CPAIA

INNOVA
innovaconsultores.com.ar

CIBERSEGURIDAD

ING. JORGE NAGUIL

LIC. ESTEBAN GESTO

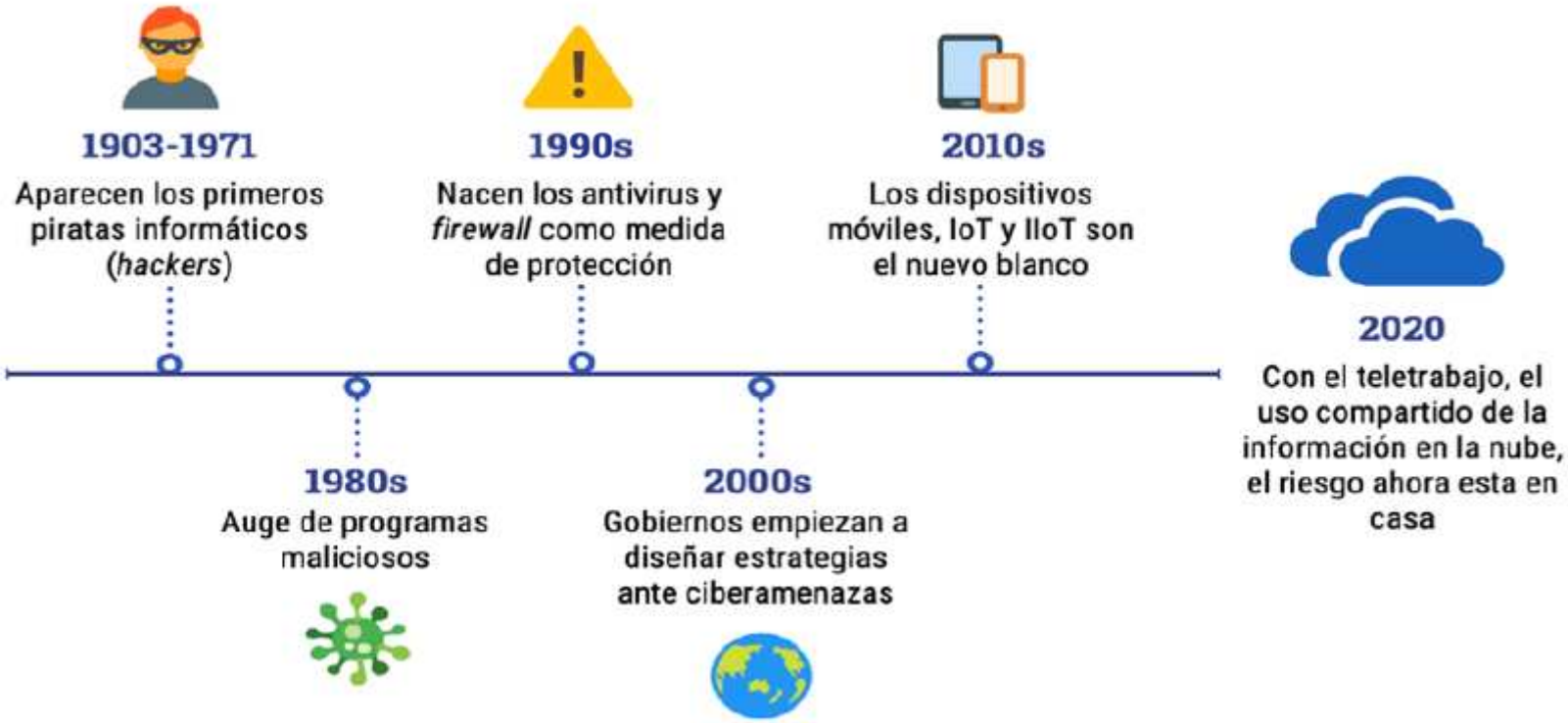
09 DE MAYO DE 2024

1. FUNDAMENTOS DE LA CIBERSEGURIDAD - IMPORTANCIA

- Es crucial en el mundo, todos estamos expuestos a posibles riesgos si no tomamos medidas adecuadas para proteger nuestra información.
- El robo de identidad, la pérdida de datos sensibles, el fraude financiero y el daño a la reputación son solo algunas de las posible consecuencias

INOVA

I. FUNDAMENTOS – EVOLUCIÓN DE LA CIBERSEGURIDAD

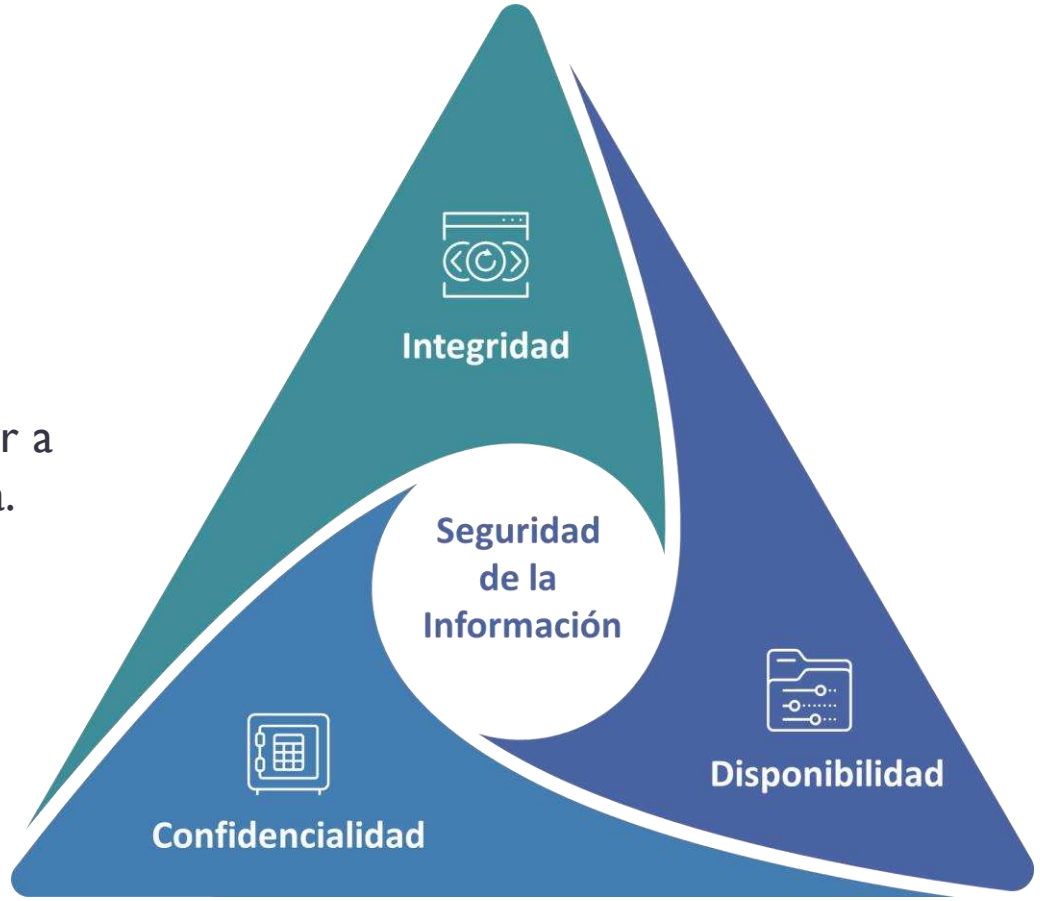


Fuente: elaborado en infograph.venngage.com (2020)

INOVA

1. FUNDAMENTOS – OBJETIVO DE LA CIBERSEGURIDAD

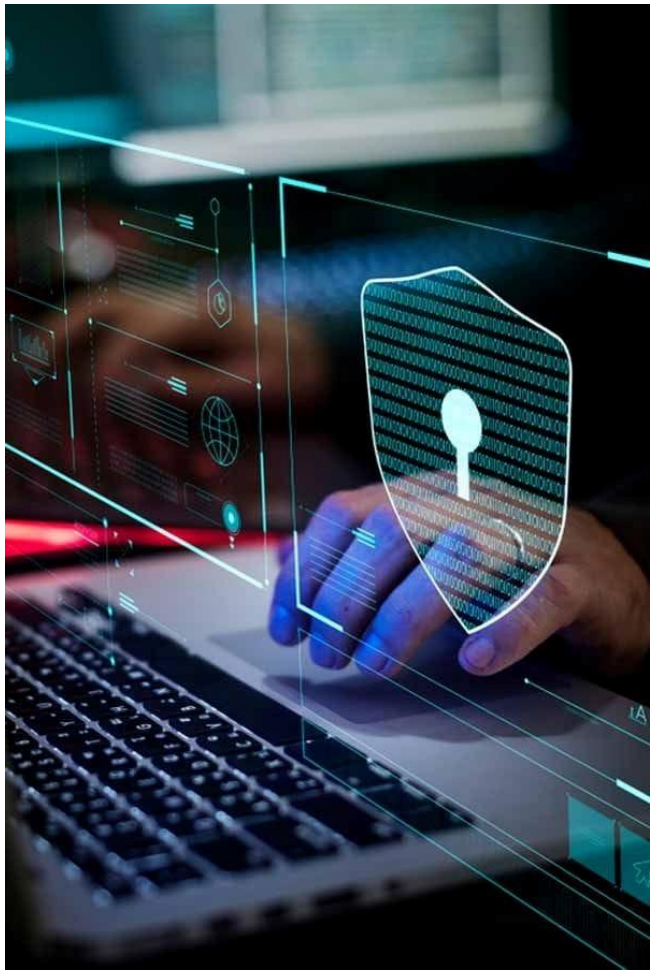
- El objetivo principal de la ciberseguridad es garantizar
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Asegurando que solo las personas autorizadas puedan acceder a ella y que no se altere ni se destruya de manera no autorizada.



INOVA

I. FUNDAMENTOS – POLÍTICAS DE LA CIBERSEGURIDAD

- Las políticas y procedimientos de seguridad son reglas y directrices establecidas para proteger su información y sistemas
- Educación y entrenamiento: Es importante que las organizaciones proporcionen entrenamiento regular para asegurarse de que comprendan cómo proteger la información de manera efectiva.
- Una política de seguridad por ejemplo puede incluir requisitos para el uso de contraseñas seguras, la instalación de software antivirus y la restricción del acceso a información confidencial solo a personas autorizadas.



INOVA

1. FUNDAMENTOS - RIESGOS E INCIDENTES

- Tipos de riesgos: Los riesgos pueden incluir malware, phishing, ataques de denegación de servicio (DDoS), robo de datos y violaciones de privacidad, entre otros.
- Impacto de los incidentes: Los incidentes de seguridad pueden tener consecuencias graves, como la pérdida de datos sensibles, interrupciones en la operación de la organización y daños a la reputación de la marca.
- Importancia de la prevención: La prevención es clave para evitar incidentes de seguridad costosos y dañinos. Esto incluye la implementación de controles de seguridad adecuados y la concienciación de las personas sobre las mejores prácticas de seguridad.

INOVA

II- HERRAMIENTAS Y MECANISMOS DE PROTECCIÓN

- Enfoque centrado en las personas:
- importancia de la seguridad digital de las personas dentro de las organizaciones, las personas son uno de los eslabones más débiles en términos de ciberseguridad.
- cultura de seguridad en toda la organización, cada individuo entienda su papel en la protección de los activos digitales y esté comprometido con prácticas seguras en línea.
- las políticas y procedimientos de seguridad debe abordar la seguridad digital de las personas, enfocándose en la capacitación en reconocimiento de amenazas.

INOVA

II- HERRAMIENTAS Y MECANISMOS DE PROTECCIÓN

- La perspectiva personal:

- Evaluación de hábitos de seguridad:
  - hábitos de seguridad en línea y a identificar áreas donde se puede mejorar, como el uso de contraseñas seguras o la protección de dispositivos.
- Importancia de la concienciación:
  - la ciberseguridad es responsabilidad de todos, cada individuo puede contribuir a mejorarla mediante prácticas seguras en línea.

INOVA

II- HERRAMIENTAS Y MECANISMOS DE PROTECCIÓN

Uso seguro del correo electrónico:

- Identificación de correos electrónicos sospechosos:
  - Los usuarios deben estar alerta ante correos electrónicos no solicitados, especialmente aquellos que solicitan información personal o financiera.
- Verificación de remitentes:
  - Antes de hacer clic en enlaces o descargar archivos adjuntos, es importante verificar la autenticidad del remitente y la legitimidad del correo electrónico.
- Uso de filtros de correo no deseado:
  - Configurar filtros de spam en el cliente de correo electrónico puede ayudar a reducir la cantidad de correos electrónicos no deseados y maliciosos que llegan a la bandeja de entrada.

INOVA

II- HERRAMIENTAS Y MECANISMOS DE PROTECCIÓN

Navegación segura en Internet:

- Verificación de sitios web:
  - Antes de proporcionar información personal o financiera en un sitio web, es importante verificar que el sitio sea seguro y legítimo, buscando el candado verde en la barra de direcciones.
- Evitar descargas no seguras:
  - Se debe tener cuidado al descargar archivos de sitios web no verificados, ya que pueden contener malware u otros programas maliciosos.
- Uso de conexiones seguras:
  - Al realizar transacciones en línea o ingresar información confidencial, se debe utilizar una conexión segura mediante HTTPS para proteger los datos en tránsito.

INOVA

II- HERRAMIENTAS Y MECANISMOS DE PROTECCIÓN

Seguridad en redes sociales:

- Privacidad de la información:
  - Ajustar la configuración de privacidad en las redes sociales para limitar la cantidad de información personal visible para el público en general.
- Reconocimiento de estafas:
  - Estar alerta ante posibles estafas en redes sociales, como solicitudes de amistad de personas desconocidas o mensajes que solicitan información personal.
- Gestión de cuentas:
  - Mantener las cuentas de redes sociales seguras mediante el uso de contraseñas fuertes y la activación de la autenticación de dos factores cuando esté disponible.

INOVA

II- HERRAMIENTAS Y MECANISMOS DE PROTECCIÓN

Seguridad en dispositivos móviles:

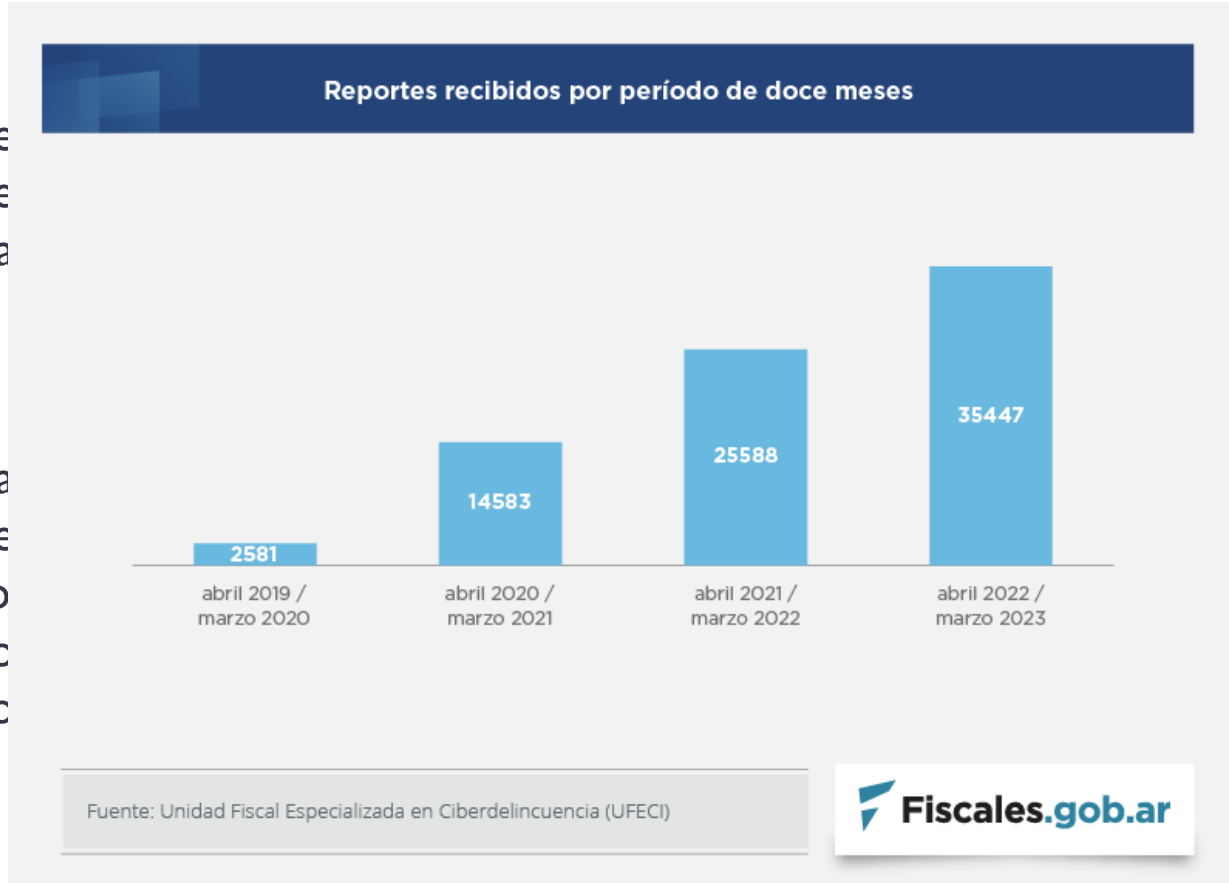
- Actualizaciones de software:
  - Mantener actualizado el sistema operativo y las aplicaciones en dispositivos móviles para protegerse contra vulnerabilidades conocidas.
- Aplicaciones de seguridad:
  - Utilizar aplicaciones de seguridad móvil, como antivirus y antimalware, para escanear y proteger el dispositivo contra amenazas.
- Respaldo de datos:
  - Realizar copias de seguridad periódicas de los datos almacenados en dispositivos móviles para protegerlos en caso de pérdida o robo del dispositivo.

INOVA

III - CIBERDELITO

Qué es un delito informático:

- Un delito informático es cualquier actividad ilegal que involucra el uso de una computadora o una red de computadoras como herramienta principal, ya sea para cometer un crimen o para facilitar su perpetración.
- Ley 26.388 de Delitos Informáticos del 2008
- incorporar diversos delitos informáticos, tales como: la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.



INOVA

III - CIBERDELITO

Delitos contra menores

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 Código Penal)
- Se suma en 2013 Ley 26.904 –Grooming

Protección de la privacidad

- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1 Código Penal)
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2 Código Penal)
- Acceso a un sistema o dato informático (art. 153 bis Código Penal)
- Publicación de una comunicación electrónica (art. 155 Código Penal)
- Acceso a un banco de datos personales (art. 157 bis, párrafo 1 Código Penal)
- Revelación de información registrada en un banco de datos personales (art. 157 bis, párrafo 2 Código Penal)
- Inserción de datos falsos en un archivo de datos personales (art. 157 bis, párrafo 2 Código Penal)

INOVA

III - CIBERDELITO

Delitos contra la propiedad

- Fraude informático (art. 173, inciso 16 Código Penal)
- Daño o sabotaje informático (art. 183 y 184, incisos 5 y 6 Código Penal)

Delitos contra las comunicaciones

- Interrupción o entorpecimiento de comunicaciones electrónicas o telecomunicaciones (art. 197 Código Penal)

Delitos contra la administración de justicia

- Sustracción, alteración, ocultación, destrucción o inutilización de objetos destinados a servir de prueba, registros o documentos confiados a la custodia. (art. 255 Código Penal)

INOVA

III – CIBERDELITO - CIBERATAQUES

1. Ransomware

- Es un software que infecta a las computadoras y muestra mensajes que exigen el pago de dinero para restablecer el acceso a la misma.

2. Ataques a dispositivos IoT

- El Internet de las cosas (IoT) es todo objeto físico, vehículos, electrodomésticos entre otros que comparte datos a través de Internet.

3. Phishing e ingeniería social

- Es la combinación de Ingeniería Social y exploits técnicos, diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante, atreves de una página web falsa.

INOVA

III – CIBERDELITO - CIBERATAQUES

4. Ataque a redes LAN inalámbricas

- este ataque se basa en utilizar herramientas conjuntamente con ingeniera social para tratar de acceder a una red inalámbrica

5. Ataque de denegación de servicio (DOS o DDOS)

- es un ataque que busca privar a los usuarios de acceso a su red o equipo, se provocan al generar grandes cantidades de información desde varios puntos de forma voluntaria, para que el usuario o la organización se vean privados de un recurso.

6. Suplantación de identidad y Sybil

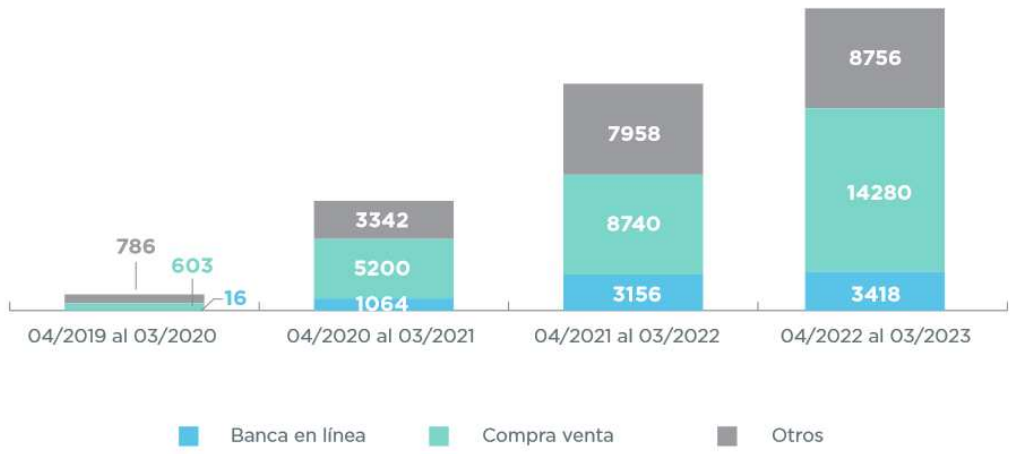
- Es la modalidad mediante la cual una persona suplanta a otra en la titularidad de un derecho con un fin en particular, mediante un medio electrónico.

7. Otros malware , virus, troyanos, spyware, backdoor y demás.

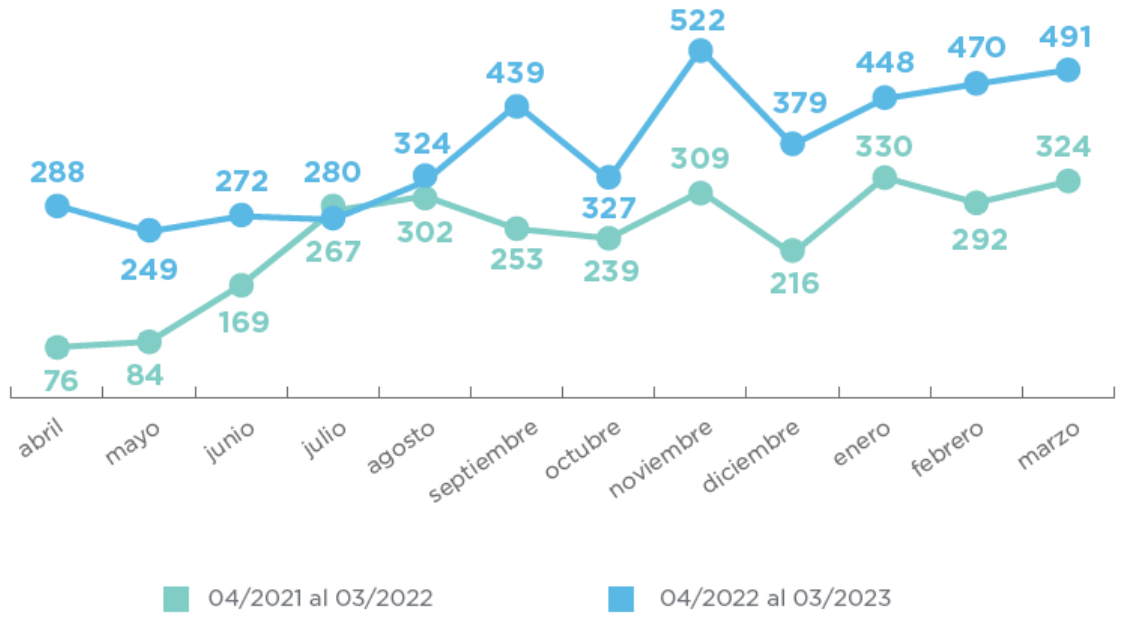
INOVA

III – CIBERDELITOS
EVOLUCIÓN DE CASOS DE FRAUDE EN LÍNEA

Fraude en línea



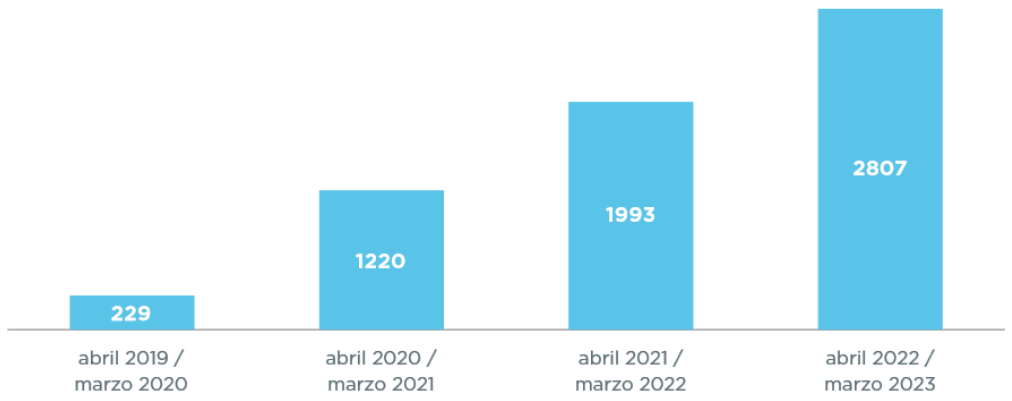
Usurpación de identidad



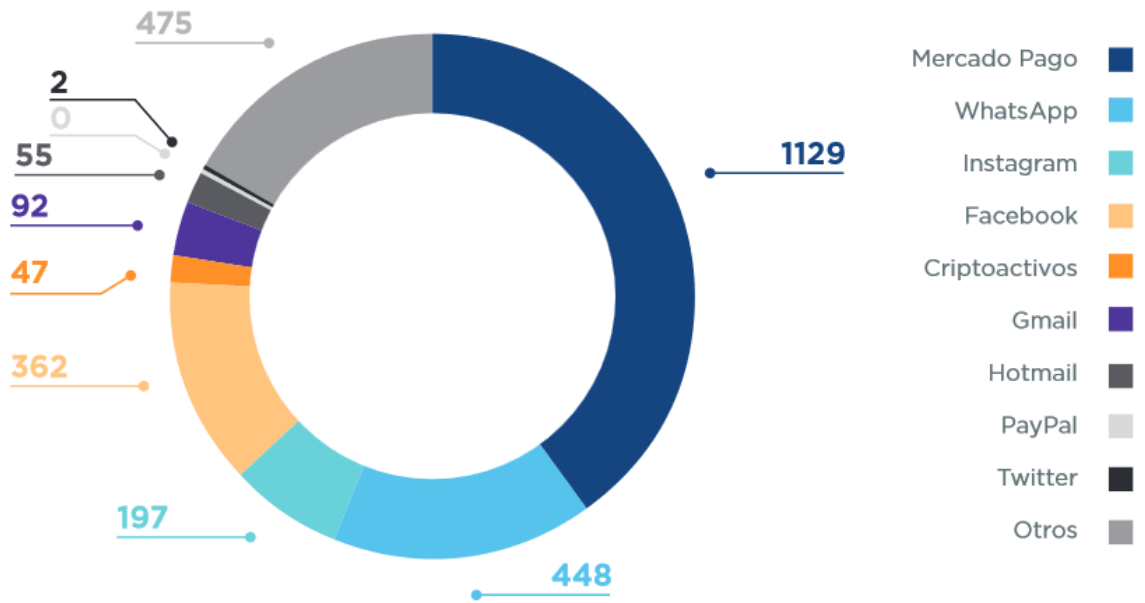
INOVA

III – CIBERDELITOS
EVOLUCIÓN DE CASOS DE ACCESO ILEGAL

Acceso ilegítimo



Abril de 2022 a Marzo de 2023



INOVA

III – CIBERDELITOS
ACTORES

- Hackers

- Ciber Criminales: Grupos organizados o individuos que realizan actividades delictivas en línea, como el fraude financiero, la extorsión y la distribución de malware con el objetivo de obtener ganancias económicas.
- Actores estatales: Gobiernos o agencias gubernamentales que participan en operaciones cibernéticas con fines políticos, militares o de espionaje.

INOVA

III – CIBERDELITOS
¿CÓMO PROTEGERSE?

- Educación y concienciación: Capacitar a las personas sobre los diferentes tipos de ciberdelitos y cómo reconocer y evitar posibles amenazas.
- Uso de herramientas de seguridad: Utilizar software antivirus, firewalls y otras herramientas de seguridad cibernética para protegerse contra amenazas en línea.
- Prácticas de seguridad: Adoptar prácticas de seguridad sólidas, como usar contraseñas fuertes, mantener el software actualizado y evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes no confiables.

INOVA

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Sistemas de gestión de la seguridad de la información:

- Un sistema de gestión de la seguridad de la información (SGSI) es un marco de políticas y procedimientos diseñado para proteger la información de una organización contra amenazas cibernéticas.
- El SGSI puede incluir la identificación de activos de información, la evaluación de riesgos, la implementación de controles de seguridad y la monitorización continua de la seguridad de la información.

INOVA

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN FACTORES

- Tecnología: La tecnología desempeña un papel fundamental en la seguridad de la información, proporcionando herramientas y soluciones para proteger los sistemas y datos contra amenazas cibernéticas.
- Personas: La capacitación y concienciación de las personas son importantes para garantizar que todos comprendan la importancia de la seguridad de la información y cumplan con las políticas y procedimientos establecidos.
- Políticas organizacionales: Las políticas y procedimientos de seguridad establecidos por una organización proporcionan el marco para proteger la información y guiar las acciones de las personas en materia de seguridad cibernética.

INOVA

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN RESPONSABILIDADES

- Roles y responsabilidades: Es importante definir claramente los roles y responsabilidades de cada individuo dentro de una organización en lo que respecta a la seguridad de la información, incluyendo la asignación de responsabilidades específicas para la gestión y protección de datos.

- Supervisión y cumplimiento: La supervisión y el cumplimiento de las políticas de seguridad son fundamentales para garantizar que se sigan los procedimientos establecidos y que se tomen medidas correctivas cuando sea necesario.

INOVA

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

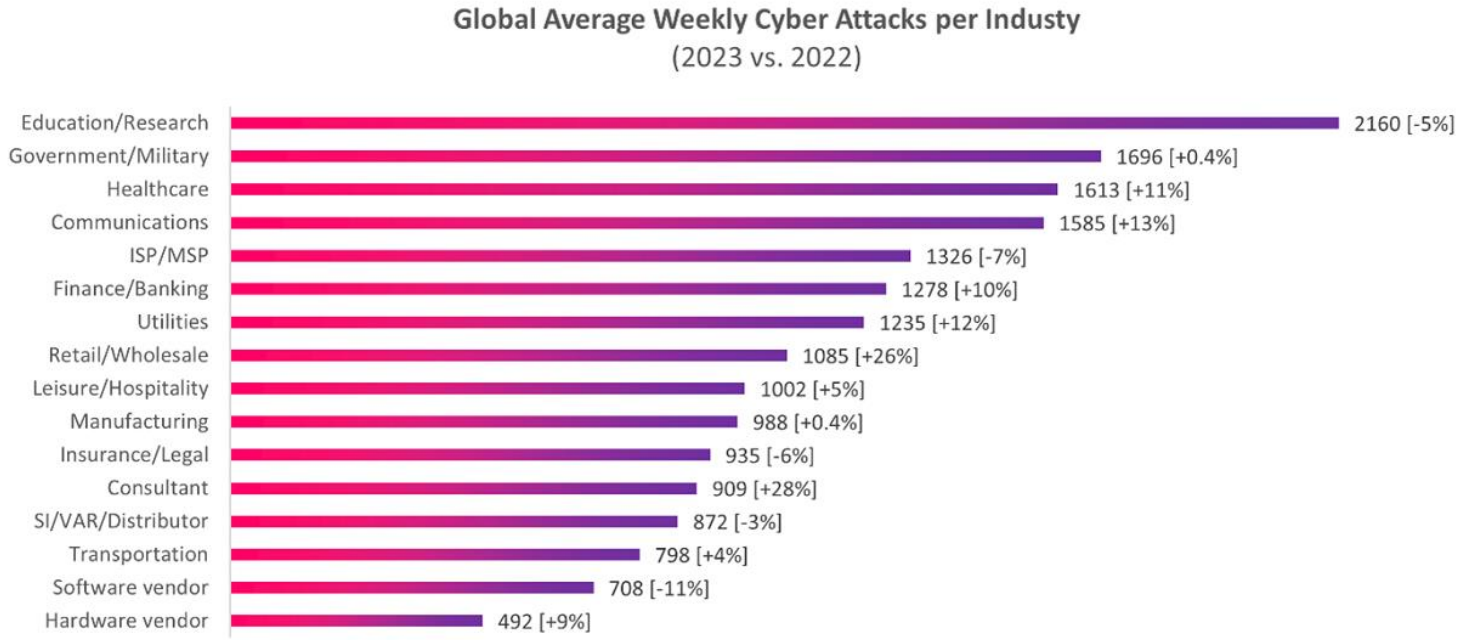
- Impacto en la reputación: Los incidentes de seguridad pueden dañar la reputación de una organización y afectar la confianza.

- Consecuencias legales: Las organizaciones pueden enfrentar consecuencias legales por la gestión inapropiada de la seguridad de la información, incluyendo multas, sanciones y responsabilidad civil.

INOVA

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Según el último informe de Check Point Software, en 2023 ha habido un incremento del 3% en el número de ciberataques semanales en todo el mundo, con un aumento del 4% en los ataques de ransomware y un crecimiento del 11% en los que se dirigen al sector de la salud.



Fuente: https://www.itdigitalsecurity.es/actualidad/2023/11/las-empresas-reciben-una-media-de-1200-ciberataques-por-semana

INOVA

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

EL PAÍS SUSCRÍBETE

Economía

MERCADOS · VIVIENDA · FORMACIÓN · MIS DERECHOS · NEGOCIOS · CINCO DÍAS · RETINA · ÚLTI

ATAQUES CIBERNÉTICOS >

El Fondo Monetario Internacional sufre un ciberataque

El incidente ocurrió el 16 de febrero y comprometió 11 cuentas de correo electrónico vinculadas al organismo

La Voz 120 años

Política / PAMI

Hackeo al Pami: ciberdelincuentes publicaron la información robada

La organización ransomware Rhysidaque pedía una alta cifra de dinero para devolver los datos. El pago no se realizó y fueron filtrados más de 1.6 millones de archivos en la dark web.

19 de agosto de 2023, 23:36

WIRED

SEGURIDAD 8 DE MAYO DE 2024

La (extraña) entrevista a los *hackers* rusos que quieren atacar el suministro de agua de EE UU

infobae

SOCIEDAD >

Le hackearon el WhatsApp a su abuelo, intentaron estafarlo y les terminó sacando dinero a los delincuentes

El joven, de la localidad de Merlo, se avivó de la maniobra, en la que le pedían 40 mil pesos y usó un ardid para timar a los hackers

INNOVA

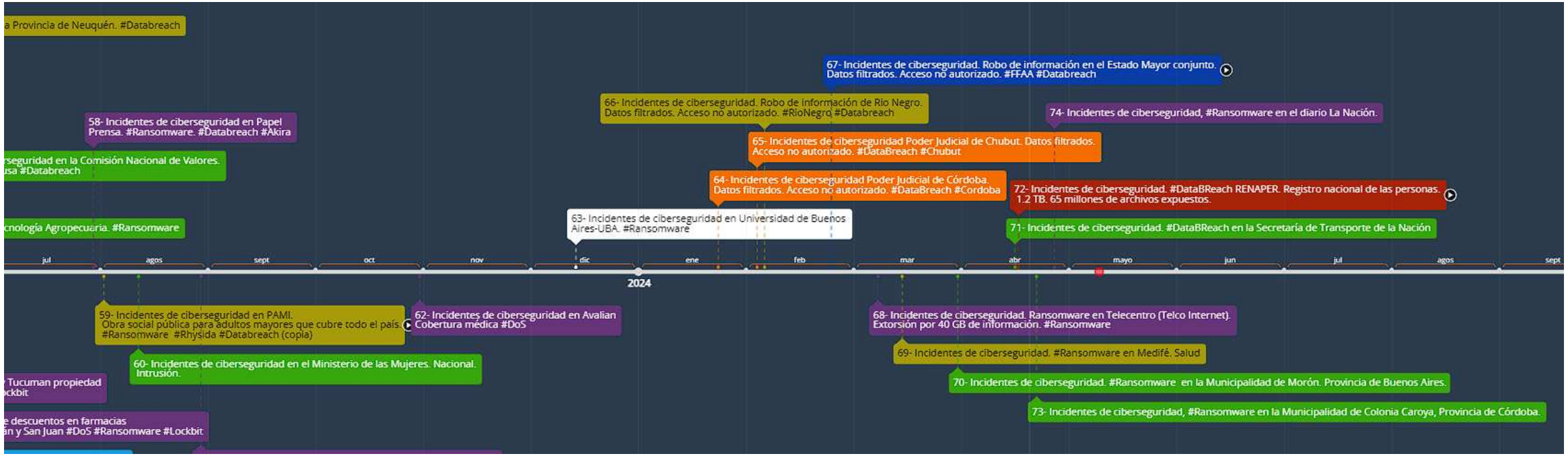
LA NACION > Seguridad

Sin fondos. Hackearon la cuenta bancaria de una comuna santafesina y se robaron 20 millones de pesos

El dinero se iba a utilizar para pagar los sueldos de los empleados públicos y de diferentes proveedores

23 de abril de 2024 • 16:37

IV: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
CIBERINCIDENTES RELEVANTES EN ARGENTINA



Fuente: https://time.graphics/es/line/630567

INOVA

CONCLUSIONES

La ciberseguridad es un aspecto fundamental en el mundo digital en el que vivimos hoy en día. Desde proteger nuestra información personal hasta salvaguardar los activos digitales de las organizaciones, la ciberseguridad juega un papel crucial en la protección contra una amplia gama de amenazas en línea.

INOVA

GRACIAS.

¿PREGUNTAS?