A los escudos!! Vamos a controlar esto!

Hasta ahora, hemos visto los grupos en los que se dividen los sistemas de control industrial debido a su naturaleza, y los ataques que pueden sufrir dichos grupos a manos de los hackers y los impactos que estos provocan, pero, todos esos incidentes como se pueden parar? Que amenazas tenemos que valorar para que eso no pase? Deberíamos anticiparnos a ellos y para eso tenemos que analizar todo muy a fondo. Gracias a El CCN-CERT y a su guía, tenemos una amplia especificación ERS (escenarios de riesgos) en sistemas de control industrial que nos darán una idea clara de las vulnerabilidades de cada sistema y las posibles amenazas. Así que, trabajemos como auditores, juguemos al juego de auditar. Vamos a Coger varias situaciones de riesgo dentro de los sistemas de control industrial y buscar los controles adecuados para auditar dichas situaciones. Aquí tenéis la tabla resuelta.

ESCENARIOS DE RIESGO	CONTROLES
· **En dispositivos portátiles**	

o Copias de seguridad de información de la lógica en ejecución en discos duros externos.	8.3.1 Gestión de soportes extraíbles. 10.5.1 Copias de seguridad de la información. 11.2.1 Emplazamiento y protección de equipos. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 12.3.1 Copias de seguridad de la información.
o Uso de USB para el traspaso de información.	8.3.1 Gestión de soportes extraíbles. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
· **En trabajo de terceros**	
o Conexión con equipos PC portátiles no revisados al sistema de control.	6.2.2 Teletrabajo 9.1.2 Control de acceso a las redes y servicios asociados 10.6.1 Controles de red. 10.6.2 Seguridad de los servicios de red.

o Existencia de conexiones para mantenimiento remoto de las que no se guarda ningún tipo de registro en el sistema o sobre el que no hay un control de acceso adecuado	6.2.2 Teletrabajo 12.4.1 Registro y gestión de eventos de actividad. 9.1.2 Control de acceso a las redes y servicios asociados 10.2.2 Supervisión y revisión de los servicios prestados por terceros. 10.6.1 Controles de red. 10.6.2 Seguridad de los servicios de red.
· **En interconexiones con otras redes**	
o Integración de procesos con socios (partners).	6.2.1 Identificación de los riesgos derivados del acceso de terceros. 6.2.3 Tratamiento de la seguridad en contratos con terceros.
o Uso de redes públicas de comunicación.	9.1.2 Control de acceso a las redes y servicios asociados
· **En gestión deficiente de copias de seguridad**	
o No verificación de las copias de seguridad del ICS.	10.5.1 Copias de seguridad de la información.

o No ejecución de copias de seguridad previas a actualizaciones de cualquier tipo.	10.5.1 Copias de seguridad de la información.
· **En falta de concienciación del personal**	
o Uso inadecuado de los equipos del ICS.	7.1.3 Uso aceptable de los activos. 8.2.3 Proceso disciplinario.
o Incapacidad para reconocer un incidente y/o desconocimiento de cómo comunicarlo o actuar	8.1.1 Funciones y responsabilidades. 8.2.3 Proceso disciplinario.
· **En inadecuada gestión de cambios**	
o No se realiza borrado seguro de los equipos del ICS	9.2.6 Reutilización o retirada segura de equipos. 9.2.7 Retirada de materiales propiedad de la empresa.
· **En inexistencia de planes adecuados de gestión de incidentes y continuidad**	
o Organizaciones sin gestión de la ciberseguridad o donde el alcance no incluye los ICS.	12.1.1 Análisis y especificación de los requisitos de seguridad. 10.10.5 Registro de fallos.

o Planes de emergencias que no contemplan un incidente de ciberseguridad como causa de la situación de emergencia.	13.1.1 Notificación de los eventos de seguridad de la información. 10.10.5 Registro de fallos.
· **En gestión deficiente de la información**	
o Obligación legal de publicar cierta información	6.1.5 Acuerdos de confidencialidad. 6.1.1 Compromiso de la Dirección con la seguridad de la información.
o · La información que se comparte con los proveedores se envía en claro a través de correo electrónico o se utilizan plataformas no verificadas por la organización.	6.1.8 Revisión independiente de la seguridad de la información. 10.8.1 Políticas y procedimientos de intercambio de información. 10.8.4 Mensajería electrónica.
· **En gestión deficiente del software**	
o No existe un inventario de programas y versiones de cada equipo.	7.1.1 Inventario de activos.
o No se revisan de manera periódica los equipos en búsqueda de documentación o software no pertinente.	9.2.4 Mantenimiento de los equipos. 7.1.3 Uso aceptable de los activos.

· **En asignación deficiente de responsabilidades y gestión de la seguridad**	
o No existe un responsable de ciberseguridad de los ICS.	6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.
o No existen procedimientos para la transferencia de propiedad de activos	7.1.2 Propiedad de los activos. 9.2.7 Retirada de materiales propiedad de la empresa.
· **En gestión deficiente de usuarios y contraseñas**	
o No se renuevan las contraseñas del ICS.	11.1.1 Política de control de acceso. 11.3.1 Uso de contraseñas.
o Los operadores usan usuarios genéricos en vez de nominales.	11.1.1 Política de control de acceso. 11.3.1 Uso de contraseñas.
o Existen usuarios y contraseñas escritas junto a los equipos del ICS.	11.1.1 Política de control de acceso. 11.3.1 Uso de contraseñas.
o Existen equipos o software desfasado	11.3.2 Equipo de usuario desatendido. 9.2.4 Mantenimiento de los equipos.

· **En falta de gestión técnica de la seguridad y sistemas**	
o No se hace uso de protocolos cifrados en la red de control	12.3.1 Política de uso de los controles criptográficos.

Como podéis ver los sistemas de control industrial más atacados son los sistemas SCADA que esta basados en datos, a los hackers les interesa mucho los datos de las cosas, saber cómo funcionan y recopilar cuanta más información y más valiosa mejor. Por lo tanto para poder analizar estos riesgos y obtener los controles más apropiados para solucionar esos riesgos he utilizado el estándar ISO 27002:2005 sobre la seguridad de la información.

Con el uso de esos controles prevendremos escenarios de riesgo que puedan provocar que nuestra empresa tenga vulnerabilidades a la vista y que puedan generar entradas fáciles para ataques o posibles incursiones.

REFERENCIAS:

https://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/ChecklistsGuidesISO17799Questionnaire!OpenDocument

http://www.iso27000.es/download/ControlesISO27002-2005.pdf

https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrial-ics/file.html

http://ieeexplore.ieee.org/document/7750821/