Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín Informativo

Veintiuno

Marzo: Desafíos de seguridad informática orientados a ICS.

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

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

Medio de divulgación: Correo Electrónico, Sitio Web

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

Número Veintiuno
Marzo 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

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 Cibercosmonautas y Ceros y Unos, y Cibercosmonautas adscritos al Grupo de Byte InDesign

Responsable de la Edición
RODRIGO IGNACIO MENDEZ KEKHAN

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 21

Marzo de 2024

Desafíos de seguridad informática orientados a ICS

Autores:

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

Rodrigo Ignacio Méndez Kekhán
https://orcid.org/0009-0003-8308-6128

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 en Colombia enfrenta desafíos significativos debido a la constante evolución de las amenazas cibernéticas, la falta de conciencia y educación en seguridad digital, la presencia de infraestructuras tecnológicas desprotegidas y la escasez de profesionales en el campo. Para abordar estos desafíos, es crucial implementar soluciones prácticas, como campañas de concientización y educación, medidas de prevención tecnológicas, colaboración público-privada y la inversión en formación y desarrollo de talentos en ciberseguridad. Estas acciones no solo pueden reducir los riesgos de ciberataques, sino que también pueden preparar a Colombia para enfrentar los desafíos futuros en el ámbito de la seguridad digital.

Los desafíos y soluciones en ciberseguridad en Colombia en un mundo digitalizado. Se enfoca en la importancia de proteger la información y los sistemas de ataques cibernéticos, así como en la necesidad de desarrollar estrategias efectivas para enfrentar estas amenazas. Se destaca la importancia de la colaboración entre el gobierno, el sector privado y la sociedad en general para fortalecer la ciberseguridad en el país.

Desarrollo

Los desafíos de la ciberseguridad en Colombia

El jefe de Estado colombiano se refirió al ataque que afecta a más de 50 entidades estatales y empresas privadas. "La ciudadanía debe tener seguridad en torno al uso cada vez más generalizado de este tipo de dispositivos que utilizan algoritmos y plataformas de software".

El presidente de Colombia, Gustavo Petro, ha denunciado "guerras entre empresas privadas" y la nueva independencia del mercado global como causas de un ciberataque que ha afectado a más de cincuenta organizaciones y empresas estatales. Según él, los piratas informáticos atacaron una empresa con la que tenían contratos múltiples organizaciones colombianas. El ataque no sólo afectó a Colombia, sino también a otros tres países e instituciones nacionales tanto gubernamentales como privadas. Según Petro, la empresa atacada violó sus contratos y mostró debilidad al no contar con protecciones de ciberseguridad para sus propias plataformas y algoritmos. Esta circunstancia pone de relieve la necesidad de que las empresas colombianas refuercen sus defensas de ciberseguridad.

Para salvaguardar la nación y la información privada de sus residentes, el Gobierno del cambio sugirió crear una agencia de ciberseguridad en el Plan Nacional de Desarrollo. Los congresistas, sin embargo, atacaron este plan, diciendo que dañaría la reputación del país. La organización existe para salvaguardar a la población en general contra el uso generalizado de plataformas de software y algoritmos en dispositivos. Los ataques los llevan a cabo profesionales expertos en gestión de programación, que pueden ser particulares u organizaciones. Es todo un reto contrarrestar estos ataques debido al bajo nivel de competitividad en el entorno altamente tecnológico, donde pueden publicarse, irradiarse y utilizarse para actividades ilegales. La seguridad del público en torno a estos dispositivos debe estar garantizada por el gobierno.[1]

Portales y páginas del Ministerio de Salud, la Superintendencia de Salud y el Consejo Superior de la Judicatura, entre las afectadas por ataque cibernético a su proveedor de servicios.

Un ciberataque que impactó múltiples operaciones digitales en Colombia fue lanzado contra la firma de servicios de tecnología y transferencia de datos IFX Networks.

Para determinar la magnitud del daño y atender los efectos causados por el incidente, que impactó a varias entidades, el Gobierno del Cambio instaló el Puesto de Mando Unificado Cibernético (PMU Cyber).[2]

[1] https://petro.presidencia.gov.co/prensa/Paginas/Colombia-victima-de-ataque-cibernetico-por-guerras-entre-empresas-privadas-a-escala-mundial-dijo-el-presidente-230918.aspx

[2] https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/278831:Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER

Luis Gabriel Castellanos, Country Manager de la compañía, informó al PMU Ciberseguridad Nacional, presidido por la Dirección de Transformación Digital de la Presidencia de la República, sobre las medidas que se están tomando para restablecer el servicio.

Fuente: https://www.freepik.es/vector-gratis/concepto-actividad-hacker_8269019.htm#query=ataque%20cibernetico&position=6&from_view=search&track=ais

Stuxnet: Gusano informático de 2010 que causó daños sustanciales al atacar deliberadamente los sistemas de control industrial, incluidos los de los reactores nucleares.

BlackEnergy: Malware utilizado en muchos ataques, como el ciberataque de 2015 en Ucrania que dejó sin electricidad a miles de personas.

TRITON/TRISIS: Malware destinado a violar los sistemas de seguridad de plantas industriales, causando potencialmente la interrupción de operaciones vitales.

Shamoon: Malware que se ha utilizado para borrar datos de sistemas comprometidos en muchos ataques a empresas petroleras.

Havex: Malware que se ha utilizado para recopilar datos sobre sistemas de control industrial como preparación para posibles asaltos en el futuro.

"Desde el PMU Ciber, para determinar el verdadero impacto en Colombia, estamos examinando qué otros organismos gubernamentales podrían haberse visto afectados. La brecha ocurrió contra IFX Networks, un proveedor de servicios, no contra organizaciones estatales, como debe quedar claro, según se le dijo al equipo asesor de Transformación Digital.

Desde el 12 de septiembre, IFX Networks está sufriendo un ataque externo de ciberseguridad del tipo ransomware, también conocido como "secuestro" digital de información y aplicaciones, que afecta a unas 762 empresas en toda América Latina.

Según el proveedor IFX, el equipo técnico está trabajando para restablecer el servicio. La mesa del PMU ha solicitado que el sector salud reciba atención prioritaria para aminorar el impacto que este incidente ha tenido en la atención digital, trámites y demás, así como otras entidades que también necesitan apoyo para seguir operando.

La empresa señaló que, con base en sus primeros pasos, ningún dato de la plataforma ha sido impactado, y prevén conocer en las próximas horas cuántos activos de información a nivel nacional están impactados.

La fiscalía general de la Nación autorizó el desplazamiento de un equipo especializado a las oficinas de IFX en Colombia, con el fin de recibir la denuncia y la aportación de pruebas.

La Ciber PMU permanecerá abierta e informará sobre el estado del restablecimiento de las operaciones en el país.[3]

[3] https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/278831:Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER

El reciente incidente es una prueba más de lo grave que es la situación, dada nuestra creciente dependencia de los ordenadores para casi todos los aspectos de la vida cotidiana, así como la creciente amenaza de la delincuencia que afecta tanto a la esfera pública como a la privada. Así pues, el principal reto digital al que se enfrenta la nación es esta amenaza.

Debilidad institucional

Enfrentamos el cibercrimen sin contar con instituciones fuertes, organizadas y efectivas para hacer frente a estos grupos criminales, tal como ocurre en el mundo real. Aunque Colombia cuenta con varios documentos CONPES y acciones administrativas para mejorar la ciberseguridad, el país carece de un norte estratégico que intente detener estos delitos y, en caso de que ocurran, enfrentarlos de manera rápida y efectiva.
La principal lección del ataque es la urgencia que tienen las entidades estatales de desarrollar una política nacional de ciberseguridad exhaustiva, tecnológicamente avanzada y adecuadamente coordinada.[4]

Oportunidades y desafíos: Investigando la ciberseguridad en América Latina

América Latina no está exenta de la tendencia mundial de que la ciberseguridad se convierta en una preocupación estratégica. El más reciente estudio de La República señala que los ciberataques han aumentado en un 65%, siendo los bancos y las industrias los blancos más frecuentes.

Brasil lidera con un 50% este escenario, seguido de México con un 23%, Colombia con un 8% y Perú con un 8%. Entre 2022 y 2023 se reportaron más de 1600 ciberataques por segundo, lo que resalta la necesidad crítica de fortalecer las defensas contra las amenazas digitales, particularmente en el sector financiero, donde la sensibilidad de la información es particularmente alta.

Es fundamental comprender que la ciberseguridad es tanto un mandato gubernamental como un deber de las empresas.

Los gobiernos deben duplicar la cantidad de dinero destinada a la ciberseguridad y realizar análisis de riesgos corporativos con más frecuencia. Los esfuerzos gubernamentales que fomentan una mentalidad consciente de la seguridad en la zona deben respaldar la necesidad de proteger los datos.[5]

Mejora de la ciberseguridad en las empresas

La gestión de datos, un componente crucial de la ciberseguridad muestra que el 40% de las empresas inician este proceso a mano. A pesar de estar muy extendido, este comportamiento tiene graves consecuencias para la productividad y la seguridad de los datos. Resulta evidente que el uso de soluciones automatizadas es esencial.

La complejidad de la situación se pone de manifiesto en un estudio realizado entre profesionales de la seguridad de la información de los sectores del comercio minorista, los seguros, la banca y la tecnología. Más de la mitad de estos expertos destacan la necesidad urgente de realizar grandes inversiones. Los ámbitos de Riesgo y Auditoría articulan ciertos

[4] https://razonpublica.com/los-desafios-la-ciberseguridad-colombia/

[5] https://www.kriptos.io/es-post/ciberseguridad-en-america-latina-gestion-2024?utm_source=google&utm_medium=paid&utm_campaign=SiSr_Kriptos_Enero_SEM&utm_content=SEM&gad_source=1&gclid=CjwKCAiArfauBhApEiwAeoB7qD2PMCl0XgT0GD2-q3k5KiYUv7jOaIJi6i2sYVzFgLs2jq_xLELGUhoCkX4QAvD_BwE

imperativos, subrayando la importancia de coordinar deliberadamente los recursos financieros con los requisitos de ciberseguridad.

Nuestra principal sugerencia es que los equipos de ciberseguridad elaboren matrices de riesgos. Estas matrices deberían tener en cuenta las implicaciones financieras, permitiendo una comparación entre la inversión necesaria y los posibles beneficios. Una tabla que clasifique los métodos de gestión en función de la posibilidad de sanciones, violaciones de la seguridad y daños a la reputación puede ayudar a orientar la toma de decisiones.

El 82% de los encuestados declararon estar muy centrados en la explotación de los PC Windows y los servidores de archivos Windows. diversas conclusiones ponen de manifiesto la necesidad de aplicar un enfoque específico a las hojas de ruta de las aplicaciones para garantizar una cobertura completa y eficaz de los distintos entornos.

Importancia de la ciberseguridad en el sector financiero

La ciberseguridad se enfrenta a numerosos obstáculos, entre ellos la falta de concienciación y educación, lo que aumenta los problemas de ciberseguridad en las empresas. Una encuesta de Kaspersky muestra un aumento del 6% en los incidentes cibernéticos contra las empresas. Además, hay una falta de inversión en tecnologías de ciberseguridad, con América Latina invirtiendo menos que otras partes del mundo y dos tercios de los países latinoamericanos carecen de leyes nacionales de ciberseguridad, lo que indica una deficiencia en las normas de ciberseguridad.

Los retos actuales de América Latina en materia de ciberseguridad

Los residentes, los datos de las empresas y los sistemas de la región están en peligro debido a las ciberamenazas, lo que hace necesaria la colaboración entre gobiernos, empresas y ONG para la investigación, el desarrollo tecnológico, la formación en ciberseguridad, las campañas de concienciación y una legislación más estricta.[6]

Ciberdelitos como el ransomware, el phishing, el hacktivismo y el deepfake son cada vez más frecuentes, lo que requiere soluciones defensivas más sofisticadas. Estos ataques no solo van dirigidos a organismos públicos, sino también a usuarios particulares, lo que plantea la cuestión de los recursos disponibles para combatir estas amenazas.

El rápido avance de la tecnología, incluyendo el aprendizaje automático, el análisis de comportamiento y la inteligencia artificial, ha mejorado significativamente la protección contra la ciberdelincuencia. Estos avances ofrecen soluciones rápidas y flexibles, mejorando las defensas y protegiendo la información y las infraestructuras críticas, según Ingrid Mora, gerente general de la empresa de ciberseguridad de Costa Rica.

En este sentido, los expertos identifican tres tecnologías cruciales que serán importantes en la batalla de 2024 contra la ciberdelincuencia:

- **La inteligencia artificial (IA)**: es una tecnología de vanguardia en rápido desarrollo que puede identificar instantáneamente anomalías y analizar tendencias.

[6] https://www.kriptos.io/es-post/ciberseguridad-en-america-latina-gestion-2024?utm_source=google&utm_medium=paid&utm_campaign=SiSr_Kriptos_Enero_SEM&utm_content=SEM&gad_source=1&gclid=CjwKCAiArfauBhApEiwAeoB7qD2PMCl0XgT0GD2-q3k5KiYUv7jOaIJi6i2sYVzFgLs2jq_xLELGUhoCkX4QAvD_BwE

- **Aprendizaje autónomo**: esta tecnología maximiza el aprendizaje automático para adaptar y mejorar las reacciones defensivas en cooperación con la IA.
- **La tecnología de nube**: en particular la nube soberana, ofrece a las empresas una mayor fiabilidad para socios y consumidores, al tiempo que mitiga los riesgos de sabotaje, espionaje y filtraciones.

Las ciberamenazas evolucionan constantemente, lo que exige una mayor concienciación y educación. Dotar a las personas y a las organizaciones de conocimientos sobre prácticas seguras en línea es crucial para una defensa sólida. La mitigación de la ciberdelincuencia requiere la colaboración entre todas las partes interesadas, la aplicación de medidas preventivas y el fomento de la confianza en la era digital. Este enfoque colaborativo es esencial para construir una ciberseguridad sólida.[7]

La realidad digital ha impactado significativamente a la sociedad colombiana, con empresas implementando proyectos y transformando las relaciones con los clientes. El sector salud también ha tenido que adaptarse a esta nueva realidad, siendo necesario el desarrollo y consolidación de una cultura organizacional de seguridad de la información. Las infraestructuras cibernéticas críticas deben comprender y garantizar las relaciones con terceros confiables para aumentar la resiliencia contra adversarios que pueden pasar desapercibidos durante las interacciones remotas y la integración de las soluciones disponibles.

El auge de la interacción digital ha alterado la relación del Estado con los ciudadanos, permitiéndoles participar en una sociedad democrática donde diferentes actores pueden expresar y generar opiniones. Sin embargo, este entorno genera inestabilidad e incertidumbre debido a noticias falsas, información engañosa y desinformación. Las plataformas de redes sociales se han convertido en escenarios naturales de controversias y manipulación, influyendo positiva o negativamente en la población. Los recientes movimientos, controversias, propaganda política e inestabilidades en Internet han creado un ambiente de tensión, reforzando la polarización pública, aumentando el descontento social y terminando con una sensación de pérdida de gobernabilidad, que favorece la búsqueda de soluciones dentro de la Constitución y la ley.[8]

Tendencias a nivel tecnológico

Los rápidos avances tecnológicos, como los chat bots, los asistentes digitales y la robótica, están transformando la vida humana y digital. Sin embargo, también presentan desafíos e incertidumbre en la dinámica del ciberespacio.[9]

Tendencias a nivel legal.

Comprender la responsabilidad y el cumplimiento en el ciberespacio es crucial para los individuos, las corporaciones, los nacionales y a nivel mundial. Las iniciativas de regulación y control legal se están acelerando debido a la creciente interacción humana en el nuevo dominio cibernético, creando áreas grises para agresores no estatales u otros estados.[10]

[7] https://forbescentroamerica.com/2023/12/27/tendencias-y-nuevas-tecnologias-sobre-ciberseguridad-para-el-2024
[8] https://www.redalyc.org/journal/4762/476274912004/html/
[9] https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html
[10] https://gsis.scholasticahq.com/api/v1/articles/27849-the-hacker-and-the-state-cyber-attacks-and-the-new-normal-of-geopolitics.pdf

El riesgo cibernético es una realidad que emerge rápidamente.

El ciberriesgo es una realidad sistémica de las organizaciones que requiere una perspectiva relacional para comprender la forma de pensar y concebir el mundo. Establece un reto cognitivo y social, demandando romper con paradigmas disciplinares para encontrar respuestas en escenarios cada vez más inestables e inciertos, ya que se configura como una apuesta relacional entre objetos físicos y realidades sociales.
El ciber riesgo desarrolla características emergentes, necesidades de una vista interdisciplinar para comprender sus movimientos y establecer patrones de interés para las empresas, y se detallan siete claves.[11]

- La incertidumbre y la dificultad de valorar la frecuencia y potencial de impacto de un sistema, enfatizando la importancia de comprender la dinámica y relaciones con el entorno.
- Tanto los analistas como los ejecutivos no están de acuerdo sobre cómo abordar o reconocer las incertidumbres en un entorno modificado digitalmente.
- La relevancia indefinida se refiere a la falta de orientación o información sobre situaciones propuestas, que pueden ser futuristas o menos creativas.
- La comunicación es difícil debido a la baja comprensión y la falta de atención, lo que lleva a puntos ocultos dentro de la organización que se pasan por alto dentro de la dinámica empresarial.
- Enfatizar el ciber riesgo requiere abordar las diferentes formas de ver la realidad, encontrar sus alcances e impactos, no es el ejercicio de un área.
- Densidad digital es un tejido que esencial para la realidad, ya que se manifiestan en relación con otros riesgos sistémicos.
- Tendencias imperceptibles son revelaciones de señales y eventos en el entorno, obtenidos a través de la identificación de realidades relevantes para el negocio.

El ciber riesgo es un riesgo emergente que necesario reinventar la gestión de riesgos desde el pensamiento sistémico, incorporando la dinámica de las posibilidades y las probabilidades asociadas con los riesgos conocidos, y movilizar los esfuerzos en el tratamiento de los riesgos.[12]

En una organización situada en un lugar con conflicto de intereses por activos digitales estratégicos, se requiere el marco general de prácticas asociadas con los riesgos informáticos para introducir capacidades críticas.

Los estándares de seguridad tradicionales tienen como objetivo determinar ataques potenciales, pero el riesgo cibernético requiere considerar las acciones, recursos, posibilidades, capacidades e impactos de los adversarios. Para abordar las amenazas digitales, las empresas deben adoptar una visión estratégica, considerando comportamientos y acciones coordinadas para retrasar, interrumpir, contener o anticipar los efectos de la ciber operación deliberada.

[11] https://sistemas.acis.org.co/index.php/sistemas/article/download/13/11
[12] https://www.researchgate.net/publication/333878946_Ciberriesgo_Aprendizaje_de_un_riesgo_sistemico_emergente_y_disruptivo

Cómo se vive todo esto desde una universidad

Los profesionales analizan constantemente las deficiencias e identifican áreas de mejora. Es crucial que las instituciones educativas comprendan los riesgos diarios y se protejan. Esto implica incorporar expertos en ciberseguridad con habilidades analíticas, inteligencia, conocimientos geopolíticos e info-políticos y colaboración gubernamental. El análisis de riesgos cibernéticos se basa en la seguridad de la información y una perspectiva mecanicista, centrándose en amenazas conocidas, latentes y emergentes.

Luis Zambrano, director del CSIRT (Equipo de Respuesta ante Emergencias Informáticas) de la Universidad Nacional Abierta y a Distancia (UNAD) contó detalles de cómo trabaja la entidad ante las amenazas.

La metodología utilizada es el marco NIST, una referencia del gobierno de EE. UU., para identificar amenazas a la ciberseguridad y su naturaleza, lo que permite detectar posibles crisis y tomar medidas adecuadas, como la implementación de bloqueos.

Además de los ataques de ransomware y phishing, Zambrano afirma que las instituciones también enfrentan otras amenazas, incluidas las inyecciones de comandos, que implican aprovechar fallas de seguridad en los sistemas para obtener datos.

La educación incentiva a los ciberdelincuentes a obtener datos de los estudiantes y brindar servicios como la modificación de calificaciones. Sin embargo, el problema está más extendido ya que las instituciones están creando sistemas relacionados con la investigación, el desarrollo, las patentes y los derechos de autor. autor que puede ser lo suficientemente impresionante como para ser adquirido y posteriormente vendido", afirma.

Esto amplía las razones por las que las universidades son un objetivo muy deseable para los ciberdelincuentes, ya que ofrecen una amplia gama de opciones. Sirven como puerta de entrada para amenazas más graves, brindan alternativas para el espionaje y los ataques políticos y, por último, brindan a los usuarios acceso a datos básicos de estudiantes y administradores que resultan atractivos para otros en la web oscura. Numerosas preocupaciones para las organizaciones que participan en la creación de la sociedad y poseen datos sensibles.[13]

Disruptivo digital es un efecto que altera expectativas y comportamientos en una cultura, mercado, industria o proceso. La organización debe monitorear el ambiente, detectar anomalías y contradicciones que advierten patrones no conocidos, y crear acciones de defensa activas y pasivas para evitar distraer e interrumpir sus acciones. Esto requiere desarrollar una mentalidad de experimentación permanente, equipos calificados en el riesgo cibernético, y buscar puntos de vista distintos para obtener una ventaja estratégica competitiva.[14]

[13] https://www.infobae.com/tecno/2023/10/30/por-que-el-sector-educativo-se-convirtio-en-el-blanco-favorito-de-los-ciberdelincuentes/
[14] https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Escasez de Profesionales en Ciberseguridad

La escasez de profesionales en ciberseguridad en Colombia dificulta una defensa sólida contra las amenazas cibernéticas debido a que la alta demanda supera la oferta.

Infraestructuras Tecnológicas Desprotegidas

Las empresas e instituciones a menudo luchan con infraestructuras tecnológicas obsoletas y desprotegidas, lo que genera vulnerabilidades debido a la falta de actualizaciones de software y a una inversión insuficiente en tecnologías de seguridad de próxima generación.

Amenazas Cibernéticas en Constante Evolución

Colombia se enfrenta a una multitud de amenazas cibernéticas, incluidos ransomware, phishing y fraude en línea, que evolucionan constantemente y representan un desafío importante para su seguridad digital.

Brecha de concientización y educación

Persisten las brechas de concienciación y educación sobre ciberseguridad, lo que aumenta la vulnerabilidad a ataques como el phishing y la ingeniería social, ya que muchos usuarios y empleados carecen de conocimientos integrales sobre prácticas seguras en línea.[15]

[15] https://www.gremioaces.com/ciberseguridad-en-colombia-desafios-y-soluciones/

Conclusiones

La ciberseguridad en infraestructuras críticas es un desafío multifacético que requiere una acción concertada a nivel global y local. A medida que las tecnologías digitales continúan transformando los entornos industriales, es fundamental adoptar enfoques proactivos para proteger sistemas de control industrial contra amenazas cibernéticas en evolución.

La seguridad informática de las ICS es un tema complejo y desafiante. Es importante que los gobiernos, las empresas y los individuos trabajen juntos para proteger estas infraestructuras críticas de ataques cibernéticos.

la seguridad de las ICS es un desafío multidimensional que requiere una respuesta coordinada a nivel global. Solo mediante la colaboración entre gobiernos, empresas y la sociedad en su conjunto podremos mitigar los riesgos asociados con los ataques informáticos a estas infraestructuras vitales para el funcionamiento de nuestras sociedades modernas.

Canales de comunicación

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


Correo: csirt@unad.edu.co


Twitter: @csirtunad


Página web: https://csirt.unad.edu.co

Referencias bibliográficas

Cano M., J. (2019). *Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo.* 63-73. https://doi.org/10.29236/sistemas.n151a5

Ciberseguridad en América Latina para Iniciar la Gestión en 2024. (s. f.). Recuperado 27 de febrero de 2024, de https://www.kriptos.io/es-post/ciberseguridad-en-america-latina-gestion-2024

Ciberseguridad en Colombia: Desafíos y Soluciones – ACES. (2024, enero 25). https://www.gremioaces.com/ciberseguridad-en-colombia-desafios-y-soluciones/

Colombia víctima de ataque cibernético por guerras entre empresas privadas a escala mundial, dijo el presidente Petro en declaraciones Nueva York. (s. f.). Presidencia de la República. Recuperado 27 de febrero de 2024, de https://petro.presidencia.gov.co/prensa/Paginas/Colombia-victima-de-ataque-cibernetico-por-guerras-entre-empresas-privadas-a-escala-mundial-dijo-el-presidente-230918

Gobierno Nacional atiende ataque cibernético que afecta a varias entidades e instala PMU CIBER - Gobierno Nacional atiende ataque cibernético que afecta a varias entidades e instala PMU CIBER. (s. f.). MINTIC Colombia. Recuperado 27 de febrero de 2024, de http://www.mintic.gov.co/portal/715/w3-article-278831.html

Https://www.gremioaces.com/ciberseguridad-en-colombia-desafios-y-soluciones/. (s. f.). Recuperado 27 de febrero de 2024, de https://www.gremioaces.com/ciberseguridad-en-colombia-desafios-y-soluciones/

Lewis, A. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. *Global Security and Intelligence Studies*, *5*(2). https://doi.org/10.18278/gsis.5.2.11

Los desafíos de la ciberseguridad en Colombia | Razón Pública 2023. (2023, septiembre 24). *Razón Pública*. https://razonpublica.com/los-desafios-la-ciberseguridad-colombia/

Martínez, J. J. C. (2022). Prospectiva de ciberseguridad nacional para Colombia a 2030. *Revista Científica General José María Córdova*, *20*(40), 814-832.

OEA. (n.d.). *DESAFÍOS DEL RIESGO CIBERNÉTICO EN EL SECTOR FINANCIERO PARA COLOMBIA Y AMÉRICA LATINA*.

Ríos, P. J. (2023, octubre 30). *Especial Tecno | Por qué el sector educativo se convirtió en el blanco favorito de los ciberdelincuentes*. infobae. https://www.infobae.com/tecno/2023/10/30/por-que-el-sector-educativo-se-convirtio-en-el-blanco-favorito-de-los-ciberdelincuentes/

Tendencias y nuevas tecnologías sobre ciberseguridad para el 2024. (s. f.). Recuperado 27 de febrero de 2024, de https://forbescentroamerica.com/2023/12/27/tendencias-y-nuevas-tecnologias-sobre-ciberseguridad-para-el-2024

The Future of Cyber Survey. (s. f.). Deloitte United States. Recuperado 27 de febrero de 2024, de https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html