Universidad Empresarial Siglo 21

Análisis del accionar gubernamental en la prevención del acceso no autorizado a sistemas informáticos en la Provincia de Córdoba

Trabajo Final de Grado

Manuscrito Científico

Licenciatura en Criminología y Seguridad

autora: Cora, Gabriela Nerea

Legajo: VCYS00278

Autora: Alberoni, Antonella Sol

Fecha: 17 de Noviembre 2024

ÍNDICE

RESUMEN

Este trabajo analiza el accionar del gobierno de Córdoba en la prevención del acceso no autorizado a sistemas informáticos, un fenómeno creciente en el contexto del cibercrimen, particularmente el hacking, debido al uso intensivo de tecnologías en los sectores público y privado. El acceso no autorizado a sistemas informáticos puede tener consecuencias graves para la seguridad de la información, la economía y la estabilidad social. La investigación examina las estrategias implementadas por el gobierno provincial para enfrentar esta amenaza, destacando los recursos tecnológicos y humanos disponibles. La metodología empleada es cualitativa, con un enfoque exploratorio-descriptivo basado en el análisis documental de políticas públicas, informes oficiales y literatura sobre ciberseguridad en Córdoba. Se revisan las leyes nacionales y provinciales vigentes, con especial énfasis en las normativas de protección frente a ciberataques. Se concluye que la provincia dispone de herramientas especializadas, como sistemas de detección temprana de intrusiones, cifrado de datos y plataformas de inteligencia artificial, que contribuyen a la seguridad de los sistemas informáticos. Los resultados muestran que la falta de un marco legal provincial específico en ciberseguridad, sumada a las desigualdades en el acceso a tecnologías y formación en zonas fuera de la capital, genera vulnerabilidades. La investigación plantea la necesidad de avanzar hacia políticas públicas más inclusivas, que aborden la prevención, sanción y educación en ciberseguridad, para fortalecer una cultura digital de protección frente a los ciberdelitos en la provincia de Córdoba.

Palabras clave: ciberdelito, ciberseguridad, políticas públicas, prevención, infraestructura tecnológica.

ABSTRACT

This paper analyzes the actions of the government of Córdoba in preventing unauthorized access to computer systems, a growing phenomenon in the context of cybercrime, particularly hacking, due to the intensive use of technologies in the public and private sectors. Unauthorized access to computer systems can have serious consequences for information security, the economy and social stability. The research examines the strategies implemented by the provincial government to address this threat, highlighting the technological and human resources available.

The methodology employed is qualitative, with an exploratory-descriptive approach based on documentary analysis of public policies, official reports and literature on cybersecurity in Cordoba. National and provincial laws in force are reviewed, with special emphasis on the regulations for protection against cyber-attacks. It is concluded that the province has specialized tools, such as early intrusion detection systems, data encryption and artificial intelligence platforms, which contribute to the security of computer systems.

The results show that the lack of a specific provincial legal framework on cybersecurity, coupled with inequalities in access to technologies and training in areas outside the capital, generates vulnerabilities. The research suggests the need to move towards more inclusive public policies that address prevention, punishment and education in cybersecurity, in order to strengthen a digital culture of protection against cybercrime in the province of Córdoba.

Keywords: cybercrime, cybersecurity, public policies, prevention, technological infrastructure.

Análisis del accionar gubernamental en la prevención del acceso no autorizado a sistemas informáticos en la Provincia de Córdoba.

Analysis of government actions in the prevention of unauthorized access to computer systems in the Province of Córdoba.

Introducción

Se entiende por ciberdelito o cibercrimen cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o internet y en el que el ordenador, teléfono, televisión, reproductor de audio o video, o dispositivo electrónico, en general, puede ser utilizado para la comisión de un delito o puede ser objeto del mismo delito. *(Rayón Ballesteros y Gómez Hernández, 2014, pp3.)*

El concepto de "hacking" consiste en "acceder en forma indebida o no autorizada, o excediendo una autorización concedida, a un sistema de tratamiento automatizado de la información de acceso restringido. La conducta típica es acceder, esto es ingresar, penetrar, en forma indebida o no autorizada, o excediendo una autorización conferida, a un sistema o dato informático. Debe tratarse de un sistema o dato informático de acceso restringido, vale decir, privado, no abierto al público en general, como lo son algunas redes o sitios de internet. Si el acceso se produce con el consentimiento o permiso del titular de la red, sitio, correo electrónico, etc., la conducta es atípica". (Buompadre, Jorge E. 2017)

El hecho de establecer conexión entre dos computadoras y de acceder a contenidos que se encuentran en webs de acceso a través de internet, requiere la necesidad de proteger la información interna de toda empresa y también la que se comparte con otras sucursales y terceras partes. Frente a este contexto la norma ISO 27000 es un conjunto

de estándares internacionales que se centran en la gestión de la seguridad de la información en las organizaciones. Estos estándares proporcionan un marco integral para establecer, implementar, mantener y mejorar continuamente la seguridad de la información dentro de una empresa. *(Perez, 2024)*

Existen diferentes tipos de información según su grado de susceptibilidad. La información crítica es aquella imprescindible para la operación de una empresa, como por ejemplo la base de datos de empleados, cuya falta afectaría gravemente su actividad. La información valiosa es considerada un activo preciado, como la base de información contable que maneja la empresa, fundamental para su gestión financiera. Por último, la información sensible es aquella que solo debe ser conocida por personal autorizado, de acuerdo con los niveles de acceso, como la base de proyectos o los códigos fuente de software propios de la empresa.

Después la clasificación de las categorías de riesgo en las organizaciones se puede dividir en tres grupos principales. Primero, los errores involuntarios de personas o máquinas, los cuales constituyen una gran parte de los problemas que enfrentan las empresas, y pueden reducirse significativamente mediante la formación adecuada de los empleados. En segundo lugar, los desastres naturales, que requieren que la empresa cuente con un plan de contingencia para enfrentar posibles catástrofes. Finalmente, los ataques voluntarios con un fin determinado, que buscan causar un daño deliberado o beneficiarse de algún modo, afectando de manera considerable a la organización. *(Flores Barahona, 2000)*

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest es el principal instrumento internacional en la lucha contra este fenómeno delictivo. Junto a su Informe Explicativo, fue aprobado por el Comité de Miembros del Consejo de Europa en su reunión número 109, celebrada el 08 de noviembre del 2001, y abierto a la firma en Budapest, el 23 de noviembre del 2001, con motivo de la celebración de la Conferencia Internacional sobre la Ciberdelincuencia. Es importante destacar que el Convenio ha sido firmado y ratificado por 68 países.

la Ley N° 27.411 aprobó el CONVENIO SOBRE CIBERCRIMINALIDAD del CONSEJO DE EUROPA adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, el cual tiene por objeto la prevención de los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos.

En las siguientes líneas se expondrá cómo se encuentra regulado el delito de acceso ilícito en el Convenio sobre la Ciberdelincuencia, al cual Argentina se adhirió, entrando en vigor en el 2018.

Ley 26.388: Ley especial contra delitos informáticos, fue promulgada en 2008 y tuvo en cuenta los siguientes aspectos:

- incorporación de los términos: documento, firma, instrumento privado y certificado (art. 77. CP)
- Incorporación de nuevas figuras delictivas: Producción, ofrecimiento y distribución de representaciones de menores de edad (art. 128, CP)
- violación, apoderamiento y desvío de comunicaciones electronicas (art. 153, Párr. 1°, CP)
- Intercepción de comunicaciones electrónicas o telecomunicaciones (art. 153, Párr. 2°, CP)
- acceso a sistemas o datos informáticos ajenos (art. 153 bis. CP)
- acceso a bancos de datos personales (art.157 bis, párr. 1°, CP)
- Fraudes a sistemas informáticos (art. 173, inciso 16, CP)

- daños informáticos (arts. 183 y 184, incisos 5° y 6°, CP)
- grooming (incorporada en 2013)

Existe una errónea creencia de que los términos “hacker” y “cibercriminal” son lo mismo o se encuentran asociados, cuando en realidad no tienen el mismo significado. Hacker es alguien que aplica el ingenio para crear un resultado inteligente, disfruta explorando las capacidades y limitaciones de los sistemas informáticos y redes.

Los hackers pueden operar dentro del ámbito legal y con fines educativos, investigativos o de mejora. Buscan ayudar a identificar, proteger y solucionar vulnerabilidades con el permiso del propietario del sistema.

Un hacker “positivo” puede realizar pruebas de penetración en un sistema para lograr identificar vulnerabilidades antes de que actores maliciosos puedan ingresar y dañar o invadir dicho sistema. En contraposición, un hacker malicioso es el que accede al sistema sin el permiso para explorar o recopilar información confidencial, aunque sus intenciones no sean con fines dañinos.

Abordando el concepto de ciberdelincuente, es una persona que utiliza la tecnología informática para la comisión de delitos. Estos pueden incluir el robo de datos o fraudes financieros, entre otras actividades ilegales. Operan con intenciones maliciosas, buscando obtener beneficios propios o causar perjuicios, ya sean económicos, sociales o políticos, mediante la explotación de las vulnerabilidades de los sistemas informáticos. Por ejemplo podemos observar a un grupo que realiza ataques de “phishing” para obtener credenciales bancarias y cometer fraudes financieros (el phishing conlleva el uso de la manipulación psicológica y el engaño mediante, los cuales los agentes de amenaza se hacen pasar por entidades benignas para embaucar a los usuarios y lograr que realicen acciones específicas, como por ejemplo hacer clic en enlaces a sitios web falsos, descargar e instalar archivos malintencionados y divulgar información privada, como números de cuentas bancarias o datos de tarjetas de crédito).

Los ataques cibernéticos tienen como objetivo generar daño y, en algunos casos, obtener beneficios económicos. Sus consecuencias van desde pérdidas humanas hasta el riesgo de sistemas esenciales, como salud, banca y seguridad. La capacitación del personal es fundamental para prevenir grandes desastres, incluyendo la configuración segura de hardware (componentes físicos y tangibles de una computadora o sistema informático) y software (conjunto de programas, aplicaciones y sistemas operativos que permiten a un ordenador o dispositivo ejecutar tareas específicas), así como la comprensión de amenazas y consejos de prevención. Un caso destacado es el ataque realizado al Senado de la Nación en el 2023, mediante Ransomware (es un software malicioso que tiene como función poner claves y cifrar archivos que tiene como función impedir el acceso a no ser que se pague el rescate).

Como menciona Marcelo Temperini (2015) por citar un caso difundido mediáticamente, el cual tuvo lugar en Santa Fe, un importante médico de la zona fue víctima de un caso de hacking (uno, 05/08/2013). El Dr. Arturo Serrano (víctima) afirmó en varias entrevistas haber intentado denunciar ante diferentes comisarías sin lograr que en alguna de ellas le tomaran la denuncia por el hecho ocurrido. Hace mención a este caso debido a que indica que “el punto medular del asesoramiento es (...): realizar la denuncia en la dependencia policial más cercana al domicilio de la víctima. Este aspecto, que puede ser considerado como simple, en una gran parte de nuestro país representa un problema en sí mismo, atento al desconocimiento y falta de capacitación que existe por parte de los agentes policiales.” *Temperini. (2015)*

El objetivo general de este manuscrito científico es describir tanto el delito de acceso no autorizado a un dispositivo digital, sistema o red informática, como las acciones implementadas por el Gobierno Provincial de Córdoba para la prevención de la comisión de dicho delito.

Mientras que como objetivos específicos se busca:

- Examinar los recursos tecnológicos y humanos con los que cuenta el Gobierno Provincial para la detección y combate del hacking.
- Describir el marco legal vigente en la Provincia de Córdoba en relación con el delito de acceso no autorizado a sistemas informáticos.
- Indagar sobre las políticas públicas actuales en cuanto a ciberseguridad en la Provincia de Córdoba relacionadas con la prevención del hacking.

Método:

El trabajo tiene un enfoque de tipo cualitativo, mediante la revisión de literatura existente, en la cual no se han tomado datos numéricos como forma de medición, sino que ha sido interpretada de manera teórica, enfocándose en la interpretación de datos textuales y documentales relacionados con las políticas y prácticas del Estado argentino en ciberseguridad.

La investigación tiene un alcance exploratorio-descriptivo, dado que busca entender en profundidad las políticas actuales y sus deficiencias, sin manipular variables de forma experimental, integrando un punto de vista objetivo acerca del tema, incorporando lo originado por las autoridades y estudiado con respecto a la prevención del delito.

Se ha utilizado un tipo de muestra no probabilística, de tipo intencional, la cual pudo aportar una gran ayuda para la recolección de información, realizada de forma subjetiva, no aleatoria. Fueron incorporados como materiales de análisis para la investigación, diversos documentos y fuentes escritas, tales como noticias, papers científicos, leyes del gobierno, información de páginas oficiales de organizaciones que se dedican a investigar y erradicar este delito, los cuales fueron seleccionados con un propósito

determinado, y no fue de forma aleatoria. Utilizando documentos e informes recolectados, que se relacionen y sean clave para poder proporcionar información relevante sobre las políticas de prevención del hacking en Argentina.

Finalmente, el tipo fue no experimental transversal, debido al análisis de casos concretos ubicados en un tiempo y espacio determinado

Participantes: En relación a las unidades de análisis, esta investigación se va a enfocar en los documentos e informes recolectados. En el cual el muestreo se realizó de modo no probabilístico, ya que cada informe sobre ciberdelitos o hacking en específico se seleccionó de acuerdo a las causas relacionadas con las características de la investigación.

Instrumentos

Los datos obtenidos en la recolección fueron fruto de un estudio documental, por lo que se consultaron fuentes escritas, donde se tuvieron en cuenta artículos, bibliografía, documentos, etc. a nivel nacional, provincial y local.

Análisis de datos

A partir de la búsqueda de información y su recolección, se realizó un análisis de datos cualitativo, donde se encontraron temas, patrones y categorías presentes en estos, que permitió interpretarlos, compararlos y explicarlos desde la perspectiva de la problemática del ciberdelito. En este manuscrito se pueden distinguir diferentes momentos: Una primera etapa consistió en un análisis bibliográfico, una segunda parte, se plantea un análisis de datos de tipo documental, donde se recolectan, seleccionan y analizan fuentes documentales según los objetivos propuestos. Y una tercera etapa concentrada en analizar los datos obtenidos, análisis que se lleva a cabo con un tipo de

enfoque cualitativo. Se intentó analizar las diversas acciones que los organismos tanto nacionales como locales llevaron a cabo.

Con respecto al análisis de datos, se plantean las siguientes categorías de análisis:

- Fuerzas de seguridad: organismos del Estado que se encargan de hacer cumplir las normas legales y de mantener el orden social. Esta categoría será referenciada por la Policía Federal, la Policía de la Provincia de Córdoba y la policía perteneciente al Servicio Penitenciario.
- Prevención del delito: Es la actividad que reúne un conjunto de estrategias ya sean situacionales o comunitarias, dirigidas a intervenir en las causas de delito y dificultar el accionar de su autor. Los diferentes conceptos mencionados se pueden describir como:
    - prevención comunitaria: hace referencia a la participación activa de los habitantes en la prevención del delito.
    - Prevención situacional: Hace referencia al aspecto del lugar donde se desarrolla el delito, y qué acciones se pueden realizar para que este disminuya al mejorar la apariencia del entorno.
- Políticas públicas: son los planes o acciones que el gobierno desarrolla para buscar el bien común y la seguridad de la sociedad.
- Centro de Respuesta y Alerta Temprana de Seguridad informática: busca proveer de herramientas, realizar gestiones, llevar a cabo procesos, agilizar los controles de seguridad e implementar acciones, para que la ciudadanía, las instituciones y las empresas puedan tener a quien recurrir ante un incidente de tipo informático.

- Infraestructura tecnológica adecuada/correcta: Se refiere a la presencia de sistemas de detección y prevención tempranas, como firewalls (cortafuegos), cifrado de datos o plataformas de inteligencia artificial.
- Oficina especializada en ciberdelitos del Ministerio Público Fiscal: Es la oficina que se encarga de la articulación y desarrollo de los recursos requeridos para abordar de forma eficaz la ciberdelincuencia, entre ellos el delito central de nuestra investigación

Resultados

La importancia de los recursos tecnológicos y humanos en la lucha contra los ciberdelitos, como el hacking, es fundamental para salvaguardar tanto la información sensible del gobierno como la de los ciudadanos, además de garantizar la seguridad de los sistemas críticos. En un contexto provincial como el de Córdoba, donde las redes informáticas son responsables de gestionar servicios esenciales tales como la salud, la educación, las finanzas públicas y la seguridad, la protección de estos sistemas frente a amenazas cibernéticas es indispensable para asegurar la estabilidad y el correcto funcionamiento de la provincia.

Los recursos tecnológicos, como el software especializado, hardware de última generación y sistemas de detección y prevención, son esenciales para el monitoreo de redes, la identificación de amenazas en tiempo real y la respuesta efectiva a incidentes de hacking. Una infraestructura tecnológica sólida, que incluya herramientas de cifrado de datos, plataformas de inteligencia artificial y/o cortafuegos (firewalls) para la

detección temprana de anomalías, permite reducir el riesgo de ataques cibernéticos y mitigar sus consecuencias.

La relevancia de contar con una infraestructura tecnológica adecuada radica en su capacidad para prevenir accesos no autorizados a sistemas críticos, garantiza la continuidad operativa de los servicios provinciales ya que acortar los tiempos de respuesta ante incidentes es sumamente importante. Sin estos recursos, la provincia se vuelve vulnerable a ataques que podrían afectar aspectos fundamentales, como la recolección de impuestos, así como los sistemas de salud y transporte.

Los recursos humanos desempeñan un papel igualmente crucial, dado que incluso la tecnología más avanzada resulta ineficaz sin un personal capacitado que sepa utilizarla y gestionarla adecuadamente. Los especialistas en ciberseguridad, ingenieros de sistemas y analistas de amenazas son responsables de implementar medidas preventivas, responder a incidentes y adaptarse a las nuevas tácticas empleadas por los ciberdelincuentes. La necesidad de contar con personal altamente capacitado se deriva del creciente nivel de sofisticación de los ataques cibernéticos. Las medidas de seguridad deben evolucionar constantemente; por lo tanto, la capacitación continua del personal es esencial para mantenerlos al tanto de las amenazas emergentes. Los equipos de seguridad cibernética bien entrenados son capaces de identificar vulnerabilidades antes de que sean explotadas, responder de manera ágil a brechas de seguridad y coordinar acciones con otras entidades para mitigar el daño.

El Centro de Respuesta y Alerta Temprana de Seguridad informática de la provincia de Córdoba (CSIRT) ingresó a la Red CSIRT Américas. Esta red reúne a los equipos de respuesta ante incidentes cibernéticos gubernamentales de los Estados Miembros de la Organización de los Estados de América (OEA).

Córdoba se convierte en la tercera provincia del país en formar parte de la red. Junto a las provincias de Buenos Aires y Neuquén, Argentina suma un total de siete Centros de Respuesta y Alerta Temprana que forman parte de la red siendo referente a nivel latinoamericano.

A través de CSIRT Américas, los Estados intercambian información sobre alertas de ciberseguridad y acceden a asistencia técnica para fortalecer los servicios de los CSIRTs. Incluye capacitación, herramientas y recursos para ayudar a los países y provincias a fortalecer sus capacidades de ciberseguridad.

De esta manera, el CSIRT Córdoba se incorpora a una plataforma que le permitirá poner a disposición de las organizaciones y ciudadanos, una gran cantidad de herramientas destinadas a la prevención, mitigación y gestión de ataques cibernéticos.

Con esta adhesión, entre otras funciones, se accede a información actualizada sobre las últimas amenazas y vulnerabilidades que existen, lo que permite responder de manera más efectiva a diferentes tipos de ataques cibernéticos.

Proteger los activos digitales frente a las amenazas que existen en la red y la seguridad de la información, software, datos y sistemas se ha convertido en una obligación para todas las organizaciones privadas y públicas y se vuelve un tema cada vez más relevante en la vida de las personas. Dentro del sector tecnológico, la ciberseguridad es una de las verticales con mayor crecimiento, ya que representa una de las claves para el crecimiento sostenible del sector. En este contexto, y con el objetivo de posicionar a la ciudad de Córdoba como un polo tecnológico referente en materia de ciberseguridad que brinda productos y servicios de alta calidad a organizaciones públicas y privadas, un grupo de empresarios, emprendedores, académicos e instituciones referentes en la temática, coordinados desde la Secretaría de Planeamiento, Modernización y Relaciones

Internacionales de la Municipalidad de Córdoba, formó el Córdoba Cyber-Security Hub. *CORLAB*. *Gobierno de Córdoba. (2022).*

Uno de los ejes que se trabaja en la organización es la necesidad de promover la demanda por servicios de ciberseguridad por parte de organizaciones públicas y privadas e incrementar el nivel de inversión que realizan en este tema. Mientras que el último desafío que se planteó, que no es un tema menor, conlleva el desarrollo de acciones para promover la generación de nuevos talentos especializados en ciberseguridad para atender a los requerimientos del sector. *CORLAB*. *Gobierno de Córdoba. (2022).*

De esta manera, para atender las problemáticas y desafíos mencionados, desde el Hub se establecieron algunas líneas de acción y trabajo entre los que se destacan: la organización de un congreso regional de Ciberseguridad, de jornadas de concientización con diferentes sectores, de competencias de seguridad informática (CTF) y de talleres y capacitaciones especializadas, la creación de un directorio de empresas y emprendimientos de ciberseguridad, la generación de un equipo de respuesta ante emergencias informáticas (CERT) y la creación de canales de comunicación y difusión especializados en la materia. *CORLAB*. *Gobierno de Córdoba. (2022).*

Para describir el marco legal vigente en la provincia de Córdoba en relación con el delito de acceso no autorizado a sistemas informáticos y las políticas públicas actuales de ciberseguridad, es esencial analizar tanto las normativas nacionales que son aplicables a la provincia como las iniciativas específicas que ha implementado el gobierno provincial en materia de prevención del hacking y otros ciberdelitos.

En la provincia de Córdoba, al igual que en el resto de Argentina, los delitos informáticos se regulan bajo la legislación nacional, dado que las provincias no

poseen competencia directa para establecer sus propias normativas penales. Los principales aspectos legales que se aplican a los ciberdelitos, incluido el acceso no autorizado a sistemas informáticos (hacking), son los siguientes:

a) Código Penal Argentino (Ley 11.179)

- El Código Penal argentino fue modificado en 2008 mediante la Ley 26.388, que incorporó específicamente el delito de acceso no autorizado a sistemas informáticos, conocido como "hacking". Esta ley introdujo diversas figuras penales relacionadas con los delitos informáticos y el uso indebido de tecnologías de la información.
- Artículo 153 bis: Penaliza el acceso ilegítimo a un sistema informático o digital, castigando con prisión de quince días a seis meses a quien, sin la debida autorización, acceda a sistemas informáticos de datos de acceso restringido. Esta norma se aplica directamente a los casos de hacking en la provincia de Córdoba.
- Artículo 157 bis: Agrega penas para quien interfiera o intercepte comunicaciones electrónicas sin consentimiento, algo común en casos de hacking.

Este marco legal abarca todas las jurisdicciones del país, incluida la provincia de Córdoba, estableciendo una sólida base jurídica para sancionar el acceso no autorizado a sistemas informáticos.

Ley Nacional de Protección de Datos Personales (Ley 25.326)

La Ley 25.326 establece disposiciones para la protección de datos personales, garantizando que los ciudadanos cuenten con derechos en cuanto a la protección de su

información. En el caso de que un ataque de hacking comprometa datos personales, esta ley es aplicable en la jurisdicción de Córdoba.

Esta ley establece que la seguridad de los sistemas informáticos que gestionan datos personales debe ser protegida, lo que impone a las instituciones provinciales la obligación de garantizar medidas adecuadas contra el acceso no autorizado.

Ley Nacional de Delitos Informáticos (Ley 26.388)

Esta ley es fundamental en la regulación de delitos como el hacking, tipificando los delitos contra la confidencialidad, la integridad y la disponibilidad de sistemas y datos informáticos. Establece penas más severas cuando los sistemas atacados pertenecen a entidades gubernamentales o afectan servicios esenciales para la sociedad.

El Gobierno de Córdoba ha trabajado en la implementación de políticas públicas y programas de ciberseguridad, alineándose con las directrices nacionales y buscando prevenir y combatir el hacking. Aquí se detallan las políticas y programas más relevantes:

a) Plan Provincial de Modernización del Estado

Córdoba ha avanzado en la modernización digital de sus servicios, lo que incluye mejoras en la infraestructura de tecnologías de la información y comunicaciones (TIC). El objetivo de este plan es digitalizar los procesos gubernamentales y mejorar la seguridad cibernética para proteger tanto la infraestructura crítica como los datos sensibles de los ciudadanos.

Dirección General de Tecnología de la Información y Comunicaciones (DGTIC): La DGTIC de Córdoba juega un papel fundamental en la implementación de políticas de seguridad informática, gestionando la infraestructura digital del gobierno provincial y

liderando las estrategias de ciberseguridad. Esta dirección supervisa el desarrollo y la aplicación de medidas de seguridad para mitigar riesgos asociados con el hacking, como la implementación de firewalls, sistemas de autenticación de múltiples factores y sistemas de detección y prevención de intrusiones (IDS/IPS).

b) Colaboración con Programas Nacionales de Ciberseguridad

Córdoba forma parte del marco nacional de ciberseguridad, colaborando con organismos como CERT.ar, que es el Centro de Respuesta a Incidentes de Seguridad Informática de Argentina. CERT.ar proporciona asistencia técnica a las provincias en la prevención, monitoreo y respuesta ante incidentes de hacking y otros ciberdelitos.

A través de su participación en el Plan Nacional de Ciberseguridad, la provincia se beneficia de herramientas y recursos ofrecidos por el gobierno nacional, que incluyen programas de monitoreo, capacitación y respuesta ante incidentes cibernéticos.

c) Creación de Unidades Especializadas en Delitos Informáticos

La Policía de Córdoba cuenta con la División de Delitos Tecnológicos, una unidad especializada en la investigación de ciberdelitos, incluyendo el hacking. Esta unidad es responsable de investigar y prevenir incidentes relacionados con el acceso no autorizado a sistemas informáticos, trabajando en coordinación con otras fuerzas de seguridad nacionales, como la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI).

Esta división también colabora en la investigación de incidentes que comprometen tanto a entidades públicas como privadas, y ha sido clave en la implementación de estrategias de respuesta rápida ante ciberataques.

d) Capacitación en ciberseguridad para el personal gubernamental

El Gobierno de Córdoba ha implementado programas de capacitación continua en ciberseguridad para su personal, buscando que los empleados estén preparados para prevenir incidentes de hacking y responder ante situaciones críticas. Estos programas son realizados en colaboración con universidades locales, como la Universidad Nacional de Córdoba (UNC), y organizaciones privadas que brindan formación en seguridad informática.

La capacitación incluye tanto el manejo de tecnologías de protección de datos como la concientización sobre las buenas prácticas de ciberseguridad, enfocándose en minimizar las vulnerabilidades humanas, que son frecuentemente explotadas en ataques de hacking.

e) Iniciativas de Concientización Ciudadana

La provincia de Córdoba ha promovido campañas de concientización pública sobre los riesgos asociados a los ciberdelitos, incluida la importancia de proteger los datos personales y mantener prácticas de seguridad en línea. Estas campañas forman parte de las políticas preventivas orientadas a fortalecer la ciberseguridad, no solo a nivel gubernamental, sino también entre los ciudadanos y empresas privadas.

DISCUSIÓN

El objetivo de esta investigación fue describir tanto el delito informático como las acciones que el Gobierno de la Provincia de Córdoba lleva a cabo para prevenir o disminuir dicho tipo delictivo.

Según enumeran los especialistas en el tema, las fortalezas del sector en Córdoba capital son varias, comenzando con que se cuenta con recursos humanos (profesionales)

capacitados y con experiencia; también se destaca la existencia de universidades con programas de estudios en ciberseguridad; se cuenta con un número significativo de empresas especializadas en ciberseguridad; y por último, existe una red consolidada de trabajo interdisciplinario. Sin embargo, también existen debilidades en el sector que son las principales cuestiones hacia donde el Hub tendrá que orientar sus esfuerzos. Ellas son: falta de concientización y cultura social en ciberseguridad tanto en empresas como en instituciones; poca inversión en ciberseguridad por parte de empresas y gobiernos; falta de coordinación y de trabajo en comunidad por parte del sector; desconexión academia-empresas; falta de capacitaciones en ciberseguridad, en especial en español; falta de retención de recursos humanos capacitados; falta de apoyo estatal para auditorías y falta de visión e integración internacional del sector. CORLAB. *Gobierno de Córdoba. (2022).*

En los últimos años, los ataques cibernéticos fueron incrementando tanto en frecuencia como en estrategia. El bajo riesgo y costo que estos delitos conllevan han sido claves en su crecimiento. Todo esto es mucho más fácil debido a que con la simple conexión de un celular a internet, el ciberdelincuente puede causar grandes perjuicios a las víctimas.

No hay que utilizar tecnología sin antes haber comprobado su confiabilidad, es así como se vuelve necesario que todas las personas conozcan sobre ciberseguridad aunque sean los temas más básicos y los vayan profundizando a medida que lo requieran.

En cuanto al análisis de los recursos tecnológicos y humanos de la Provincia de Córdoba, revela que es sumamente importante contar con una infraestructura tecnológica y un personal altamente capacitado para prevenir y enfrentar ciberdelitos, como el hacking. De acuerdo a lo mencionado en el apartado de Resultados se logra resaltar que en un entorno donde los sistemas provinciales son los que gestionan y

administran los servicios esenciales, como la educación, la salud, la finanzas públicas y la seguridad, es sumamente indispensable tener la adecuada protección de estos sistemas frente a amenazas cibernéticas. La presencia de recursos tecnológicos de última generación como sistemas de cifrado, es clave para detectar y prevenir accesos no autorizados, lo cual responde a la necesidad de tener una infraestructura sólida que proteja los sistemas críticos ya mencionados anteriormente. Además de esto, la constante capacitación de los recursos humanos es igualmente esencial, ya que los ataques cibernéticos son cada vez más sofisticados y la tecnología únicamente, no basta sin un personal informado y especializado capaz de gestionar y adaptarla frente a nuevas amenazas.

Es imperativo incluir la temática de la ciberseguridad en el ámbito académico a todos los niveles. Actualmente, diversas universidades están implementando contenidos relacionados con esta materia y considerando la ciberseguridad como parte de las habilidades blandas. Es fundamental integrar esta temática en los planes de estudio, no solo en carreras afines, sino también en otras disciplinas.

Las personas hoy en día confían demasiado en la tecnología porque no son conscientes del riesgo que todo esto conlleva. Se debe trabajar arduamente en la formación de las personas en este asunto, para así poder evitar y prevenir que más ciberataques sigan ocurriendo. A la gente se le ha dado libre acceso a la tecnología pero no se ha asegurado un trabajo previo de concientización que explique el riesgo que es el consumo e ingreso inconsciente a las redes.

Hoy en día ya no se puede hablar solo de antivirus, concepto familiar cuando se plantea sobre aspectos de seguridad. Desde que todos estamos hiperconectados e internet ya

forma parte de nuestras vidas, el ambiente se vuelve más complejo, por lo que hay que protegerse desde el primer momento en el que se utiliza el internet.

Los delincuentes que emplean la tecnología para alcanzar sus metas han evolucionado hacia el ciberdelito. Para protegernos, es fundamental implementar mecanismos, procedimientos y conductas alineados con la seguridad en el entorno de Internet, razón por la cual es crucial abordar el tema de la ciberseguridad. Un ejemplo sencillo es el uso del teléfono móvil, que se ha convertido en nuestra plataforma de trabajo, albergando correos, contactos y mensajes. Además, contiene datos personales sensibles, como información de salud, fotografías y aplicaciones, y ha llegado a funcionar incluso como nuestra billetera digital.

Al considerar la Norma ISO 27000 y los procesos organizacionales, es fundamental que la ciberseguridad garantice tres aspectos clave: disponibilidad (asegurando que la información sea siempre accesible), integridad (garantizando que no sea alterada de ninguna manera) y confidencialidad (limitando el acceso únicamente a las personas autorizadas). Sin embargo, es igualmente importante abordar el factor humano. Es imprescindible capacitar a los empleados y fomentar la conciencia sobre los riesgos asociados al ciberespacio. Aunque Internet ofrece oportunidades valiosas, como la posibilidad de ver una película en línea, el uso de redes WiFi compartidas, como las de un vecino, puede permitir que personas no autorizadas accedan a nuestros dispositivos y a nuestros datos.

Un muy buen ejemplo son los ataques bancarios, los cuales todos concluyen en quebrantar la voluntad del cliente a través del llamado “hacking social”, el cual hace referencia a que el usuario inhabilite su racionalidad y de alguna manera interactúa con el criminal dando sus datos de confianza sobre sus productos bancarios como

contraseñas de tarjetas, datos los cuales bajo plena conciencia no hubieran brindado a un extraño, un claro y conocido ejemplo de esto es el popularmente llamado “cuento del tío”. Considerando esto, se debe trabajar arduamente en la educación del cliente bancario, estas situaciones aumentaron mucho desde que la mayoría de los clientes comenzó a operar mediante el home banking.

Lamentablemente las empresas o entidades no se animan a exponer abiertamente cuando sufrieron un ataque, debido a que creen que esto les da una mala imagen, así es como debido a esto, no existen estadísticas certeras sobre los ataques de ciberseguridad en Córdoba.

La falta de una estrategia integral que combine la inversión pública y privada, la creación de una cultura organizacional orientada a la ciberseguridad y la capacitación de personal es una de las barreras identificadas en esta investigación. Todos estos son factores independientes que determinan la efectividad de las políticas públicas. Como una posible conclusión se plantea que una infraestructura tecnológica sólida es crucial, pero que su efectividad depende indudablemente de la capacitación constante del personal especializado, debido a que sin equipos bien entrenados, incluso las mejores y mas avanzadas tecnologias pueden no ser suficientes para prevenir o mitigar un ataque de hacking.

Los temas tecnológicos evolucionan a un ritmo vertiginoso, lo que requiere estar constantemente actualizado sobre las últimas novedades y colaborar estrechamente con los expertos en informática para comprender y, de este modo, generar seguridad desde la perspectiva jurídica. Entre las principales normativas nacionales e internacionales vigentes en el ámbito de la seguridad informática se destacan la Ley de Delitos

Informáticos, la Ley de Protección de Datos Personales, la Ley de Firma Digital y la Ley de Grooming.

Estas regulaciones buscan proteger los derechos de los usuarios y garantizar un entorno digital seguro y confiable.

Al igual que las empresas y las personas, las áreas gubernamentales también son muy vulnerables a los ataques cibernéticos. La transformación de base hacia el gobierno electrónico y digital en la Argentina trae consigo nuevas realidades y aspectos a tener en cuenta. Para Enrique Dutra, especialista el ciberseguridad y fundador de PuntoNet, la ciberseguridad en el sector público debe ser tenida en cuenta por sobre todas las cosas: "No nos olvidemos que una ciudad funciona con servicios que son usados por la ciudadanía, y si es víctima de un ciberataque, podría afectar a miles de personas", destaca.

A modo de ejemplo, Dutra recordó que en plena pandemia unos ciberdelincuentes dejaron fuera de servicio la red de distribución de agua de la ciudad de Curitiba en Brasil, sobre todo en la zona donde estaban los hospitales con mayor cantidad de pacientes con Covid-19 y el impacto fue muy alto. *CORLAB*. Gobierno de Córdoba. (2022). pag 22

Considerando lo anterior el marco legal vigente en la Provincia de Córdoba, podemos identificar ciertas generalizaciones como, la legislación nacional como una base común, esto significa que las provincias se rigen por un mismo marco jurídico nacional, esto asegura que haya una uniformidad, pero al mismo tiempo plantea una limitación de la

autonomía provincial en cuanto a la formulación de normas o políticas específicas de acuerdo a cada región. La ley 26.388 mencionada y descrita anteriormente, establece sanciones claras para el acceso indebido a sistemas informáticos, lo que proporciona un marco legal coherente para abordar el hacking en todo el país, incluyendo a Córdoba.

A pesar de la fortaleza y aplicabilidad de las leyes nacionales, existen varios aspectos que limitan la efectividad de la legislación en la provincia:

Aunque las leyes nacionales son aplicables en Córdoba, se da por supuesto que los actores locales (gobierno provincial, las empresas, y los ciudadanos) conocen y aplican estas normativas de manera efectiva. Sin embargo, la implementación de estas normativas nacionales en la provincia pueden verse afectadas por las deficiencias en la infraestructura local que pueden existir, la falta de recursos para la capacitación y sensibilización, y la escasa cooperación entre las instituciones locales, puede crear "lagunas" en la aplicación efectiva de la ley.

La Ley 25.326 de Protección de Datos Personales se presenta como una pieza clave en la lucha contra el hacking, ya que impone una "obligación a las instituciones" (incluidas las provinciales) de proteger los datos personales de los ciudadanos frente a accesos no autorizados. De esta forma, la ley se vincula directamente con la protección contra los ciberdelitos, en particular aquellos orientados al robo o compromiso de datos personales.

La criminología crítica señalaría que la legislación actual no aborda lo suficiente las "desigualdades estructurales" en el acceso a la tecnología y la ciberseguridad. En un contexto en el que las empresas y actores gubernamentales en la provincia de Córdoba

pueden tener capacidades desiguales para implementar medidas de protección, la ley podría no ser completamente equitativa en su aplicación. Esto se relaciona con la crítica de la criminología crítica sobre cómo las “normas jurídicas no siempre consideran las realidades sociales” de los distintos actores involucrados.

La criminología crítica también resalta que las políticas públicas deben ser construidas de manera que reflejen las necesidades de las comunidades locales y no solo las necesidades normativas. Aunque las leyes nacionales como la Ley 26.388 tienen un enfoque preventivo y punitivo, la falta de políticas locales que contemplen el contexto socioeconómico de Córdoba puede generar desigualdades en la aplicación de estas normas. En otras palabras, el marco legal vigente podría beneficiarse de un enfoque más integrador y menos “uniforme”, que considere las particularidades locales.

Al ser una legislación nacional, existe una clara falta de regulación provincial específica que considere las características y necesidades locales. Las provincias, incluyendo a Córdoba, podrían enfrentarse a desafíos únicos en la prevención de ciberdelitos debido a factores como el acceso desigual a las tecnologías, la infraestructura variable y la escasa cultura de ciberseguridad en muchas instituciones provinciales.

Desde la criminología crítica, se podría argumentar que la prevención de ciberdelitos no solo debe depender de la represión a través de leyes más severas, sino también de una estrategia integral que incluya la educación, la concientización y la creación de una cultura de ciberseguridad. En este sentido, las leyes deben ser acompañadas de un esfuerzo social y educativo que vaya más allá de la simple sanción penal.

En cuanto a las políticas públicas de ciberseguridad en la provincia de Córdoba, para la prevención del hacking, los resultados indican que el gobierno de la provincia ha dado significativos pasos en la implementación de políticas públicas de ciberseguridad, manteniendo una linealidad tanco con las directrices nacionales como locales. Dichas políticas buscaron prevenir y mitigar los riesgos asociados al hacking y otros ciberdelitos, a través de diversas estrategias. Como por ejemplo el plan provincial de Modernización del Estado ha sido uno de los principales instrumentos en la digitalización de los procedimientos gubernamentales. Dicho plan integra mejoras sustanciales en la infraestructura de las tecnologías de información y comunicación, esto no solo ha permitido a la provincia modernizar los servicios públicos, sino también fortalecer la seguridad cibernética.

La colaboración Nacional e internacional con programas nacionales como CERT.ar y el "Plan Nacional de Ciberseguridad" es una característica a destacar de las políticas provinciales. Dicha cooperación no solo brinda herramientas y recursos técnicos, sino que también fortalece la capacidad de respuesta ante incidentes cibernéticos y facilita la capacitación continua del personal provincial.

La existencia de la División de Delitos Tecnológicos dentro de la policía de Córdoba refleja el compromiso del gobierno para la prevención e investigación de ciberdelitos, sobre todo aquellos relacionados al hacking. Dicha unidad coopera tanto con las fuerzas nacionales como con el sector privado, la cual ha sido un punto de ayuda clave para mejorar la respuesta ante incidentes de hacking.

A pesar de los avances significativos en materia de ciberseguridad, existen diversas áreas que podrían mejorar o que no han sido completamente resueltas, como por ejemplo, la desigualdad en el acceso a la capacitación y recursos, ya que a pesar de la oferta de programas de formación en ciberseguridad estos no son accesibles para todos los sectores, especialmente en áreas fuera de la Capital provincial, ciudades o provincias que podrían carecer de los recursos para implementar políticas de seguridad adecuadas. Dicho desequilibrio en el acceso a la capacitación puede generar brechas de vulnerabilidad en algunas partes de la provincia e incluso el País. En cuanto a dicha desigualdad en el acceso a recursos, la criminología crítica argumentaría que las políticas de ciberseguridad no pueden ser realmente efectivas si no tienen en cuenta las desigualdades estructurales en el acceso a la tecnología y educación.

Desde la criminología crítica se puede argumentar que la intervención estatal debe incluir tanto la sanción a los ciberdelincuentes como la responsabilidad de las instituciones públicas y privadas en la protección de datos y la seguridad cibernética.

Desde el punto de vista teórico, la investigación destaca que las políticas públicas de ciberseguridad a pesar de estar alineadas al marco nacional, deben avanzar hacia una adaptación local más precisa, que aborde las particularidades tecnológicas y socioeconómicas de la provincia en sí.

Claramente las políticas públicas de ciberseguridad en Córdoba, son adecuadas en términos de infraestructura y alineación con políticas nacionales, pero la implementación realmente efectiva en todos los sectores de la provincia continúa siendo un desafío. La criminología crítica puede brindar una perspectiva útil para reformular las políticas, sugiriendo un enfoque preventivo y educativo que aborde las desigualdades y fortalezca la cohesión social.

El rol del estado en la prevención del ciberdelito es sumamente importante para poder proteger y cuidar la información y los sistemas. La combinación de recursos tecnológicos y humanos es indispensable, pero su efectividad depende de una cultura de ciberseguridad bien establecida y determinada, como de la inclusión de todos los sectores sociales en estas políticas. La criminología crítica nos ayuda a ver que el contexto social y las estructuras de poder deben ser considerados al evaluar la eficacia de las medidas adoptadas..

En términos de la teoría crítica, también es importante examinar el papel del Estado en la producción y distribución de la seguridad. Las políticas de ciberseguridad del gobierno de Córdoba pueden ser vistas como una forma de garantizar la estabilidad del sistema económico y político dominante. A través de la protección de los sistemas críticos (salud, transporte, educación, etc.), el Estado no solo busca proteger a los ciudadanos, sino también garantizar la continuidad operativa de las instituciones que sustentan el orden social y económico establecido.

Desde una perspectiva criminológica crítica, esto podría interpretarse como un intento de mantener la estabilidad y el control del sistema a través de acciones preventivas que buscan evitar que los ciudadanos, colectivos sociales o actores privados desafíen el status quo. Así, el hacking, en lugar de ser simplemente un acto delictivo, podría ser visto como una forma de resistencia cibernética que pone en cuestión la autoridad de las instituciones estatales y empresariales

La teoría criminológica crítica proporciona una lente valiosa para analizar no solo las acciones del gobierno provincial en la lucha contra el hacking, sino también las dinámicas de poder, las desigualdades estructurales y la función del control social que subyacen a las políticas de ciberseguridad. Desde esta perspectiva, el hacking no es solo un acto individual de ilegalidad, sino una respuesta a un sistema desigual que controla y monitorea los espacios digitales en beneficio de unos pocos.

Es fundamental fomentar la conciencia pública acerca de la ciberseguridad mediante la implementación de campañas de concientización en escuelas, empresas y comunidades, con el objetivo de cultivar una cultura de prevención más sólida. Además, es crucial aumentar la inversión en educación, desarrollando programas accesibles en ciberseguridad que presten especial atención a grupos más vulnerables, garantizando así que todos tengan acceso a la información y herramientas necesarias para protegerse en el entorno digital. Por último, fortalecer la colaboración interinstitucional es esencial; se debe promover la cooperación entre los sectores público, privado y académico para establecer una red de apoyo efectiva en la lucha contra el ciberdelito, lo que permitirá un enfoque más integral y eficaz en la prevención y respuesta ante amenazas cibernéticas.

En cuanto a las futuras líneas de investigación, considero que sería fundamental explorar el impacto social de la ciberseguridad, investigando cómo las políticas implementadas afectan a diferentes grupos sociales, con un enfoque especial en las poblaciones vulnerables, que no tienen acceso a los mismos recursos.

En cuanto a las fortalezas de la presente investigación encontramos que esta abarca de manera amplia el fenómeno del acceso no autorizado a sistemas informáticos,

incorporando aspectos técnicos, sociales y legales, lo cual permite una comprensión más compleja de las políticas públicas y las prácticas gubernamentales de la provincia de córdoba en cuanto a la ciberseguridad y el hacking. Uno de los puntos más fuertes de esta investigación es su enfoque en las políticas públicas de la provincia, al centrar el análisis en esta, se brinda un visión contextualizada que considera las particularidades socioeconómicas y culturales del lugar.

El tema de la ciberseguridad es altamente relevante a día de hoy, debido al aumento global de los ciberdelitos, especialmente en contextos gubernamentales. Al centrar el análisis en la provincia de Córdoba, la investigación aborda un ámbito local de gran interés, ofreciendo información que puede ser útil tanto a nivel provincial como nacional.

Sin embargo en cuanto a limitaciones de la investigación, el enfoque provincial y no nacional pasa a tener importancia también, dado que las políticas públicas de ciberseguridad y las prácticas gubernamentales varían significativamente en cada provincia de Argentina, los hallazgos pueden no ser directamente aplicables a otras regiones del país. En temas como la ciberseguridad, donde la tecnología y las amenazas evolucionan rápidamente, algunos datos y recursos recopilados en la investigación pueden haber quedado desactualizados. La velocidad del cambio tecnológico implica que las políticas públicas y las estrategias de respuesta puedan haberse modificado después de la recopilación de información, lo que limita la validez de los resultados a largo plazo.

Posibles mejoras a implementar:

Refuerzo de la capacitación continua, especialmente en el ámbito de las nuevas amenazas cibernéticas y el uso de tecnologías emergentes.

Aumento de la inversión en ciberseguridad, tanto a nivel provincial como en el sector privado, para asegurar que los recursos tecnológicos sean de vanguardia y se mantengan actualizados.

Fomento de una cultura de ciberseguridad, que involucre no solo a los expertos en tecnología, sino a todos los sectores de la sociedad, incluidos los ciudadanos

Referencias

Argentina.gob.ar. (2008, 25 junio). Argentina.gob.ar.

https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Temperini, Marcelo Gabriel Ignacio. *El desafío de la lucha contra el cibercrimen en Argentina. (2015).* Papeles. Universidad Nacional del Litoral. Facultad de Ciencias Jurídicas y Sociales. Conicet.

https://ri.conicet.gov.ar/handle/11336/48467

Flores Barahona, J. F. (2000). *Diseño de un software criptográfico de seguridad para las comunicaciones navales* [Tesis de grado]. Recuperado de*:* http://www.dspace.espol.edu.ec/handle/123456789/3300

Perez, P. (2024, 23 febrero). *Todo lo que necesitas conocer sobre la norma ISO 27000 - PMG SSI - ISO 27001. PMG SSI - ISO 27001.*

https://www.pmg-ssi.com/2024/02/todo-lo-que-necesitas-conocer-sobre-la-norma-iso-27000/

Gobierno de Córdoba. (2022). *Ciberseguridad Hub: Documento de orientación en ciberseguridad.* CORLAB

https://corlab.cordoba.gob.ar/wp-content/uploads/2022/07/Publicacion-Ciberseguridad-Hub-vertical.pdf

Gobierno de Córdoba. (2022, 21 junio). *Ciberseguridad: Córdoba se incorporó a la Red CSIRT Américas. Gobierno de la Provincia de Córdoba*

https://www.cba.gov.ar/ciberseguridad-cordoba-se-incorporo-a-la-red-csirt-americas/