Centro de Respuestas a Incidentes Informáticos

CSIRT Académico UNAD

Boletín Informativo

Veintidós

Abril: Protegiendo los Sistemas Críticos en la Era de la Interconexión

VIEM Vicerrectoría de Innovación y Emprendimiento

ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veintidós
Abril de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Especialización en Seguridad Informática
CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Centro de Respuestas a Incidentes Informáticos CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CSIRT Académico UNAD

Semilleros de Investigación Ceros y Unos y Ciber cosmonautas adscritos al Grupo de Byte InDesign

Responsable de la Edición
ARNOL ARTURO TENORIO CAICEDO

Revisó
Hernando José Peña Hidalgo
Esp. Seguridad Informática

Estado legal:
Periodicidad: mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 22

Abril de 2024

“Protegiendo los Sistemas Críticos en la Era de la Interconexión"

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

ARNOL ARTURO TENORIO CAICEDO
Esp. Seguridad Informática
Estudiante

Eduard Antonio Mantilla Torres
Esp. Seguridad Informática
https://orcid.org/0000-0002-4690-3526

Ever Luis Arroyo Baron
Esp. Seguridad Informática
https://orcid.org/0009-0004-0725-2013

Introducción

La ciberseguridad industrial se ha transformado en un campo crítico debido a la progresiva interconexión de sistemas informáticos en entornos industriales y de infraestructura crítica. La protección de los sistemas de control industrial (ICS) y otros sistemas informáticos utilizados en estos entornos es esencial para responder a las medidas que requiere la seguridad, la disponibilidad y la integridad de las sistematizaciones industriales y de servicios públicos.

Los retos en ciberseguridad industrial incluyen la protección contra una amplia gama de amenazas, como la inyección de código malicioso, los ataques de denegación de servicio, la maniobra de datos y los ataques físicos. Además, la complejidad de los sistemas industriales y la composición de tecnologías que va saliendo, como el IoT y plantean desafíos adicionales en términos de seguridad como la inteligencia artificial.

Es decisivo realizar medidas de seguridad consistentes, como sistemas de localización de intrusiones y políticas de seguridad para los activos informáticos. Además, el aprendizaje del personal en prácticas mejores prácticas de cibernética es fundamental para proteger los sistemas industriales contra las crecientes amenazas cibernéticas.

exploramos la importancia de la ciberseguridad industrial y cómo los estándares y marcos de referencia, como el Marco NIST y la norma ISO/IEC 27002:2022, pueden ayudar a proteger los sistemas de control industrial y otros sistemas críticos. También analizamos los estándares ISA/IEC 62443, que proporcionan pautas específicas para la ciberseguridad de los sistemas de automatización y control industria

Desarrollo

Sistemas de control industrial

Conocidos como ICS debido a sus siglas en ingles Industrial **Control Systems en inglés** son sistemas informáticos utilizados en fábricas, plantas de energía y otros lugares para controlar procesos físicos, como la producción de bienes o el suministro de servicios.

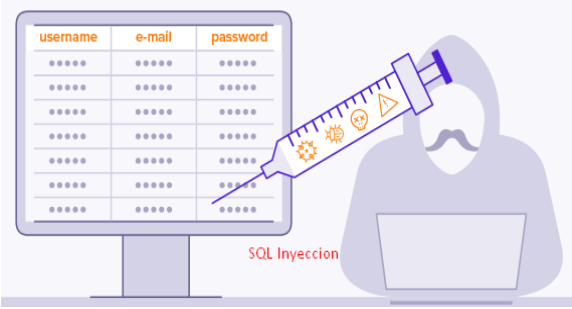
Se refieren a los sistemas utilizados en entornos industriales y de infraestructura crítica para controlar y monitorear procesos físicos. Estos sistemas incluyen componentes hardware y software especializados, como controladores lógicos programables, sistemas de supervisión y adquisición de datos y sistemas de control distribuido DCS. (EXPERTIS, 2016)

Estos son algunos de los ataques relacionados con ICS

Inyección de código: Consiste en insertar código malicioso en los sistemas de control para alterar su funcionamiento o robar información.

Ataques de denegación de servicio (DoS): Buscan saturar los sistemas de control con solicitudes, haciendo que dejen de responder y afectando la operatividad de los procesos controlados.

Ataques de manipulación de datos: Alteran los datos de los sistemas de control para inducir errores o cambios no deseados en los procesos industriales.



Fuente: https://www.avast.com/es-es/c-sql-injection

Intercepción de comunicaciones: Consiste en la captura de datos transmitidos entre los diferentes componentes de los sistemas de control para obtener información sensible o controlar los procesos.

Ataques físicos: Involucran el camino no permitido en los procedimientos de inspección para manipular o dañar los componentes.

ingeniería social: Buscan mentir a los usuarios para lograr acceso no permitido al sistema de control o información confidencial. (EXPERTIS, 2016)

Estos ataques pueden tener consecuencias graves, como interrumpir la producción, dañar la infraestructura o poner en peligro la seguridad pública. Por eso, es importante tomar medidas para proteger los sistemas de control industrial.

Desafíos de seguridad informática en ICS

Algunos de los desafíos que se pueden mencionar para Amenazas cibernéticas específicas: Los sistemas de control industrial enfrentan amenazas cibernéticas específicas, como malware diseñado para atacar sistemas SCADA o ataques de denegación de servicio (DoS) dirigidos a interrumpir operaciones críticas.

Interconexión creciente: La creciente interconexión de los sistemas de control industrial con redes corporativas e Internet aumenta la superficie de ataque y la exposición a amenazas cibernéticas. (ECYBERSECURE, 2022)

Obsolescencia tecnológica: Muchos sistemas de control industrial utilizan tecnologías obsoletas y sin soporte, lo que los hace vulnerables a las amenazas cibernéticas debido a la falta de actualizaciones de seguridad.

Falta de conciencia de seguridad: El personal que opera y mantiene los sistemas de control industrial a menudo carece de conciencia y capacitación adecuadas en seguridad cibernética, lo que puede llevar a prácticas inseguras y vulnerabilidades.

Complejidad de los sistemas: La complejidad de los sistemas de control industrial, que incluyen una variedad de dispositivos y componentes interconectados, dificulta la implementación de medidas efectivas de seguridad cibernética.

Integración de tecnologías emergentes: La composición de tecnologías salientes, como el IoT en los sistemas de control industrial introduce nuevos retos de seguridad informática y en la infraestructura por causa de mejores prácticas y estándares establecidos.

Cumplimiento normativo: El cumplimiento de normativas y estándares de seguridad cibernética en entornos industriales puede resultar complicado debido a la complejidad de los sistemas y la falta de claridad en los requisitos específicos para ICS.

Políticas públicas de ICS y la seguridad digital

Estas suelen abordar diversos aspectos para proteger la infraestructura crítica y garantizar la seguridad cibernética. Algunas de las políticas públicas comunes incluyen:

Regulaciones y estándares de seguridad: Establecer normativas y estándares de seguridad cibernética específicos para los sistemas de control industrial, como los estándares ISA/IEC 62443, para garantizar prácticas seguras y mitigar riesgos. (SOCIAL, 2020).

Coordinación entre sectores: Fomentar la colaboración entre sectores público y privado, así como entre países, para compartir información sobre amenazas y mejores prácticas de seguridad. (ECYBERSECURE, 2022)

Incentivos para la ciberseguridad: Ofrecer incentivos económicos o fiscales para que las organizaciones implementen medidas de ciberseguridad en sus sistemas de control industrial.

Capacitación y concienciación: Promover la capacitación y concienciación en seguridad cibernética entre los trabajadores y responsables de sistemas de control industrial para mejorar la respuesta ante amenazas.

Resiliencia y recuperación: Desarrollar procedimientos de réplica a incidentes y sistemas de recuperación que certificar la persistencia de las operaciones en caso de ciberataques.

Estimación de riesgos: ejecutar valoraciones habituales de los riesgos y fragilidades de los sistemas de control industrial para nivelar y disminuir amenazas. (SOCIAL, 2020).

Defensa de la privacidad: Establecer medidas para proteger la reserva de los datos del sistema de control industrial y garantizar su cumplimiento con las regulaciones de protección de datos. (ECYBERSECURE, 2022)

Estas políticas públicas buscan mejorar la seguridad cibernética en el sistema industrial y la protección la infraestructura crítica de posibles ciberataques. (Sanders, 2022)

Ciberseguridad Industria

Esta trata de salvaguardar los sistemas informáticos que controlan entidades, sistemas de salud, empresas como fábricas de energía y sistemas de transporte entre otros cientos. Estos sistemas, son vitales para mantener nuestras infraestructuras en funcionamiento.

Imagina que un hacker pudiera ingresar y manipular estos sistemas. Podría causar estragos, deteniendo la producción, dañando equipos y poniendo en peligro la seguridad pública. Para evitar esto, se utilizan medidas de ciberseguridad, como sistemas y firewalls de localización de delitos informáticos, para proteger estos sistemas y mantenerlos seguros y en funcionamiento. Además, es importante capacitar al personal en prácticas de seguridad cibernética para mantener estos sistemas seguros en todo momento. (Jove, 2021).

La Industria 4.0

Es un término que describe la adopción de tecnologías de la información y la comunicación (TIC) en la industria para crear entornos de producción más inteligentes, eficientes y autónomos. Algunos de los conceptos clave de la Industria 4.0 incluyen. (Deloitte, 2020).

Big Data: El estudio de grandes cantidades de datos generados por sistemas de producción para identificar patrones, tendencias y oportunidades de mejora.

Inteligencia Artificial (IA): El uso de algoritmos y modelos computacionales para simular procesos de pensamiento humano, como el aprendizaje automático y el reconocimiento de patrones, para optimizar la producción y la toma de decisiones.

Computación en la nube: El uso de recursos informáticos remotos a través de internet para almacenar datos, ejecutar aplicaciones y realizar análisis, lo que permite una mayor flexibilidad y escalabilidad en los procesos industriales.

Realidad aumentada (RA): La superposición de información digital, como gráficos y datos, sobre el mundo físico para mejorar la visualización, la capacitación y el mantenimiento de equipos en entornos industriales.

Fabricación aditiva: También conocida como impresión 3D, permite la creación de componentes y productos mediante la adición de capas sucesivas de material, lo que ofrece mayor flexibilidad y eficiencia en la producción. En conjunto, estas tecnologías están transformando la forma en que se diseñan, fabrican y gestionan los productos, permitiendo a las empresas adaptarse rápidamente a las demandas del mercado y mejorar su competitividad en un entorno globalizado.

que deben abordarse mediante la implementación de medidas de seguridad adecuadas.

Infraestructura critica

Se trata de sistemas y activos físicos, tecnológicos y humanos que son esenciales para el funcionamiento de una sociedad y economía. Esto incluye sectores como el suministro de energía, el transporte, las comunicaciones, la salud, el agua, la seguridad pública y otros servicios que son fundamentales para mantener la vida diaria y el bienestar de la población. La protección de la infraestructura crítica es crucial para garantizar la seguridad nacional y el funcionamiento continuo de la sociedad. (Agency, 2021)

Sistemas de control industrial

son conjuntos de dispositivos electrónicos y software que se utilizan para controlar procesos y maquinaria en entornos industriales. Estos sistemas se encargan de monitorear variables como temperatura, presión, flujo, nivel, entre otros, y de ajustar los parámetros de control para garantizar que los procesos se lleven a cabo de manera eficiente y segura.

Es decir, son como el cerebro y los nervios de una fábrica o planta. Ayudan a controlar máquinas y procesos para

que funcionen correctamente y produzcan cosas de manera eficiente. Estos sistemas se aseguran de que todo esté en el lugar correcto, en el momento correcto, y de que las cosas se hagan de manera segura y sin problemas. Son como el director de una orquesta, asegurándose de que cada instrumento toque en armonía para crear una hermosa melodía de producción. (Deloitte, 2020)

Los sistemas de control industrial pueden incluir diferentes componentes, como controladores lógicos programables técnicamente conocidos como PLC, sistemas de control distribuido también llamados DCS, sistemas de supervisión, control y adquisición de datos técnicamente SCADA, entre otros. Estos sistemas son fundamentales en la automatización de procesos industriales, ya que permiten mejorar la calidad de los productos, aumentar la productividad y reducir los costos de operación. diseñados para controlar y monitorear diferentes procesos industriales. Algunos de los más importantes incluyen son

Controladores Lógicos Programables: Son dispositivos electrónicos programables utilizados para controlar procesos en tiempo real, como en líneas de producción en fábricas.

Sistemas de Control Distribuido: Son sistemas que controlan y monitorean múltiples equipos y procesos en una planta industrial, permitiendo la comunicación entre ellos.

Sistemas de Supervisión, Control y Adquisición de Datos: Estos sistemas supervisan y controlan procesos industriales a larga distancia, a menudo a través de redes de comunicación. (PÚBLICA, 2018)

Sistemas de Control de Procesos: Se utilizan para controlar procesos continuos o batch en industrias como la química, petroquímica y de alimentos.

Sistemas de Instrumentación y Control I&C: Incluyen dispositivos y sistemas utilizados para medir, controlar y monitorear variables como temperatura, presión, flujo, nivel, etc.

Sistemas de Automatización de Edificios (BAS): Se utilizan en edificios comerciales para controlar sistemas como calefacción, ventilación, aire acondicionado, iluminación, etc.

Cada sistema tiene su importancia dependiendo del contexto y los procesos industriales que se estén controlando. Los PLC y los DCS suelen ser los más comunes y fundamentales en muchas aplicaciones industriales. (PÚBLICA, 2018)

Conocido como National Institute of Standards and Technology son conjuntos de modelos, mejores prácticas y pautas para mejorar la ciberseguridad en entidades públicas o privadas. Proporciona un enfoque estructurado y basado en riesgos para encargarse y mejorar la seguridad de la información, contenida la ciberseguridad industrial. El marco NIST se centra en ayudar a las organizaciones a identificar, proteger, detectar, responder y recuperarse de las amenazas cibernéticas.

Por otro lado, la norma ISO/IEC 27002:2022 es parte de la serie de normas ISO/IEC 27000 y proporciona pautas (Agency, 2021)detalladas para la implementación de controles de seguridad de la información. Esta norma se centra en aspectos específicos de la seguridad de la información, como la gestión de activos, el control de accesos, la seguridad en el desarrollo y mantenimiento de sistemas, la gestión de incidentes, entre otros.

Ambos marcos son importantes en el contexto de la ciberseguridad industrial, ya que proporcionan orientación y mejores prácticas para proteger los sistemas de control industrial y otros sistemas críticos contra las amenazas cibernéticas. (EUROPEAS, 2005)

Boletín de Ciberseguridad

Reflexión

Si las infraestructuras críticas, como las redes eléctricas, sistemas de agua, hospitales y transporte, son vulneradas por ciberdelincuentes, el impacto podría ser devastador a nivel mundial y local.

A nivel mundial, podríamos enfrentar interrupciones masivas en los servicios básicos, como la energía y el agua, lo que afectaría a millones de personas y empresas. Esto podría provocar caos y dificultades para mantener el orden público. Además, las infraestructuras críticas son fundamentales para la economía global, por lo que un ataque exitoso podría tener repercusiones en los mercados financieros y en el comercio internacional.

A nivel local, los impactos serían igualmente graves. Por ejemplo, un ataque a un hospital podría poner en peligro vidas al interrumpir los servicios médicos. Del mismo modo, un ataque a una red eléctrica podría dejar a una ciudad entera sin electricidad durante días o semanas, causando estragos en la vida diaria y en la economía local.

En resumen, la vulnerabilidad de las infraestructuras críticas ante los ciberdelincuentes es un tema de gran importancia, ya que un ataque exitoso podría tener consecuencias desastrosas a nivel mundial y local. Por lo tanto, es fundamental tomar medidas para proteger estas infraestructuras y prevenir posibles ataques cibernéticos.

Ciberseguridad y ciberdefensa ICS

Técnica: La ciberseguridad en sistemas de control industrial (ICS) se refiere a la protección de los sistemas informáticos que controlan procesos físicos en entornos industriales. Incluye medidas para proteger estos sistemas contra ataques cibernéticos, como el malware y los ataques de denegación de servicio, que podrían interferir con la operación segura de los procesos industriales.

Formal: La ciberseguridad en ICS implica la implementación de políticas, procedimientos y tecnologías para proteger los sistemas de control industrial contra amenazas cibernéticas. Esto incluye la identificación de vulnerabilidades, la implementación de controles de seguridad y la respuesta a incidentes de seguridad para garantizar la disponibilidad, integridad y confidencialidad de los sistemas y datos. (Santos, 2021)

Cotidiana: En términos simples, la ciberseguridad en sistemas de control industrial se trata de proteger las fábricas, plantas de energía y otros lugares donde se controlan procesos físicos importantes de los ataques cibernéticos. Es como asegurarse de que nadie pueda ingresar de manera no autorizada a los sistemas que controlan estos procesos para evitar daños o interferencias. La ciberdefensa, por otro lado, implica estar preparado para responder a posibles ataques y minimizar su impacto en caso de que ocurran.

Otros

Adicional a lo ya planteado para esta fase y en el presentes boletín también se debe hablar de

Seguridad física: La seguridad física de los sistemas de control industrial es crucial para proteger los equipos y istemas contra el acceso no autorizado, daños intencionales o accidentales, y robos.

Resiliencia y continuidad del negocio: Es importante desarrollar planes de respuesta a incidentes y de continuidad del negocio para garantizar que los sistemas de control industrial puedan recuperarse rápidamente de posibles interrupciones y mantener la operación en caso de ataques cibernéticos u otros eventos adversos.

Gestión de riesgos: La gestión de riesgos en sistemas de control industrial implica identificar, evaluar y mitigar los riesgos asociados con la seguridad cibernética, la seguridad física y otros riesgos operativos que puedan afectar la operación segura de los sistemas.

Normativas y estándares: Existen normativas y estándares específicos para la seguridad de los sistemas de control industrial, como los estándares ISA/IEC 62443, que proporcionan pautas y mejores prácticas para proteger los sistemas contra amenazas cibernéticas.

Integración de tecnologías emergentes: La integración de tecnologías emergentes, como el Internet de las cosas (IoT) y la inteligencia artificial, en los sistemas de control industrial plantea nuevos desafíos de seguridad

Conclusiones

Podríamos terminar diciendo que la ciberseguridad y la protección de los sistemas de control industrial (ICS) son aspectos críticos en la gestión de la seguridad de infraestructuras críticas a nivel mundial y local. La interconexión creciente de estos sistemas con redes corporativas e Internet, junto con la integración de tecnologías emergentes como el IoT y la inteligencia artificial, ha aumentado la complejidad y el riesgo de posibles ataques cibernéticos.

Para abordar estos desafíos, es necesario implementar medidas de seguridad física y cibernética robustas, cumplir con normativas y estándares específicos como los estándares ISA/IEC 62443, y desarrollar planes de resiliencia y continuidad del negocio para garantizar la operación segura y continua de los sistemas de control industrial.

Además, la concienciación y capacitación del personal en prácticas de ciberseguridad son fundamentales, al igual que la colaboración entre sectores público y privado para compartir información sobre amenazas y mejores prácticas. Solo a través de un enfoque integral y proactivo en la ciberseguridad de los sistemas de control industrial podemos mitigar eficazmente los riesgos y proteger nuestras infraestructuras críticas de posibles ataques cibernéticos.

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:


Correo: csirt@unad.edu.co


Página web: https://csirt.unad.edu.co

Bibliografía

Agency, C. &. (2021). *CISA Year in Review 2021.Open this document with ReadSpeaker docReader.* Obtenido de https://www.cisa.gov/sites/default/files/publications/21-0860_EOY_REPORT_508c.pdf

Deloitte. (2020). *El Impacto de la Ciberseguridad en la "Infraestructura Crítica" de la nueva normalidad.* Obtenido de https://www2.deloitte.com/content/dam/Deloitte/cl/Documents/povs-covid19/nuevos/cl-impacto-ciberseguridad-infraestructura-cr%C3%ADtica-nueva-normalidad.pdf

ECYBERSECURE. (2 de febrero de 2022). *Panorama global de amenazas afectando a infraestructura crítica mundial.* Obtenido de https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1153/

EUROPEAS, L. C. (2005). *Libro verde sobre un Programa Europeo para la Protección de Infraestructuras Críticas PEPIC.Open this document with ReadSpeaker docReader.* Obtenido de https://www.ucm.es/data/cont/media/www/pag-72481/UNISCIDP35-17DELRIO-MIRANZO.pdf

EXPERTIS, G. F. (noviembre de 2016). *LOBAL FORUM ON CYBER EXPERTISE.* Obtenido de https://www.meridianprocess.org/siteassets/web_106011_tno_brochure-good-practice-guide---spaans-def.pdf

Jove, E. C.-R. (2021). *Revista DYNA.* Obtenido de https://books.google.es/books?hl=es&lr=&id=GoNTEAAAQBAJ&oi=fnd&pg=PP9&dq=que+es+Ciberseguridad+industrial&ots=bvef2zqnKr&sig=gnFCDUybidq7oXqLocDQ4BsF47I#v=onepage&q=que%20es%20Ciberseguridad%20industrial&f=false

PÚBLICA, F. (2018). *Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades públicas.* Obtenido de http://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Sanders, P. B. (2022). *Critical energy infrastructure and the evolution of cybersecurity.* Obtenido de https://www-sciencedirect-com.bibliotecavirtual.unad.edu.co/science/article/pii/S1040619022001506

Santos, L. (2021). *Ciberseguridad e Infraestructuras Críticas. En UEM STEAM Essentials.Open this document with ReadSpeaker docReader.* Obtenido de Ciberseguridad e Infraestructuras Críticas. En UEM STEAM Essentials.Open this document with ReadSpeaker docReader

SOCIAL, C. N. (2020). *Política Nacional de Confianza y Seguridad Digital.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf