INSTITUTO COSTARRICENSE DE
ACUEDUCTOS Y ALCANTARILLADOS

UEN Investigación y Desarrollo
Centro Documentación e Información

Formulario: Informe técnico final Vigilancia Científica Tecnológica (VCT). Búsqueda documental sobre Ciberseguridad en Empresas de Sistemas de Agua Potable y Saneamiento

Fecha de entrega: 27-10-2022

CÓDIGO DE REGISTRO DEL DOCUMENTO: 2022-106-323

Elaborado por:	Revisado por:	Aprobado por:
ELVIRA GUEVARA RODRIGUEZ (FIRMA) Firmado digitalmente por ELVIRA GUEVARA RODRIGUEZ (FIRMA) Fecha: 2022.11.21 12:01:50 -06'00' Elvira Guevara Rodríguez	JUAN CARLOS FLORES ZUÑIGA (FIRMA) Firmado digitalmente por JUAN CARLOS FLORES ZUÑIGA (FIRMA) Fecha: 2022.11.21 12:23:50 -06'00' MA. Juan Carlos Flores Zúñiga	GERMAN GUSTAVO MORA RODRIGUEZ (FIRMA) Firmado digitalmente por GERMAN GUSTAVO MORA RODRIGUEZ (FIRMA) Fecha: 2022.11.21 13:37:22 -06'00' Ing. German Mora Rodríguez

Instituto Costarricense de Acueductos y Alcantarillados
Centro de Documentación e Información
UEN Investigación y Desarrollo

AUTORIZACIÓN INSTITUCIONAL PARA PUBLICAR TESIS, ESTUDIOS, ARTÍCULOS Y/O INFORMES PROPIEDAD INTELECTUAL DE AyA EN EL REPOSITORIO DIGITAL DEL CEDI

Yo, Jorge Luis Zapata Arroyo

_____

_____

N° Cédula: 2-0564-875

_____

Dependencia: Gerencia General

_____

Autorizo como Gerente General y representante legal del Instituto Costarricense de Acueductos y Alcantarillados (AyA) cédula jurídica 4-000-042138 al Centro de Documentación e Información (CEDI) de la UEN Investigación y Desarrollo la inclusión, publicación y difusión en su Repositorio Digital y Catálogo en línea (OPAC) la documentación incluida en la lista adjunta.

Se trata de estudios y documentos cuyos derechos intelectuales y de uso son exclusivos de nuestra institución.

E-mail: gerenciageneral@aya.go.cr **N° Teléfono**: 2242-5090

JORGE LUIS ZAPATA ARROYO (FIRMA)
Firmado digitalmente por JORGE LUIS ZAPATA ARROYO (FIRMA)
Fecha: 2022.08.29 19:48:12 -06'00'

Firma: _____

TABLA DE CONTENIDOS

1. INTRODUCCIÓN 3
1.1. Antecedentes 3
1.2. Objetivos 3
1.2.1. Objetivo General 3
1.3. Alcance de la solicitud 3
1.4. Limitaciones 4
2. METODOLOGÍA 4
2.1. Conformación del equipo CEDI 4
2.2. Actividades realizadas 4
3. RESULTADOS 5
4. CONCLUSIONES 5
5. RECOMENDACIONES 5
6. REFERENCIAS BIBLIOGRÁFICAS 6
7. ANEXOS 14

1. INTRODUCCIÓN

1.1. Antecedentes

El director de la UEN de Investigación y Desarrollo, Ing. German Mora Rodríguez, realizó una serie de solicitudes de vigilancia científico-tecnológica (VCT) al Centro de Documentación e Información (CEDI), con base en la minuta UEN-ID-2022-00488 del 23/08/2022. La cual fue aprobada por el CEDI de acuerdo con la modalidad y programación que se adjuntó al memorando UEN-ID-2022-00492 del 31/08/2022 comunicado al solicitante.

La primera solicitud de VCT corresponde a ***Ciberseguridad en Empresas de Sistemas de Agua Potable y Saneamiento***. La misma fue registrada en el PIDi de la UEN-ID con el N° 2022- 06-164 con fecha 6-09-2022.

1.2. Objetivos

1.2.1. Objetivo General

Contar con información actualizada y documentada sobre las investigaciones o propuestas que se han desarrollado a nivel nacional e internacional sobre el tema de ciberseguridad en empresas que administran sistemas de agua potable y saneamiento, para que sirva como referencia para consultas de los funcionarios de AyA, en general, y funcionario de la Dirección de Sistemas de Información institucional para la toma de decisiones en materia de ciberseguridad.

1.3. Alcance de la solicitud

Obtener información de referencia que permita fortalecer e implementar con criterio los niveles de seguridad en los sistemas administrados por AyA. Además de contar con las experiencias y aprendizaje de investigadores y expertos a nivel internacional sobre el tema.

1.4. Limitaciones

Se realizó un proceso de búsqueda de información prospectiva utilizando los diferentes recursos bibliográficos disponibles en línea sobre la temática; sin embargo, a nivel nacional se identificaron limitadas fuentes de información; además, de que la mayor parte de los datos acopiados y procesados en publicaciones especializadas están disponibles en inglés.

2. METODOLOGÍA

Para elaborar el VCT, se acudió a diferentes fuentes de información como: Google Académico, sitios especializados en agua potable y saneamiento, y base de datos de Taylor And Francis Online; plataforma multidisciplinaria con revistas científicas arbitradas que cuenta con otras bases de datos de consulta.

Adicionalmente, como parte de la metodología acordada con el solicitante, se realizó una entrevista al Ing. Luis Fernando Vargas Ulate, director del Área de Ingeniería en Tecnologías del AyA para que sumara su experticia en el tema investigado.

2.1. Conformación del equipo CEDI

El responsable del subproceso, Mag. Juan Carlos Flores Zúñiga, realiza la programación del VCT según el subproceso establecido asignando como responsable de esta actividad a la Licda. Elvira Guevara Rodríguez. La investigación dio inició el 31 de agosto del 2022, y se programó la entrega para el 31 de octubre del presente.

2.2. Actividades realizadas

Para realizar este trabajo se llevaron a cabo las siguientes actividades:

- Búsqueda de información por palabras claves en inglés y español sobre la temática en los diferentes sitios web a saber: Google Académico, Google Scholar, sitios especializados, base de datos especializada Taylor And Francis Online.

- Revisión de cada uno de los archivos en formato pdf. recuperados, con el propósito de valorar la pertinencia de la información.

- Acopio de la información y elaborar las referencias bibliográficas de todo el material seleccionado.

- Entrevista realizada al Ing. Luis Fernando Ulate Vargas, experto en el tema. **(Anexo).**

3. RESULTADOS

Como producto final se incluye el Informe Técnico Final Vigilancia Científico-Tecnológica (VCT), con base en los recursos acopiados, procesados y su condensación en el reporte para el tema investigado. Además, de la información procesada se incluye un breve resumen en español e inglés de cada una de las referencias que corresponden a artículos en línea y acceso al documento digital para su respectiva descarga a conveniencia.
También se cuenta con los documentos en formato pdf., en nuestro acervo en caso de que se requiera su entrega de manera alternativa.

4. CONCLUSIONES

De acuerdo con la investigación realizada se determinó que existe suficiente información a nivel internacional sobre el tema de marras, entre ellos; informes, investigaciones, estudios, propuestas y recomendaciones sobre el tema de ciberseguridad en sistemas de agua potable y saneamiento.

5. RECOMENDACIONES

No aplican en este reporte.

6. REFERENCIAS BIBLIOGRÁFICAS

1. Borja Pérez. (2021). Sector del agua: ciberseguridad en un entorno con necesidades propias. (artículo técnico). *Revista digital en linea Red de Seguridad.* https://www.redseguridad.com/sectores/servicios-esenciales-pic/sector-del-agua-ciberseguridad-en-un-entorno-con-necesidades-propias_20211225.html.

Resumen

El artículo hace énfasis en la importancia que tiene la ciberseguridad en el sector de agua potable y organizar su ciberresiliencia cada vez más frecuentes y peligrosos. Por lo que es importante realizar cambios necesarios como reforzar el marco normativo, mejorar la cooperación fronteriza y avanzar en la concienciación de los usuarios. Además de contar con la mejor tecnología, con el fin de contar con una industria mejor protegida en el futuro.

Abstract

The article emphasizes the importance of cybersecurity in the drinking water sector and organizing its increasingly frequent and dangerous cyberresilience. Therefore, it is important to make necessary changes such as reinforcing the regulatory framework, improving border cooperation, and advancing in user awareness. In addition to having the best technology, in order to have a better protected industry in the future.

2. Clark, Robert M., Panguluri, Srinivas, Nelson, Trent D., & Wyman, Richard P. Protecting drinking water utilities from cyberthreats. (2016). Protecting drinking water utilities from cyber threats. United States. https://www.osti.gov/pages/servlets/purl/1372266.

Resumen

Los desafíos de la seguridad cibernética tienen el potencial de convertirse en uno de los problemas definitorios de nuestro tiempo. Los ataques cibernéticos se han transformado en una amenaza cada vez mayor. Por ejemplo, las empresas de servicios públicos de agua potable están incorporando cada vez más tecnología en

sus operaciones rutinarias y, por lo tanto, son cada vez más vulnerables a las ciberamenazas.

Entre 2014 y 2015, el número de los incidentes del Sector Agua aumentaron un 78,6% (de 14 a 25). En este documento, se analizan los siguientes aspectos; preocupaciones de EE. UU. sobre la seguridad cibernética, relación de la ciberseguridad con la protección de infraestructuras críticas, designación del suministro de agua en los EE. UU. como infraestructura crítica y nuevos enfoques tecnológicos que se pueden utilizar para mejorar la protección de la infraestructura, incluidos los sistemas de abastecimiento de agua.

Abstract

SCADA systems vary in complexity, as indicated by the sample of four utilities evaluated in this study. The American Water Works Association (AWWA) has developed a cyber security tool that offers a layered approach for utilities to address cyber threats. The Division of Public Health State Drinking Water Loan Funds Program initiated actions to investigate cybersecurity in the State's water services. This study recommends that the division adopt a common set of controls applicable to all utilities with SCADA systems in Delaware.

3. Donoso, M. C. (2022). Foro: ¿Cuán importante es la seguridad cibernética para lograr la seguridad hídrica? *Revista de Ciencias Ambientales*, *56*(1), 284-297. https://doi.org/10.15359/rca.56-1.15.

Resumen

El artículo expone una visión amplia del concepto de seguridad hídrica e ilustra la amenaza real de ataques cibernéticos, identificando los diversos elementos que pueden ser objeto de los ciberdelincuentes. Las consideraciones finales apuntan a sugerir acciones de sensibilización del sector del agua ante los peligros de agresiones cibernéticas y adelantar gestiones tendientes a consolidar la ciberseguridad para propiciar o fortalecer una seguridad hídrica sostenible.

Abstract

This article presents a broad vision of the concept of water security and illustrates the real threat of cyberattacks, identifying the various elements that

can be targeted by cybercriminals. The final considerations aim to suggest actions to raise awareness of the water sector in the face of the dangers of cybernetic attacks

and to take steps to consolidate cybersecurity to facilitate or strengthen Sustainable Water Security.

4. Environmental Protection Agency. (s.f.). Water sector cybersecurity brief for states.https://www.epa.gov/sites/default/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf

Resumen

La implementación de las mejores prácticas de ciberseguridad es fundamental para las empresas de servicios públicos de agua y aguas residuales. Los ciberataques son una amenaza creciente para los sectores de infraestructura crítica. Muchas instalaciones de infraestructura crítica han experimentado incidentes de ciberseguridad que llevaron a la interrupción de un proceso de negocio o una operación crítica. El artículo plantea también los daños significativos que pueden causar los ataques cibernéticos en empresas de servicios públicos, los beneficios y desafíos para las empresas al iniciar un programa de ciberseguridad.

Abstract

Implementing cybersecurity best practices is critical for water and wastewater utilities. Cyber-attacks are a growing threat to critical infrastructure sectors. Many critical infrastructure facilities have experienced cybersecurity incidents that led to the disruption of a business process or critical operation. The article also raises the significant damage that cyber-attacks can cause in public service companies.

5. Germano, Judith H. (2019). Cybersecurity risk & responsibility in the water sector. American Water Works Association. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013

Resumen

La ciberseguridad es un desafío complejo que requiere un enfoque interdisciplinario basado en el riesgo, involucrando a los líderes de negocios de una organización, así como a sus técnicos y asesores legales. Un programa de ciberseguridad sólido y probado es fundamental para proteger la salud y la seguridad públicas, prevenir interrupciones en el servicio y salvaguardar los datos personales y personales de clientes y empleados. Las organizaciones, por sí mismas y con personal técnico y expertos legales, deben desarrollar un plan y brindar una atención suficientemente

rigurosa a la ciberseguridad, tomar medidas razonables para prevenir, detectar y responder a incidentes cibernéticos.

Abstract

Cybersecurity is a complex challenge that requires an interdisciplinary approach based on risk, involving the business leaders of an organization, as well as its technical and legal advisors. A robust and proven cybersecurity program is critical to protecting public health and safety, preventing service interruptions, and safeguarding customer and employee personal and personal data. Organizations, by themselves and with technical staff and legal experts, must develop a plan and provide sufficiently rigorous attention to cybersecurity, take reasonable steps to prevent, detect and respond to cyber incidents.

6. Kash Srinivasan Group. (2016). Cyber security assessment and recommended approach. State of Delaware drinking water systems: Final report. https://dhss.delaware.gov/dhss/dph/hsp/files/dwsrfcr.pdf

Resumen

Los sistemas SCADA varían en complejidad, como lo indica la muestra de cuatro empresas de servicios públicos evaluadas en este estudio.

La American Water Works Association (AWWA) ha desarrollado una herramienta de seguridad cibernética que ofrece un enfoque en capas para que las empresas de servicios públicos aborden las ciberamenazas. La División de Salud Pública Programa de Fondos de Préstamos Estatales para Agua Potable inició acciones para investigar la ciberseguridad en los servicios de agua del Estado. Este estudio recomienda que la división adopte un conjunto común de controles aplicables a todas las empresas de servicios públicos con sistemas SCADA en Delaware.

Abstract

SCADA systems vary in complexity, as indicated by the sample of four utilities evaluated in this study. The American Water Works Association (AWWA) has developed a cyber security tool that offers a layered approach for utilities to address cyber threats. The Division of Public Health State Drinking Water Loan Funds Program initiated actions to investigate cybersecurity in the State's water services. This study recommends that the division adopt a common set of controls applicable to all utilities with SCADA systems in Delaware**.**

7. Hassanzadeha, A., Rasekhb, A. Galellic, S. Aghashahid, M., Taorminae, R., Ostfeldf, Banksg, M. K. (2020). A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering*, 146, 1-15. https://search.ebscohost.com/login.aspx?direct=true&db=edsoai&AN=edsoai.on1228388339&lang=es&site=eds-live&scope=site.

Resumen

Este estudio presenta una revisión crítica de los incidentes de seguridad cibernética divulgados, documentados y maliciosos en el sector del agua para informar los esfuerzos de protección contra las amenazas de seguridad cibernética. La revisión se presenta dentro de un contexto técnico de arquitecturas de sistemas de control industrial, modelos de ataque-defensa y soluciones de seguridad. Se seleccionaron y analizaron quince incidentes a través de una estrategia de búsqueda que incluyó una variedad de fuentes de información pública que van desde informes de investigaciones federales hasta artículos científicos. Para cada incidente individual, se compilaron y describieron la situación, la respuesta, la remediación y las lecciones aprendidas. Los hallazgos de esta revisión indican un aumento en la frecuencia, diversidad y complejidad de las ciberamenazas al sector del agua. Aunque se detectó la aparición de nuevas amenazas, como ransomware o cryptojacking, también fue evidente la recurrencia de vulnerabilidades y amenazas similares, como amenazas internas, lo que enfatiza la necesidad de un enfoque adaptativo, cooperativo e integral para la ciberdefensa del agua.

Abstract

This study presents a critical review of disclosed, documented, and malicious cybersecurity incidents in the water sector to inform safeguarding efforts against cybersecurity threats. The review is presented within a technical context of industrial control system architectures, attack-defense models, and security solutions. Fifteen incidents were selected and analyzed through a search strategy that included a variety of public information sources ranging from federal investigation reports to scientific papers. For each individual incident, the situation, response, remediation, and lessons learned were compiled and described. The findings of this review indicate an increase in the frequency, diversity, and complexity of cyberthreats to the water sector. Although the emergence of new threats, such as ransomware or cryptojacking, was found, a recurrence of similar vulnerabilities and threats, such as insider threats, was also evident, emphasizing the need for an adaptive, cooperative, and comprehensive approach to water cyberdefense.

8. Li D, Paynabar K, Gebraeel N. A. (2021). Degradation-based detection framework against covert cyberattacks on SCADA systems. *IISE Transactions*.*53(*7),812-829. https://www.tandfonline.com/doi/full/10.1080/24725854.2020.1802537

Resumen

Los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA) se utilizan comúnmente en infraestructuras críticas. Sin embargo, estos sistemas suelen ser vulnerables a los ciberataques. Entre los diferentes tipos de ciberataques, el ataque encubierto es uno de los más difíciles de detectar, es indetectable cuando el sistema funciona en condiciones normales. En este artículo, se desarrolla un marco de detección basado en datos que utiliza el proceso de degradación del sistema para detectar ataques encubiertos. Se obtienen características matemáticas de los procesos de degradación bajo ataques encubiertos que se utilizan para desarrollar un método de prueba de relación de probabilidad secuencial para la detección de ataques. Se verifica la metodología a través de un extenso estudio numérico y un estudio de caso sobre una configuración de maquinaria rotativa. El resultado muestra que la metodología ayuda a detectar ataques encubiertos dentro de un tiempo de demora razonable y es aplicable en entornos del mundo real.

Abstract

Supervisory Control and Data Acquisition (SCADA) Systems are commonly used in critical infrastructures. However, these systems are often vulnerable to cyber-attacks. Among the different types of cyber-attacks, the covert attack is one of the most difficult to detect, it is undetectable when the system works under normal conditions. In this article, a data-driven detection framework is developed that uses the system degradation process to detect covert attacks. Mathematical characteristics of degradation processes under covert attacks are obtained and used to develop a sequential likelihood ratio test method for attack detection. The methodology is verified through an extensive numerical study and a case study on a rotating machinery configuration. The result shows that the methodology helps to detect covert attacks within a reasonable delay time and is applicable in real world environments.

9. Tuptuk, N., Peter, H., Watson, J., and Hailes, S. (2021). "A Systematic Review of the State of Cyber-Security in Water Systems". *Water, 13(*81*)*,1-29. https://www.mdpi.com/2073-4441/13/1/81.

Resumen

En este trabajo, se analiza el estado de la investigación en ciberseguridad que se centra en mejorar la seguridad del suministro de agua y sistemas de recolección y tratamiento de aguas residuales que forman parte de la infraestructura crítica nacional. Se consideran las estadísticas de publicación de la investigación en esta área, los aspectos de seguridad que se abordan
y el trabajo futuro requerido para lograr una mejor seguridad cibernética para los sistemas de agua.

Abstract

In this paper, the state of cybersecurity research that focuses on improving the security of water supply and wastewater collection and treatment systems that are part of the national critical infrastructure is analyzed. The publication statistics of the research in this area are considered, the security aspects that are addressed, and the future work required to achieve better cyber security for water systems.

10. Water Information Sharing and Analysis Center. (2019). 15 Cybersecurity fundamentals for water and Wastewater utilities: best practices reduce exploitable weaknesses and attacks. Washington: Water SAC. https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

Resumen

Los servicios públicos de agua y aguas residuales brindan servicios vitales críticos para sus comunidades y sus regiones. El agua segura y el agua limpia son esenciales para la salud pública, la protección de los ecosistemas y la fortaleza económica. Apoyar estas funciones importantes requieren de información segura tecnología (TI) y tecnología operativa (OT). En este documento se plantean 15 fundamentos de ciberseguridad para agua y servicios públicos de aguas residuales útiles para informar sobre los planes de respuesta de emergencia, abordar las opciones de mitigación y resiliencia.

Abstract

Water and wastewater utilities provide vital services critical to their communities and their regions. Safe water and clean water are essential for public health, ecosystem protection, and economic strength. Supporting these important functions requires secure information technology (IT) and operational technology (OT). This document outlines 15 cybersecurity fundamentals for water and wastewater utilities useful for informing emergency response plans and addressing mitigation and resiliency options.

11. West Yost Associates. (2019). water sector cybersecurity risk management guidance. American Water Works Association. https://www.awwa.org/Portals/0/AWWA/ETS/Resources/AWWACybersecurityGuidance2019.pdf?ver=2019-09-09-111949-960

Resumen

En respuesta a la amenaza general a la infraestructura crítica, se elaboró una amplia gama de normas y directrices para ayudar a las organizaciones a implementar controles de seguridad para mitigar el riesgo de ataques cibernéticos.

El objetivo inicial de esta guía de AWWA es proporcionar a los propietarios/operadores de servicios públicos del sector del agua una herramienta de evaluación y curso de acción recomendado para reducir las vulnerabilidades a los ataques cibernéticos según lo recomendado en ANSI/AWWA G430: Prácticas de seguridad para operaciones y administración y EO 13636. La actualización de la herramienta de orientación y evaluación de AWWA se desarrolló para ayudar a los sistemas de agua comunitarios; es decir, servicios públicos, en cumplimiento con la sección 2013 de la Ley de infraestructura de agua de Estados Unidos (AWIA) del 2018.

Abstract

In response to the general threat to critical infrastructure, a wide range of standards and guidelines have been developed to help organizations implement security controls to mitigate the risk of cyber-attacks. The initial goal of this AWWA guide is to provide utility owners/operators in the water sector with an Enhanced Course of Action and Assessment Tool to reduce vulnerabilities to cyber-attacks as enhanced by ANSI/AWWA G430: Security Practices for Operations and Management and EO 13636. The AWWA Assessment and Guidance Tool update is enhanced to help community water systems; that is, utilities, in compliance with section 2013 of the United States Water Infrastructure Act (AWIA) of 2018.

7. ANEXOS

Luis Fernando Ulate Vargas

Director General Ingeniería en Tecnologías

Experiencia

2022 Actualidad

Instituto Costarricense de Acueductos y Alcantarillados

- Encargado del Área de Administración de Infraestructura y Telecomunicaciones.
- Quince años de experiencia en Gerencia en Seguridad de Información y Administración Tecnológica.
- Enlace con la Red Nacional de Ciberseguridad con el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

Educación

Universidad Central de Costa Rica
Ingeniería Informática

Contacto

Email: lulate@aya.go.cr
Telef. : 2242-5588
Sitio web: www.aya.go.cr
San José, Costa Rica

Entrevista

- ¿Cuáles son tres impactos negativos principales cuando se materializa un riesgo en ciberseguridad en una empresa como AyA?

  La respuesta a esta pregunta va muy relacionada al área de impacto del evento, puede ser tan bajo como que se robaron una máquina o exfiltración de datos institucionales, la pérdida de información institucional de sistemas o en casos la suspensión total en los servicios que la institución estamos definidos como de infraestructura crítica nacional.

- ¿Existe una estrategia o política en materia de ciberseguridad para los sistemas que administra AyA? (Si es así, indicar la documentación).

  Existen las políticas de seguridad de la información que están publicadas en la intranet, cabe anotar que están en revisión con la entrada en vigencia del margo de gestión de TI emitido por MICITT, además de los diferentes decretos que el MICITT, por medio de la dirección de Gobernanza Digital ha emitido en esta materia y se encuentran disponibles en el sitio de MICITT.

- ¿Cuáles son los componentes principales de una estrategia de ciberseguridad para los sistemas de una institución como AyA?

  Dentro de los componentes podríamos mencionar en términos generales, la integridad, disponibilidad, confidencialidad de la información y servicios tecnológicos.

- Si la institución ha experimentado la materialización de un riesgo en ciberseguridad ¿Cuáles han sido las medidas de mitigación remediales implementadas?

  Sí, fortalecimiento de los esquemas de respaldo y recuperación, mejora y robustecimiento de accesos y privilegios de servicios externos.

- A futuro ¿Cómo se puede robustecer la ciberseguridad en la institución?

  Se debe seguir invirtiendo en esta temática, principalmente en un plan de capacitación a los usuarios, se debe definir un área específica que gestione todo lo que tiene que ver con la temática de la seguridad de la información.

Referencia

Ulate, L. (26 de octubre 2022). Ciberseguridad en el AyA. Correo electrónico.