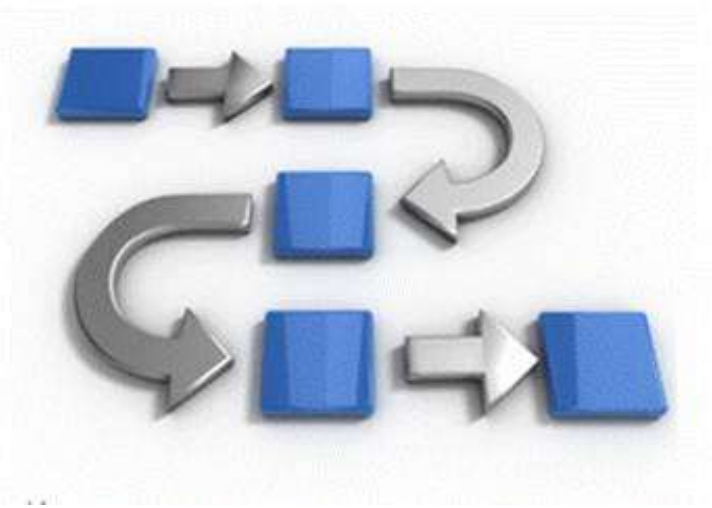
BASQUE INDUSTRY 4.0

TALLER PRÁCTICO

Diagnóstico de ciberseguridad en un entorno de automatización industrial

Metodología y entrevistas práctica

Metodología



Pasos

1. Preparación.
2. Aspectos a revisar.
3. Recopilación de información (Campo)
4. Verificación de información.
5. Desarrollo de informe.
6. Presentación de resultados.

Paso I. Preparación

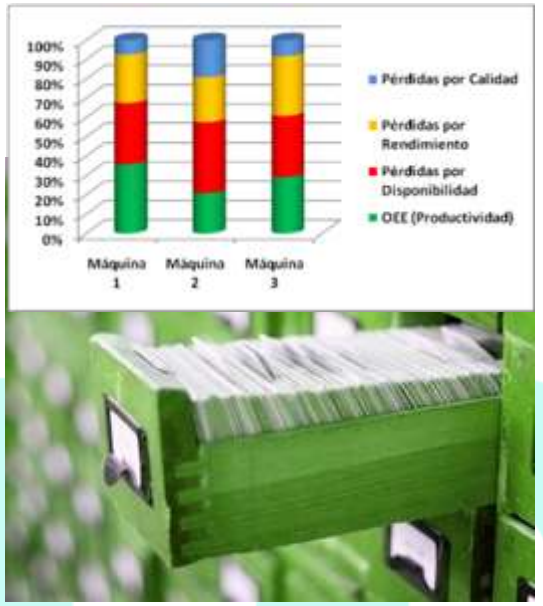
Conocer el Entorno

- Complejo.
- Requiere conocimiento multidisciplinar.
- Se va a recibir muchísima información, así que cuanto más se conozca a priori (y cuanto más a priori se conozca), mejor se podrá asimilar y enfocar.
- Conocer la instalación (saber a qué se dedica, investigar instalaciones similares)

Paso I. Preparación

Tener presentes los objetivos de la instalación:

- Fiabilidad y eficiencia de las operaciones.
- El equilibrio operatividad / seguridad es vital



Identificar una **Persona de Contacto** que:

- Facilite acceso a las instalaciones.
- Ayude a identificar personal clave.
- Organice las reuniones.

Paso I. Preparación

La actitud

- Explicar por qué se necesita la información y qué se va a hacer con ella.
- Tener en cuenta al interlocutor. **Hablar su idioma**.
- Gestionar actitudes a la defensiva ante la auditoría.
- Mantener actitud positiva.
- Ser muy profesional.
- Gestionar los posibles conflictos que pudieran surgir con el personal de planta (cuando no son ellos quienes han solicitado la revisión, lo cual será habitual).

Paso II. Aspectos a revisar

Arquitectura de redes

- Es fundamental porque condiciona en gran medida la seguridad de los sistemas.
- Habitualmente la arquitectura física está muy clara y documentada.
- Pero la arquitectura lógica no.
- Identificar zonas de seguridad (existentes o que deberían existir)
- Red de control, de supervisión. Red corporativa. Otras.

Paso II. Aspectos a revisar

Sistemas

- Usuarios Windows.
- Usuarios HMI.
- Direccionamiento IP de nodos.
- Auditoría de credenciales.
- Políticas de contraseñas.
- Métodos de autenticación.
- Robustez.

Paso II. Aspectos a revisar

Seguridad Física

- Con diferencia el aspecto más avanzado en instalaciones industriales.
- Identificar áreas seguras.
- Controles de acceso.
- Seguridad en ubicaciones remotas.
- Seguridad del cableado.
- Interferencias en comunicaciones.
- Sistemas de soporte y acondicionamiento.

Paso II. Aspectos a revisar

Terceras partes

- Identificar personal externo que accede a las instalaciones. (Proveedores de servicios, mantenimientos, suministradores, consultores, limpieza, temporalis,…)
- Tipo (lógico/físico) y métodos para acceder a la información y los dispositivos.
- Contratos. Referencias a seguridad.
- Acuerdos de nivel de servicio.

Paso III. Recopilación de información

Trabajo previo al trabajo de campo

Sirve para:

- Obtener conocimiento preciso del entorno.
- Planificar las visitas.

Solicitar información:

- Mapas de red.
- Direccionamiento público.
- Planes de direccionamiento.
- Procedimientos y políticas existentes.
- Información general sobre la instalación.

Paso III. Recopilación de información

- Entrevistas con personal relevante.
- El personal relevante debe identificarse a priori:

  - *Responsables de explotación y de procesos*
  - *Responsable de mantenimiento del sistema de control*
  - *Responsable administración*
  - *Responsable safety*
  - *Personal de operaciones*
  - *Jefe mecánico*
  - *Jefe de procesos*
  - *Jefe de operación de mantenimiento*

Paso III. Recopilación de información

- Planificar y organizar las entrevistas con ayuda de la PoC (Persona de Contacto).
- Explicar el objetivo de la entrevista.
- Usar un guión, pero ser flexible.
- Información relevante en la conversación (no en las respuestas).

Paso III. Recopilación de información

Contenido de la entrevista

Guía de Entrevista

Diagnóstico de Ciberseguridad industrial

- No todos los puntos son aplicables a todos los perfiles.
- Es una guía para realizar la entrevista.
- No es algo grabado en piedra. Debe adaptarse en cada caso.

BASQUE INDUSTRY 4.0

11 de marzo de 2018

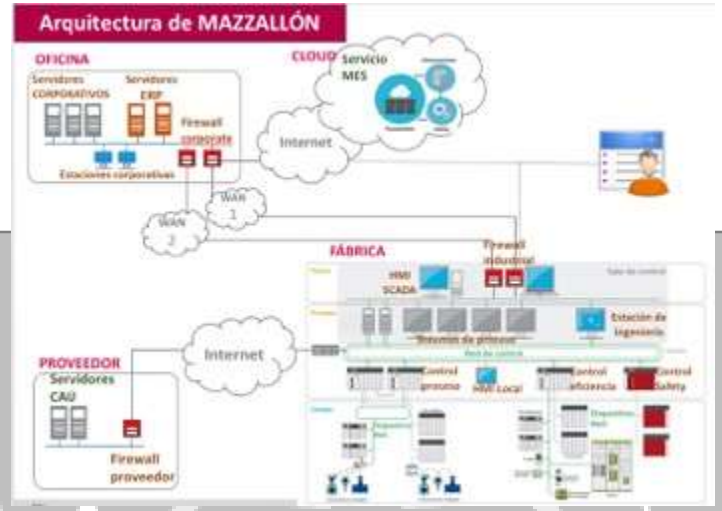
Informe Diagnóstico de Ciberseguridad de Planta TRASTER

Pepe García

Contenido

Práctica

Recopilación de información - entrevista



20 minutos

Paso III. Recopilación de información

ORGANIZACIÓN

- Nombre
- Puesto
- Descripción del trabajo
- Objetivos
- Relación con otras áreas

ACTIVOS

- Información manejada
- Sistemas críticos
- Dependencia o influencia en otros sistemas
- Objetivos
- Relación con otras áreas

PERSONAS

- Roles y responsabilidades
- Trabajadores externos
- Acuerdos relacionados con seguridad de la información
- Objetivos
- Relación con otras áreas

SEGURIDAD FÍSICA

- Áreas seguras
- Identificación
- Control de Acceso
- Controles ambientales
- Suministro (electricidad, AA, agua)
- Acceso de terceras partes

OPERACIONES

Documentación. Aspectos de seguridad de la información	
Gestión de cambios	¿Se realiza un registro de los cambios que sufren los sistemas?
Segregación de responsabilidades	¿Existen tareas en las que una sola persona podría actuar de forma ilícita o incorrecta sin que sea detectado?
Entornos de prueba y operación	
Monitorización de terceras partes	
Planificación y aceptación de sistemas	
Controles contra código malicioso	
Copias de seguridad	

COMUNICACIONES

Seguridad en redes	Segmentación. Conexión de sistemas.
Flujos y Protocolos	
Intercambio de información	
Acuerdos de intercambio	
Medios físicos	
Intercambios electrónicos	
Integración con otros sistemas	
Monitorización	
Uso de sistemas	
Registros de operación	
Registros de acceso	

Centro de Ciberseguridad Industrial

Escuela Profesional de Ciberseguridad Industrial

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Paso IV. Verificación de información

- Implica acceder a los sistemas.
- El objetivo es completar la información recopilada y… verificar que ésta es precisa.
- Gran número de sistemas: Trabajar con muestreos.

Paso IV. Verificación de información

Barridos (Escaneos).

- Los escaneos activos (nmap) son peligrosos.
- ¿Existen sistemas de prueba?
- Métodos Indirectos.

Identificación de sistemas.

- Capturas de tráfico.
- Tablas MAC en switches.

Identificación de puertos.

- Desde el sistema (netstat)

Paso IV. Verificación de información

Algunas recomendaciones en el uso de nmap

- No es aconsejable emplear la opción -O de detección de Sistema Operativo. Genera gran cantidad de tráfico. Nunca usar -A (Aggressive) que además de lo anterior incluye detección de servicios.

- No utilizar el escaneo –sU, ya que no contiene payload y al no cumplir con el estándar podría deriver en un comportamiento inesperado.

- No seleccionar gran cantidad de puertos, mejor especificar uno por uno aunque lleve mayor cantidad de tiempo

Paso IV. Verificación de información

Búsqueda pasiva de vulnerabilidades.

- Información sobre software y versiones instalados en los sistemas.
- Búsqueda en repositorios:
  - National Vulnerability Database (http://nvd.nist.gov/)
  - Open Source Vulnerability Database (http://www.osvdb.org/)
  - International Cybersecurity Community CVE (https://cve.mitre.org/)
- Manual. Consume tiempo.
- Falsos positivos. El resultado es que posiblemente el sistema tenga la vulnerabilidad.
- No hay certeza de que no se haya solucionado.
- Informar al responsable y explicar las implicaciones.

Paso IV. Verificación de información

Verificación manual automatizada.

- Automatizan las operaciones que haría manualmente un auditor (scripts con python, Powershell,…).
- Comprobar configuraciones de seguridad óptimas para algunos ICS.
- Entra en los sistemas y comprueba de manera segura el cumplimiento respecto a la configuración óptima.
- Impacto mínimo sobre el sistema.
- Genera informes de desvíos sobre la configuración segura recomendada.

Paso IV. Verificación de información

Hacking Ético externo.

- Muy similar al de las auditorías TIC clásicas.
- Sigue existiendo el problema de afectar al funcionamiento de los sistemas auditados.
- ¡Pero son sistemas públicos!. Cualquiera podría haberlo hecho.

Paso IV. Verificación de información

Hacking Ético externo.

- Búsqueda del perfil de la instalación en Internet.
- Servicios accesibles.
- Credenciales débiles o por defecto.
- Software vulnerable.
- Sistemas “olvidados”
- Configuración incorrecta de firewalls.

Paso V. Consolidar información

- Ordenar información recopilada.
  - Uno de los beneficios para el cliente es obtener documentación actualizada sobre sus sistemas.
- Investigar hallazgos.
- Revisión de configuraciones.
- Desarrollo de esquemas de red.
- Relacionar datos y sacar conclusiones.

Paso V. Consolidar información

- Puede que surjan dudas.
- Aclarar con el PoC
- Volver a visitar la instalación.
- Los hallazgos que puedan suponer un problema inminente deben ser comunicados de forma inmediata.

Paso VI. Presentación de resultados

Documento de resultados

Estructura

- Resumen Ejecutivo
- Estado Actual
- Recomendaciones

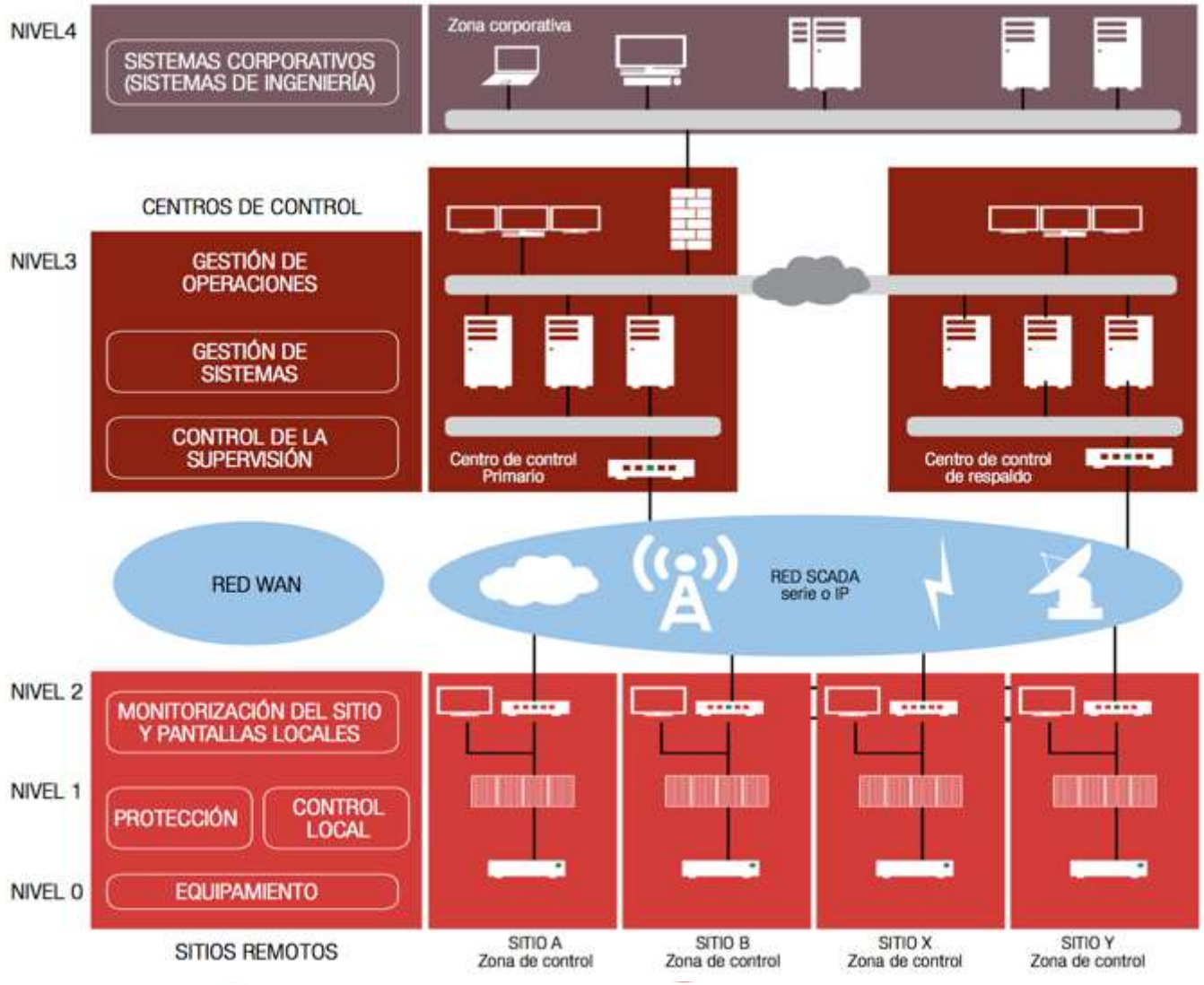
BASQUE INDUSTRY 4.0

TALLER PRÁCTIC0

Diagnóstico de Ciberseguridad en un entorno de automatización Industrial

Arquitectura de redes

Arquitectura de redes



Arquitectura de redes

- Identificar posibles caminos a la red de control.
- Identificar servicios de red.
- Protocolos utilizados.
- Puntos de interconexión con otras redes.
  - Redes de partners o proveedores.
- Identificar el perímetro lógico de la red.
- Líneas de datos.
- Router del operador.
- Accesos remotos y de terceras partes.
  - Líneas de datos no controladas.

Arquitectura de redes

- Redes Inalámbricas.
  - Alcance.
  - Utilización.
  - Protocolos de seguridad.

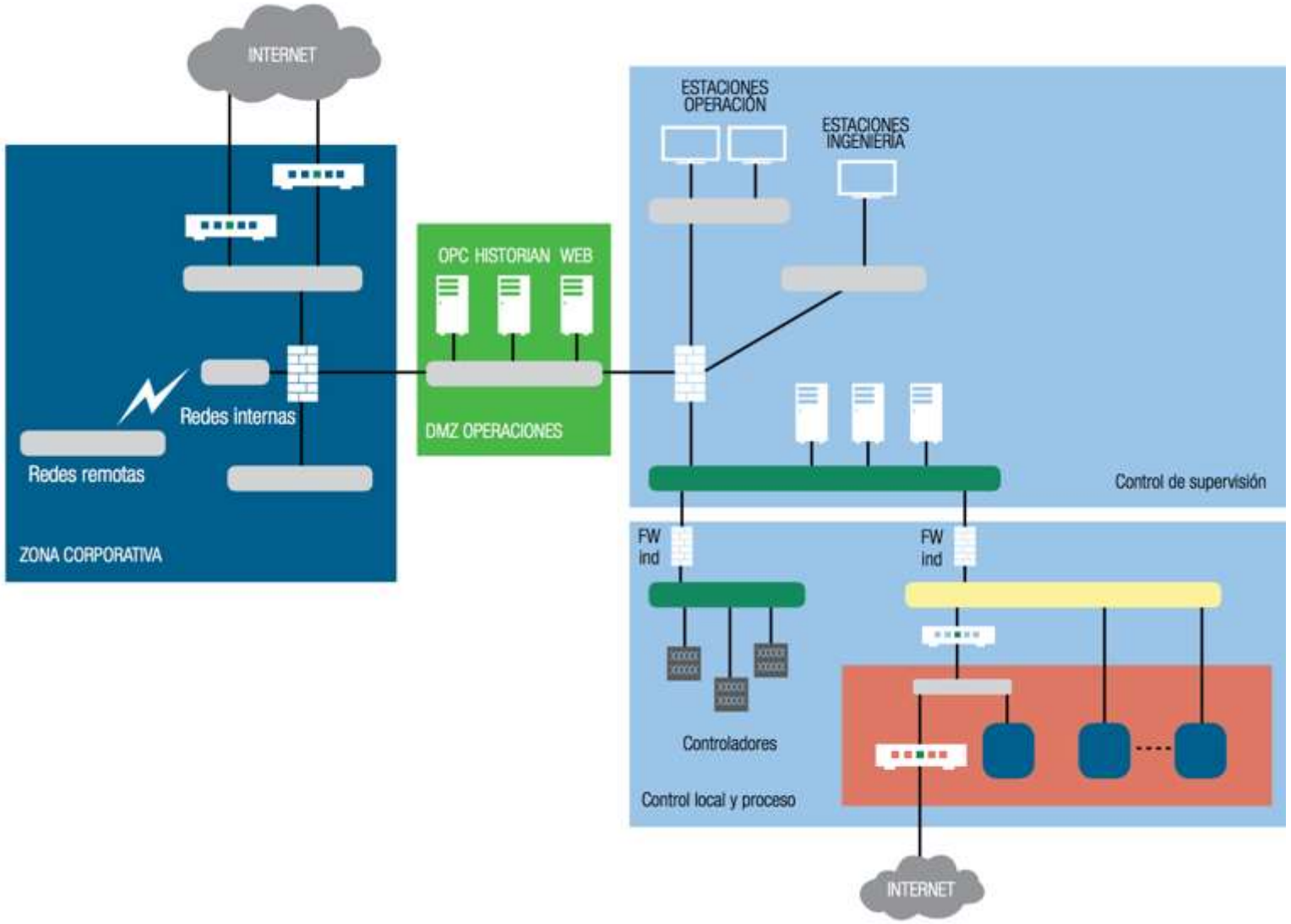
- Perfil de la instalación en Internet.
  - Direccionamiento público.
  - Nombres de dominio.
  - Servicios públicos.

Arquitectura de redes

Errores comunes

- Servidores dual-homed.
  - Servidores con dos interfaces de red conectados a distintas redes.
  - Permiten acceso a niveles inferiores desde niveles superiors y la propagación del malware.
- Escasa segmentación y filtrado.
- Accesos directos no controlados.
  - Acceso de PLCs directamente desde internet.
- Dispositivos no controlados.
  - Dispositivos de almacenamiento externo.

Arquitectura de red ideal



BASQUE INDUSTRY 4.0

11 de marzo de 2018

Informe Diagnóstico de Ciberseguridad de Planta TRASTER

Pepe García

Contenido

BASQUE INDUSTRY 4.0

Arquitectura

Mazzallón

Práctica

20 minutos

BASQUE INDUSTRY 4.0

TALLER PRÁCTIC0

Diagnóstico de Ciberseguridad en un entorno de automatización Industrial

Sistemas

Sistemas

- Revisión de servicios activos (no necesarios)
- Uso de medios extraibles.
- Configuraciones de routers.
  - Tablas de rutas.
  - ACLs.
- Versiones de software instaladas.

Usuarios

- Roles y perfiles.
- Contraseñas.
- Políticas de asignación de identidades y permisos.
- Usuarios externos.

Control de acceso lógico

Evitar accesos no autorizados o de usuarios no autorizados a equipos, sistemas o redes; garantizar la seguridad de la información cuando se utiliza informática móvil y teletrabajo; detectar actividades no autorizadas.

Mínimo Privilegio

Necesidad de Conocer

Deberá existir un proceso administrativo que dirija el A-B-M de las cuentas de usuario

Control de acceso lógico

Problemas en entornos industriales

- Dispositivos legacy que no son capaces de manejar identificaciones y/o autorizaciones.
- Requiere centralizar las autorizaciones.
  - Incorpora nuevos sistemas a la organización
  - Introduce nuevos puntos de fallo
- Los protocolos industriales tendrán que acomodarse a estos mecanismos de control.
  - Difícil con los protocolos antiguos
  - Los modernos (OPC) lo incorporan desde el inicio
    - OPC UA

Control de acceso lógico

Identificación

- En ambientes técnicos, se denomina “Identificación” al proceso por el cual una persona o un sistema se identifica (indica su nombre de usuario, id, etc.) de manera única e irrepetible en otro sistema.
- El proceso de identificación es fundamental y obligatorio en todo proceso que deba ser auditado.
- La identificación de personas y sistemas permite disminuir los riesgos asociados a la ciberseguridad industrial.

Control de acceso lógico

Identificación

Problemas en entornos industriales

- Ausencia de perfiles de usuario.
- Cuentas en desuso.
- Sesiones permanentemente abiertas.
- Ausencia de registros de log.

Control de acceso lógico

Autenticación

- Los procesos de autenticación permiten definir si la identidad presentada por una persona o sistema es real o no.
- Existen básicamente tres tipos de autenticación:
  - *Algo que sé.*
  - *Algo que tengo.*
  - *Algo que soy.*
- El tipo de autenticación más utilizado en el mundo de los sistemas es basado en “algo que sé”, como por ejemplo las contraseñas. Sin embargo, es de público conocimiento que tienden a desaparecer.

Control de acceso lógico

Autenticación

Problemas en entornos industriales

- En emergencias:
  - Cada segundo cuenta.
  - Las contraseñas retrasan las operaciones
  - Operador nervioso: no acierta o no recuerda.
  - Si hay *clipping levels* se puede bloquear la cuenta en el peor momento.
- Los ICS deben:
  - Permitir contraseñas robustas.
  - Transmitir datos cifrados.
  - Ser flexibles en caso de emergencias.
    - Reconocer intentos fallidos de alguien que conoce la contraseña pero no acierta a introducirla.

Control de acceso lógico

Autorización

- Posterior a la autenticación
- Aumentar la seguridad mediante el control de acceso de los usuarios a la información y los recursos.
- Autorización: Permisos de acceso.
  - Ver un documento
  - Modificar una configuración
  - Realizar operaciones sobre un dispositivo

Control de acceso lógico

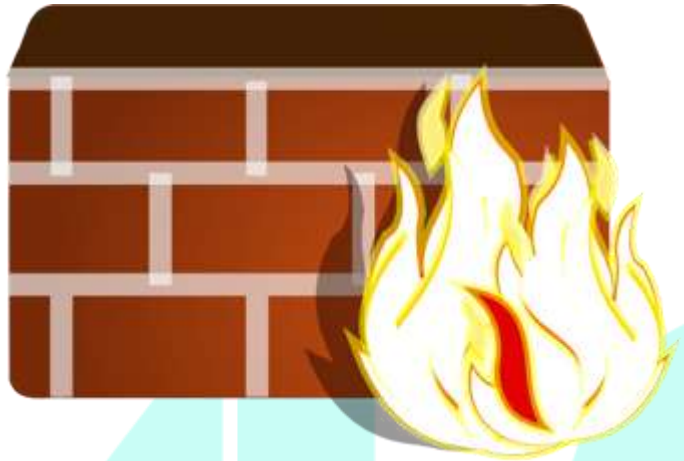
Autorización

Problemas en entornos industriales

- La gestión de autorizaciones se complica a medida que aumenta el número de usuarios y de dispositivos.
- En las instalaciones industriales puede haber miles de dispositivos y una alta rotación de usuarios.
- Es necesario un compromiso (*trade-off*)
  - Seguridad vs. Funcionalidad
- Role Based Access Control (RBAC)
  - Define roles.
  - Establecer permisos y autorizaciones por rol.
  - Asigna usuarios a los roles.
  - La autorización que tiene un usuario depende de los roles que tenga.

Seguridad de firewalls

- Dispositivos de filtrado básicos.
- Herramientas fundamentales para incorporar seguridad.
  - Segmentación de redes.
  - Idealmente, la red de control es un sistema cerrado.
  - Sólo deben acceder a ella algunos sistemas internos de confianza (HMI, historians).
  - Sin embargo, existe la necesidad de acceso desde la zona corporativa e incluso desde redes de terceros!



Seguridad de firewalls

- No permitir conexiones directas desde Internet a la red de control y viceversa.
  - El tráfico no solicitado podría congestionar o corromper la red de control.
  - Tráfico malicioso o malformado podría causar DoS
  - El tráfico saliente podría afectar al rendimiento de la red.
- Restringir el acceso desde la red corporativa a la red de control.
  - La red corporativa no deberá tener acceso directo para consultar o controlar dispositivos de control en la planta.
  - Las redes corporativa y de control deben estar aisladas física y lógicamente.

Seguridad de firewalls

- Controlar los accesos inalámbricos.
  - Mantener las redes inalámbricas segregadas.
- Monitorizar el tráfico que intenta acceder a la red de control.
  - Emplazar IDSs
- Gestión segura del firewall.
- Políticas de filtrado estrictas y bien definidas.
  - Denegar por defecto.
  - Controlar todo el tráfico entre zonas.

Seguridad de firewalls

- Evitar tráfico directo entre la red de control y la corporativa. La comunicación entre ambos mundos debe pasar siempre por la DMZ.
- Todas las reglas permitir deben ser lo más específicas posible. Estableciendo puertos e IPs de origen y destino. Activar IDS.
- Los protocolos permitidos entre la red de control y la DMZ no deben estar permitidos entre la DMZ y la red corporativa. Evita comunicaciones transitivas.
- Controlar spoofing de direcciones. Sólo se permite tráfico saliente de las redes de control cuando procede de IPs de las redes de control.
- Nunca permitir acceso a Internet desde la red de control.
- Nunca publicar en Internet sistemas de la red de control.

Seguridad de firewalls

Inconvenientes

- No están diseñados para determinadas aplicaciones industriales.
- Tienen que estar complementados por otros sistemas como IDS, sistemas de monitorización, métodos de autenticación y autorización y criptografía.
- **Los firewalls han evolucionado y se han convertido en sistemas complejos que requieren conocimiento experto y específico para cada modelo**.
- La revisión de sus logs es importante, pero es una tarea tediosa y que consume tiempo y recursos.

Seguridad de firewalls

+ Inconvenientes

- Requieren mantenimiento. (Actualizaciones)
- Forman un punto de fallo.
- Causan desconfianza. En muchas ocasiones causada por el desconocimiento del tráfico que los atraviesa.
- Pocos firewalls son capaces de entender protocolos industriales o protocolos que no sean IP.
- Incorporan latencia en las comunicaciones.

BASQUE INDUSTRY 4.0

11 de marzo de 2018

Informe Diagnóstico de Ciberseguridad de Planta TRASTER

Pepe García

Contenido

BASQUE INDUSTRY 4.0

TALLER PRÁCTIC0

Diagnóstico de Ciberseguridad en un entorno de automatización Industrial

Seguridad física

Seguridad física

Con diferencia el aspecto más avanzado en instalaciones industriales. Se debe:

- Identificar áreas seguras.
- Controles de acceso.
- Seguridad en ubicaciones remotas.
- Seguridad del cableado.
- Interferencias en comunicaciones.
- Sistemas de soporte y acondicionamiento.

TALLER PRÁCTIC0

Diagnóstico de Ciberseguridad en un entorno de automatización Industrial

Terceros

Terceras partes

- Identificar personal externo que accede a las instalaciones. (Proveedores de servicios, mantenimientos, suministradores, consultores, limpieza, temporales)

- Métodos para acceder a la información y los dispositivos. Revisar:
  - Contratos. Referencias a seguridad.
  - Acuerdos de nivel de servicio.

Terceras partes

BASQUE INDUSTRY 4.0

MANUAL DE USUARIO
HERRAMIENTA DE EVALUACIÓN DE REQUISITOS DE CIBERSEGURIDAD PARA PROVEEDORES DE SERVICIOS

El ámbito del diagnóstico abarca cuatro áreas:

1 **Organización**
Cumplimiento de políticas y procedimientos corporativos.

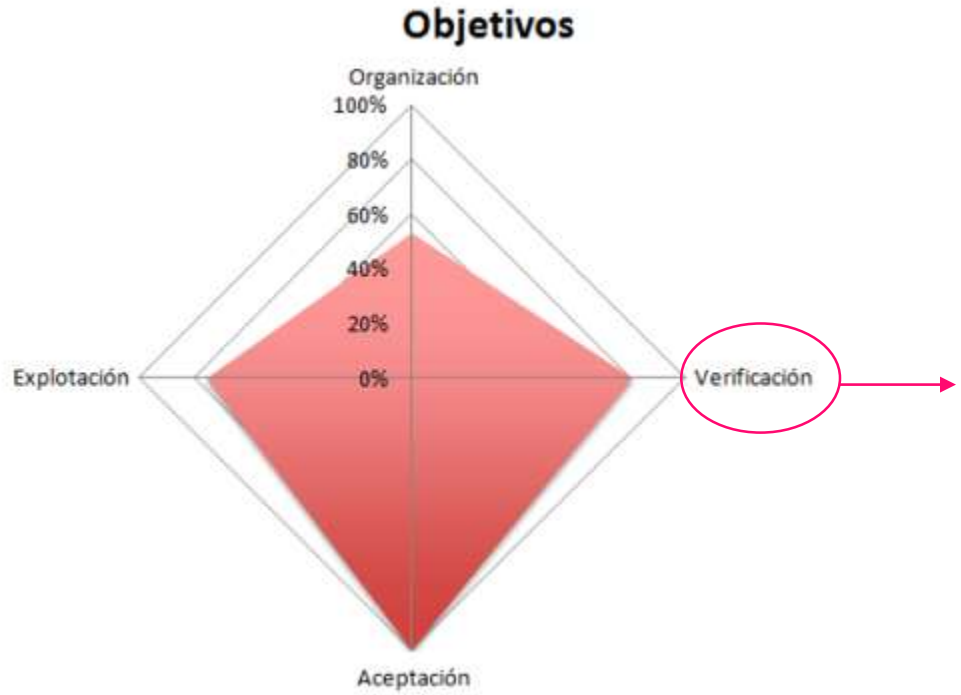
2 **Verificación**
Capacidades de ciberseguridad del servicio y controles compensatorios.

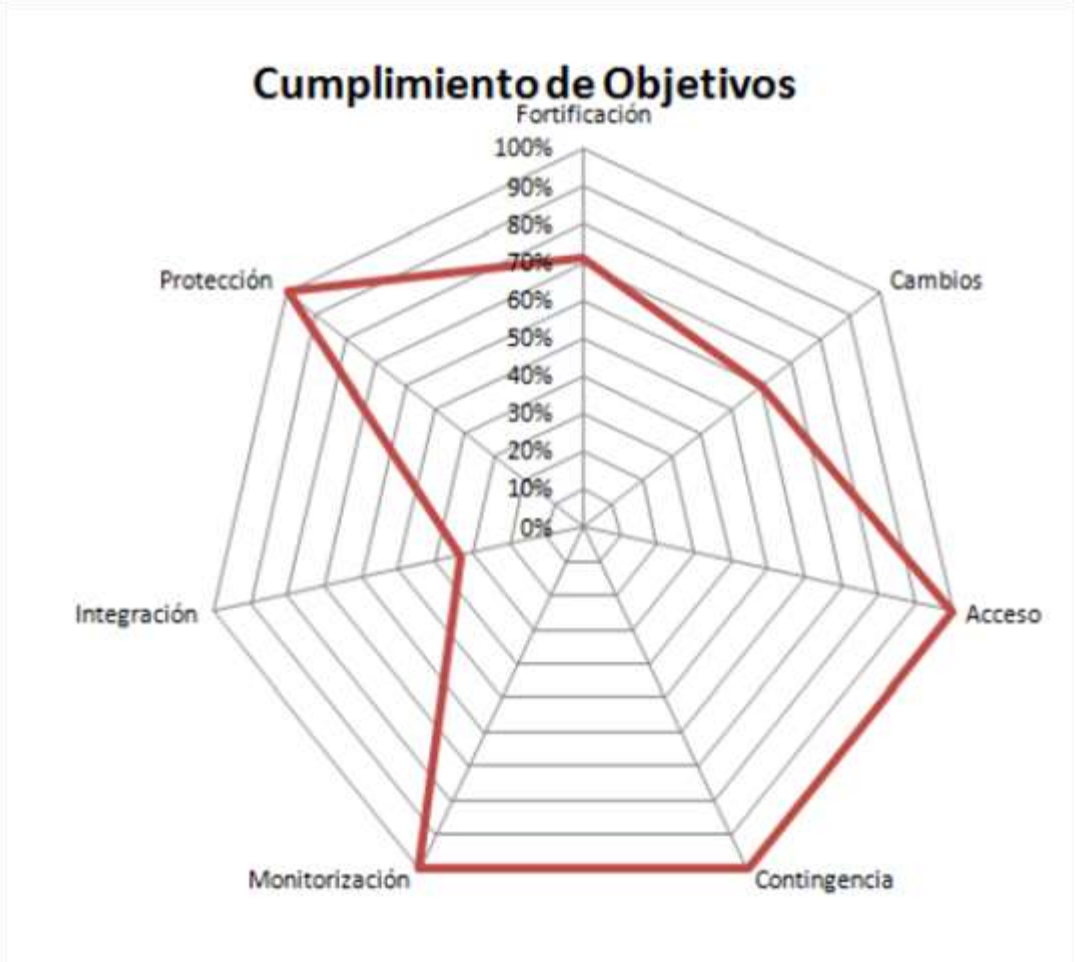
3 **Aceptación**
Demostración de que las capacidades de ciberseguridad están correctamente implementadas y que puede comenzar la provisión del servicio.

4 **Explotación**
Demostración de un correcto mantenimiento de las funciones de ciberseguridad y de una respuesta adecuada en caso de producirse eventos de ciberseguridad.

Objetivo	Requisito	Código	Tipo (B/M)	Complejidad	Cumplido (S/N/-)
Reconocimiento	El proveedor asegurará que el personal, propio o subcontratado, y los suministradores de materiales y componentes asignado a las actividades del servicio conocen los requisitos básicos de ciberseguridad establecidos por el cliente.	RO.Pr.1	B	1	N
	El proveedor dispone de políticas y procedimientos de ciberseguridad propios que complementan los del cliente y que son, al menos, igual de restrictivos que los de éste.	RO.Pr.2	M	2	S
	El proveedor dispone de mecanismos para hacer cumplir a su personal los procedimientos y las políticas de ciberseguridad establecidas por el cliente.	RO.Pr.3	M	3	N
	El proveedor deberá garantizar la existencia de personal de respaldo con el mismo perfil que el equipo que está dando el servicio o un plan realista de encontrarlo para prevenir la ocurrencia de rotación de personal	RO.Pr.4	M	2	S

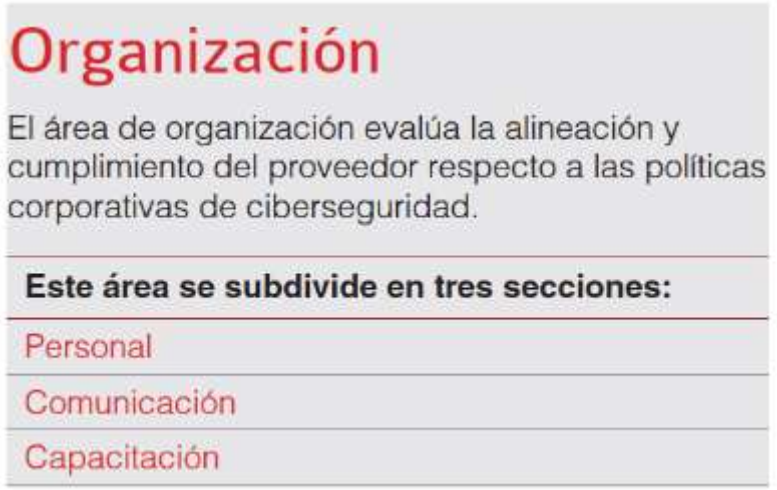
Terceras partes





Terceras partes

- Personal. Se estudian las responsabilidades en cuanto a ciberseguridad del personal del proveedor asignado a la prestación del servicio.
- Comunicación. Se analizan los mecanismos de comunicación utilizados entre cliente y proveedor durante la prestación del servicio.
- Capacitación. Trata los conocimientos, aptitudes y herramientas que posee el proveedor para la prestación del servicio.



Terceras partes

- Fortificación. Trata aspectos del servicio relacionados con su resistencia ante ataques o incidentes

- Cambios. Comprueba la manera en la que se gestionan las modificaciones realizadas sobre el servicio prestado y sobre los sistemas.

- Acceso. Controla la manera en que se realizan los accesos a los sistemas requeridos por el funcionamiento del servicio.

- Contingencia. Trata los mecanismos incorporados por el servicio para garantizar su funcionamiento ante incidentes.

Terceras partes

- Monitorización. Comprobar las capacidades que el servicio proporciona para el reporte y verificación de su funcionamiento.
- Integración. Revisar las capacidades y mecanismos que el servicio proporciona para el intercambio de información con sistemas externos.
- Protección. Verificar las medidas de protección de la información incorporadas por el servicio prestado.

Terceras partes

- **Despliegue**. Comprueba la instalación de los sistemas requeridos para la provisión del servicio.
- **Fortificación**. Comprueba la resistencia ante ataques o incidentes de seguridad.
- **Cambios**. Chequea como se gestionan las modificaciones realizadas sobre el servicio prestado y sobre los sistemas que éste requiere para su funcionamiento.
- **Acceso**. controla la manera en que se realizan los accesos a los sistemas requeridos por el funcionamiento del servicio.

Aceptación

El área de Aceptación trata de comprobar que las capacidades de ciberseguridad incluidas en el servicio están correctamente implementadas y que, por tanto, puede comenzar su provisión.

Las secciones del área de aceptación son:
Despliegue
Fortificación
Cambios
Acceso
Contingencia
Documentación
Protección

Terceras partes

- Despliegue. Demuestra que los componentes tecnológicos del servicio son correctamente mantenidos.
- Fortificación. Demuestra que los sistemas que soportan al servicio se mantienen asegurados correctamente.
- Cambios. Garantiza que los sistemas están actualizados en cuanto a parches de seguridad.
- Acceso. Demuestra que las credenciales de acceso y su utilización son revisadas periódicamente. Demuestra que los accesos remotos al servicio se realizan de la manera adecuada.

Explotación

El área de explotación está orientada a demostrar que se realiza un correcto mantenimiento de las funciones de ciberseguridad del servicio, así como una respuesta adecuada en caso de que ocurran eventos de ciberseguridad.

Las secciones del área de explotación son:
Despliegue
Fortificación
Cambios
Acceso
Contingencia
Documentación
Protección

Centro de Ciberseguridad Industrial

Escuela Profesional de Ciberseguridad Industrial

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO

EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA

DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

BASQUE INDUSTRY 4.0

TALLER PRÁCTIC0

Diagnóstico de Ciberseguridad en un entorno de automatización Industrial

Informe y presentación de resultados

Informe. Presentación de resultados

- Resultados más relevantes.
- Mantener actitud positiva.
- Centrarse en causas y consecuencias.
- Evitar detalles técnicos.
- Intercambio de opiniones.
- Posibles modificaciones al informe.

Centro de Ciberseguridad Industrial

Escuela Profesional de Ciberseguridad Industrial

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO

EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA

DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

Próximos pasos

- Proyectos resultantes del informe/recomendaciones.

- Plan de acción.
  - Recursos necesarios (internos/externos).
  - Importe aproximado.
  - Plazo de ejecución.

- Participación:
  - Ejecución.
  - Gestión.

BASQUE INDUSTRY 4.0

11 de marzo de 2018

Informe Diagnóstico de Ciberseguridad de Planta TRASTER

Pepe García

Contenido

Práctica

Presentación de resumen ejecutivo

Fortalezas
* ----
* ---
* ----

Debilidades
* ----
* ---
* ----

Acciones recomendadas
* ----
* ---
* ----

BASQUE INDUSTRY 4.0

Calendario 2020 de la Escuela Profesional de Ciberseguridad Industrial

TALLERES, CURSOS y MÁSTER	DURACIÓN	PLAZAS	CALENDARIO 2020										
			ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
T01. Taller Evaluación de Madurez del Proceso de Ciberseguridad en Organizaciones Industriales	7H 9:30 A 17:30	12 presenciales 6 virtuales			Lunes 9					Lunes 21			
T02. Taller Diagnóstico de Ciberseguridad en un entorno de Automatización Industrial	7H 9:30 A 17:30	12 presenciales 6 virtuales		Lunes 10				Lunes 8					Lunes 14
T03. Taller Ciberseguridad en el Ciclo de Vida de un Proyecto Industrial	7H 9:30 A 17:30	12 presenciales 6 virtuales			Lunes 23						Lunes 19		
T04. Taller Aplicación de un Sistema de Gestión de la Ciberseguridad Industrial	7H 9:30 A 17:30	12 presenciales 6 virtuales	Lunes 20				Lunes 11					Lunes 2	
T05. Taller Análisis Forense en un entorno de automatización industrial	7H 9:30 A 17:30	12 presenciales 6 virtuales				Lunes 27						Lunes 23	
C01. Curso multidisciplinar de Seguridad Digital en la Industria [4.0] y Protección de servicios esenciales	23H 2 jornadas y 1 mañana	35 presenciales										X 18, J 19 y V 20	
C02. Curso Responsable de Ciberseguridad en IACS (Sistemas de Automatización y Control Industrial)	16H 2 jornadas	25 presenciales				M 21 X 22					M 6 X 7		
M01. Máster Profesional Online de Ciberseguridad Industrial (Título propio; 9 trabajos)	450H 12 masterclass de 19:00 a 20:30	20 virtuales			MOD1	MOD2	MOD3	MOD4	TFM				

Contacto | Buscar... | Plataforma colaborativa | Inglés

Centro de Ciberseguridad Industrial

El Centro | Actividades | Beneficios | Ecosistema | Opinión

Portal CCI > El Centro > Sala de Prensa > Actividad-detalles

- El Centro
- El Equipo
- Sala de Prensa
- Decálogo de ética

Programa de Reconocimiento del Compromiso con la Ciberseguridad Industrial

3 marzo 2017

CCI, ha lanzado este nuevo proyecto cuyo objetivo es, precisamente, el reconocimiento de aquellos profesionales de su ecosistema ocupados y preocupados por la ciberseguridad industrial y las consecuencias de "lo ciber" en el seno de sus organizaciones, o como eje central de su formación, y que demuestren un compromiso con el desarrollo de esta disciplina.

Tweet

BASQUE INDUSTRY 4.0

		Estudiante			Profesional		
1	Tener 25 años o menos	√	√	√			
2	Ser miembro del ecosistema CCI	√	√	√	√	√	√
3	Acceso a la documentación del Centro y participación activa en el ecosistema CCI					√	√
4	Asistencia a eventos sobre la temática	8h	16h	24h	8h	16h	24h
5	Formación en ciberseguridad industrial	8h	20h	30h	8h	20h	30h
6	Trabajo de investigación sobre ciberseguridad Industrial			√			√
7	Experiencia en proyectos/publicaciones/docencia en ciberseguridad industrial			√			√
8	Superar test online	√	√	√	√	√	√

BASQUE INDUSTRY 4.0

Categoría estudiante nivel blanco

Categoría estudiante nivel verde

Categoría estudiante nivel negro

Categoría profesional nivel blanco

Categoría profesional nivel verde

Categoría profesional nivel negro

Centro de Ciberseguridad Industrial

Escuela Profesional de Ciberseguridad Industrial

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

BASQUE INDUSTRY 4.0

Muchas gracias

Centro de Ciberseguridad Industrial

Escuela Profesional de Ciberseguridad Industrial

BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA GOBIERNO VASCO

EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA

DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS