UNIVERSIDAD DE BUENOS AIRES

**FACULTADES DE CIENCIAS ECONÓMICAS,
CIENCIAS EXACTAS Y NATURALES E INGENIERÍA**

CARRERA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

TRABAJO FINAL

Ataques a la confidencialidad de los datos personales en organismos públicos argentinos

AUTOR: Lic. PABLO OSCAR VAIRA

TUTORA: Mag. Dra. MARÍA PATRICIA PRANDINI

COHORTE 2022

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO: PABLO OSCAR VAIRA DNI 17.475.706

Resumen

Esta investigación se enfoca principalmente en analizar, evaluar y brindar algunos lineamientos para concientizar acerca de los ciberataques más relevantes registrados en organismos públicos argentinos, sobre la base de información pública obtenida a través de páginas web de organismos oficiales, medios de prensa, documentaciones de tecnología, publicaciones en revistas de ciberseguridad y seguridad de la Información y estadísticas referidas al tema.

En su primera parte se enumerarán los tipos de ataques conocidos y los efectos que ellos producen y se explicarán las maneras de prevenir las situaciones perjudiciales relacionadas con estos tipos de ataques.

A continuación, se mencionará la normativa vigente en materia de Seguridad de la información y sus implicancias respecto a la obligatoriedad de reportar o denunciar incidentes.

Se expondrán también casos de ciberataques ocurridos en la Argentina, las causas o debilidades que permitieron su ocurrencia y sus posibles formas de prevención, y se analizarán las vulnerabilidades habituales que facilitaron la explotación.

Por último, a modo de conclusiones, se hará referencia a las situaciones que dieron lugar a los citados incidentes y cómo se deberían encarar líneas de acción, a manera de recomendaciones basadas en conocimientos adquiridos durante la Especialización en Seguridad Informática y a partir de experiencias profesionales del autor.

ÍNDICE

1 INTRODUCCIÓN

1.1 Conceptos previos

La información es un activo importante con el que cuentan los organismos públicos para satisfacer sus objetivos y por lo tanto, es crítica para su desempeño y subsistencia y para el bien común. Por este motivo, es fundamental tener presente que existen amenazas que pueden afectarla. Es por ello que deben tomarse recaudos e implementar controles para protegerla.

Para abordar la complejidad del proceso de seguridad de la información, deben tenerse presente ciertos conceptos que explican cómo puede originarse un riesgo y qué efectos puede provocar.

Cuando en el ámbito de la seguridad informática mencionamos el concepto de incidentes, nos referimos a aquellos eventos adversos en un entorno informático, que pueden comprometer o comprometen la confidencialidad, integridad y/o disponibilidad de la información, así como también las amenazas inminentes de violación o las violaciones concretas de una política de seguridad de la información, de políticas de uso aceptable o de mejores prácticas de seguridad.

Si en una dependencia pública alguien accediera, sin la debida autorización, a la información personal que se tiene de los ciudadanos o de los empleados del organismo (por ejemplo, ingresos anuales, deudas impositivas, domicilio o historia clínica, entre otras), podríamos imaginar una serie de riesgos que afectarían a las instituciones y que podrían impactar negativamente en la vida cotidiana de las personas.

En estos casos, se entiende que debe protegerse no solo la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

La propiedad por la cual se garantiza el acceso a la información sólo a aquellas personas autorizadas para evitar su divulgación inapropiada se denomina **confidencialidad**.

Si se alteraran los datos contenidos en nuestras PC o se cambiara su configuración, sin la debida directiva o autorización, seguramente en muchos casos, esto tendría graves consecuencias para nosotros, para el organismo y/o para terceros. Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo, sino que también se deben considerar otros elementos como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc. La propiedad por la cual se garantiza la protección contra modificaciones no autorizadas para evitar su alteración de la información se denomina **integridad**.

Supongamos ahora que un organismo publica información importante en su sitio web, como por ejemplo vencimientos de pagos o instrucciones para realizar un trámite complicado como presentación en línea de declaraciones juradas y alguien impide de algún modo, el acceso a dicho sitio. De nada sirve la información si se encontrara intacta en el sistema, pero los usuarios no podrían acceder a ella. Proteger la información también significa garantizar que se pueda ser visualizada y utilizada en tiempo y forma para aquellas personas autorizadas, de manera que puedan llevar adelante sus objetivos y actividades. Esta propiedad se conoce como **disponibilidad**.

1.2 Tipos de Ataques

Teniendo en cuenta el hecho de que podrían existir distintos puntos de vista relacionados con la forma de categorización de los ataques, especialmente cuando se relacionan con algún tipo de código malicioso, se aclara que en este punto se utiliza un criterio de clasificación vinculado a su funcionalidad y a la manera en que afecta a los activos de información.

De esa forma, a continuación se describen una serie de ciberataques habituales en la actividad, que comprometen una o varias de las actividades antes mencionadas.

1.2.1 Denegación de Servicio *(DOS)*

Este tipo de incidente se registra cuando un atacante intenta evitar que los usuarios legítimos accedan a información o a servicios disponibles. La sigla responde a la expresión Denegación de Servicios o *Denial of Service*, en idioma inglés.

El tipo más común de ataque ocurre cuando un actor malicioso "inunda" una red con información. Cuando escribimos una URL de un sitio web, en nuestro navegador, estamos enviando una solicitud al servidor web del sitio para poder ver la página en concreto o acceder a un servicio. El servidor solo puede procesar una cierta cantidad de solicitudes por vez, por lo que si un atacante sobrecarga el servidor con solicitudes, causa una inhabilitación para responder cualquier petición o requerimiento. En otras palabras, se produce una "denegación de servicio" ya que no se puede acceder al sitio, comprometiendo fundamentalmente la disponibilidad de la información y los servicios.

1.2.2 Phishing

Es un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza y haciéndose pasar por una persona, entidad, organización, empresa o servicio de confianza. En otras palabras, se produce una suplantación de identidad de un tercero de confianza, con el objetivo de manipular a la víctima y lograr que realice acciones que no debería realizar (por ejemplo, revelar información confidencial o hacer click en un enlace).

Esto se puede dar, a modo de ejemplo, enviando correos electrónicos o mostrando publicidades a la víctima diciéndole que ha ganado un premio y que haga clic en un enlace para recibirlo, siendo estas promesas falsas. Habitualmente el objetivo es robar información, pero otras veces es instalar malware, sabotear sistemas o robar dinero a través de fraudes, entre otros motivos.

Este tipo de ataques puede comprometer las 3 características de la seguridad de la información, ya que partiendo de un intento de manipulación y como ya se explicó, puede hacer que el usuario divulgue información restringida (confidencialidad), modifique un dato (integridad) o instale un código malicioso de tipo ransomware (ver sección siguiente) en forma involuntaria (disponibilidad).

1.2.3 Ransomware

Es un tipo de programa dañino que impide el acceso a determinadas partes o archivos del sistema operativo infectado o a servicios afectados y pide un rescate a cambio de quitar esta restricción. Algunos tipos de *ransomware* cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate, lo que en principio comprometería la disponibilidad de la información, aunque podría extenderse a afectar la integridad y la confidencialidad, dependiendo el caso.

Aunque los ataques se han hecho populares desde mediados de la década del 2010, el primer ataque conocido fue realizado a finales de la década de los 80, por el Dr. Joseph Popp. Su uso creció internacionalmente a partir de junio del 2013 y se incrementó notablemente durante la reciente pandemia de COVID-19.

1.2.4 Data Breach

Es una infracción de la seguridad en la que datos sensibles, protegidos o confidenciales son copiados, transmitidos, vistos,

robados o utilizados por una persona no autorizada para hacerlo. Otros términos son divulgación involuntaria de información, fuga de datos, fuga de información o derrame de datos. Los incidentes van desde los ataques concertados de individuos que piratean en beneficio personal o con malicia *(black hats*), el crimen organizado, los activistas políticos o los gobiernos nacionales, hasta la seguridad de sistemas mal configurados o la eliminación descuidada de equipos informáticos o soportes de almacenamiento de datos usados, afectando su confidencialidad y en algunos casos, su disponibilidad.

La información filtrada puede abarcar desde asuntos que comprometen la seguridad nacional hasta información sobre acciones que un gobierno o funcionario considera vergonzosas y quiere ocultar.

1.2.5 Ping Flood

Se basa en enviar a la víctima una cantidad abrumadora de paquetes ping, usualmente usando el comando "ping" de UNIX como hosts (el indicador -t en los sistemas Windows tiene una función mucho menos maligna). Es muy simple de lanzar, el requisito principal es tener acceso a un ancho de banda mayor que la víctima.

1.2.6 *Ping* de la muerte

El atacante envía un paquete *ICMP* (del inglés *Internet Control Message Protocol* o Protocolo de Mensajes de Control de Internet, por su traducción al español) de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo. Hoy en día, la mayoría de los sistemas operativos descartan dichos paquetes por sí mismos. No obstante es dable mencionarlo ya que podría afectar versiones antiguas de dichos sistemas. Este tipo de ataque podría vulnerar la disponibilidad y la integridad de la información.

1.2.7 Escaneo de puertos

El escaneo de puertos es una de las técnicas de reconocimiento más populares que utilizan los atacantes para descubrir los servicios expuestos a posibles ataques. Todas las máquinas conectadas a una red de área local (*LAN*) o Internet ejecutan muchos servicios que escuchan en puertos conocidos y no tan conocidos. Un escaneo de puertos ayuda al atacante a encontrar qué puertos están disponibles.

Esencialmente, un escaneo de puertos consiste en enviar un mensaje a cada puerto, uno a uno. El tipo de respuesta recibida indica si el puerto está a la escucha y, por lo tanto, puede probarse más detalladamente para detectar debilidad, pudiendo afectar la confidencialidad de la información. Se clasifican en:

- Puertos conocidos (0 - 1023)
- Puertos registrados (1024 - 49151)
- Puertos dinámicos y / o privados (49152 - 65535)

1.2.8 ARP Spoofing

ARP (del inglés *Address Resolution Protocol* o Protocolo de Resolución de Direcciones, en español*) Spoofing e*s una técnica utilizada para atacar una red cableada o inalámbrica de *Ethernet. ARP Spoofing* permite que un atacante detecte *frameworks* de datos en una red de área local *(LAN*), modifique el tráfico o lo detenga por completo. El ataque solo se puede usar en redes que realmente usan el protocolo *ARP* y no en otro método de resolución de direcciones IP.

La detección se realiza mediante *ARP* inverso (*RARP, Reverse ARP*) que es un protocolo utilizado para consultar la dirección IP asociada con una dirección MAC dada. Si se devuelve más de una dirección IP, la clonación MAC está presente, incidiendo en la disponibilidad de los datos.

Los tipos de ataques *ARP Spoofing* más conocidos son:

- Ataque de inundación *MAC*
- Envenenamiento de caché *DNS*
- *IP Spoofing*

1.2.9 Man-In-The-Middle

Un ataque MITM (del inglés *Man In The Middle* u hombre en el medio, por su traducción al español) ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa. Esto puede suceder en cualquier forma de comunicación en línea, como correo electrónico, redes sociales, navegación web, etc. No solo están tratando de escuchar nuestras conversaciones privadas, sino que también pueden dirigir toda la información dentro de los dispositivos.

Más allá de los detalles técnicos, el concepto de un ataque MITM se puede describir en un escenario simple. Si imaginamos que volvemos a los tiempos antiguos cuando el uso del correo postal era más frecuente, imaginemos que Ernesto le escribe una carta a Susana en la que le expresa su amor después de años de ocultar sus sentimientos. Él envía la carta a la oficina de correos, en la que es recogida por un cartero entrometido. La abre y por puro gusto, decide reescribir la carta antes de entregar el correo a Susana, cambiando su sentido original. Esto puede hacer que Susana odie a Ernesto por el resto de su vida.

Un ejemplo más moderno sería un hacker entre nuestro navegador y el sitio web que una persona está visitando, que busca interceptar y capturar cualquier información que se envíe al sitio, como credenciales de inicio de sesión o información financiera, lo que comprometería las tres características de la Seguridad de la Información: la confidencialidad, la integridad y la disponibilidad.

1.2.10 Ingeniería Social

Figura 1 - Ataque de Ingeniería Social

La ingeniería social es el arte de manipular a las personas para que entreguen voluntariamente información confidencial. Los tipos de información que buscan estos delincuentes puede variar, pero cuando los individuos son blanco, generalmente intentan engañarlos para que le den su contraseña o información bancaria, o permitan acceder a su PC para instalar software malicioso, que le dará acceso a información personal u obtener control sobre el recurso.

Los delincuentes usan tácticas de manipulación porque generalmente es más fácil explotar la inclinación natural a confiar que descubrir formas de *hackear* tu *software*. Por ejemplo, es mucho más fácil engañar a alguien para que le dé su contraseña que intentar piratearla (a menos que la contraseña sea realmente débil).

Sin dudas, el eslabón más débil en la cadena de seguridad es el ser humano que acepta a una persona o un escenario al pie de la letra, sin preguntarse en la mayoría de los casos, si existe un peligro en lo que está haciendo. No importa cuántas cerraduras y cerrojos hay en nuestras puertas y ventanas, o si tenemos perros guardianes, sistemas de alarma, reflectores, cercas con alambre de púas y

personal de seguridad armado. Si confiamos en la persona de la puerta que dice que él es el repartidor de pizzas y lo dejamos entrar sin verificar primero si es legítimo, estamos completamente expuestos a cualquier riesgo que represente dejarle entrar. Lo mismo ocurre en el mundo virtual. Este tipo de ataque viola fundamentalmente la confidencialidad de la información.

1.2.11 *OS Fingerprinting*

El término en español "huella digital del sistema operativo" (*OS Finger Printing,* en inglés) se refiere a cualquier método utilizado para determinar qué sistema operativo se ejecuta en una computadora remota. Al analizar ciertos indicadores de protocolo, opciones y datos en los paquetes que un dispositivo envía a la red, podemos hacer conjeturas relativamente precisas sobre el sistema operativo que envió esos paquetes. Al identificarlo en forma precisa, un atacante puede lanzar un ataque certero contra un host o equipamiento destino. En un mundo de desbordamientos de búfer, conocer la característica y la arquitectura exactos de un sistema operativo podría ser toda la oportunidad que un atacante necesita, pudiendo impactar en la integridad y la confidencialidad de los datos.

1.2.12 KeyLoggers

Un *keylogger* (derivado del inglés: *key* ('tecla') y *logger* ('registrador'); en español “registrador de teclas”) es un programa de software o una pieza de hardware que utiliza un atacante para registrar las pulsaciones de teclas en el teclado de un usuario. Con un Keylogger, un atacante puede conocer remotamente sus contraseñas, números de tarjetas de crédito o débito, mensajes, correos electrónicos y todo lo que escriba la víctima, impactando sobre la confidencialidad de los datos

Es más probable que los registradores de pulsaciones de teclas estén basados en software que en hardware, ya que estos últimos requerirían que el atacante tenga acceso físico al dispositivo en algún momento.

Los registradores de pulsaciones basados en software generalmente infectan el sistema en forma de un malware que un usuario podría haber descargado inadvertidamente haciendo clic en un enlace malicioso, ya sea en línea a través de Internet o enviado por correo electrónico.

Un software de captura de pulsaciones se ejecuta en segundo plano sin notificar al usuario y tomará nota de cada golpe de teclado. Luego lo alimentará en un servidor en línea al que puede acceder el atacante.

Revisar todo el historial de registros de teclas puede brindarle a cualquier atacante una idea de los sitios web que visitó la víctima y la información que ingresó en ellos, lo que le da una forma fácil de acceder a datos de la tarjeta de crédito o credenciales de banca por Internet. Los ataques de teclado son utilizados por personas maliciosas con la intención de monitorear las pulsaciones de teclas, siendo importante protegerse contra ellos, para que no seamos vulnerables a perder información de identificación personal, incluidas las credenciales personales o corporativas.

1.2.13 *ICMP Tunneling*

El protocolo de mensajes de control de Internet (del inglés *Internet Control Message Protocol) Tunneling* se usa a menudo para eludir los firewalls que no bloquean los paquetes *ICMP* o para establecer un canal de comunicación cifrado y difícil de rastrear entre dos computadoras sin interacción directa de la red. Un túnel *ICMP* establece una conexión encubierta entre dos computadoras remotas (un cliente y un proxy), utilizando solicitudes de eco *ICMP* y paquetes

de respuesta. Un ejemplo de esta técnica es tunelizar el tráfico *TCP* completo a través de peticiones y respuestas de *ping*, alterando la confidencialidad y la integridad de la información.

1.2.14 Secuencia *TCP*

Un ataque de predicción de secuencia *TCP* (Protocolo de control de transmisión o *Transmission Control Protocol*, en inglés) es un intento de predecir el número de secuencia utilizado para identificar los paquetes en una conexión TCP, que se puede usar para duplicar paquetes que conducen al secuestro de la sesión.

En un escenario típico de ataque de predicción de secuencia *TCP*, un atacante pasaría algún tiempo monitorizando el flujo de datos entre dos hosts, uno de los cuales es el sistema de destino. El atacante cortaría el otro sistema (que es confiable para el objetivo) de la comunicación, tal vez a través de un ataque de denegación de servicio (*DOS*), tomando el lugar de ese sistema confiable para lograr su objetivo.

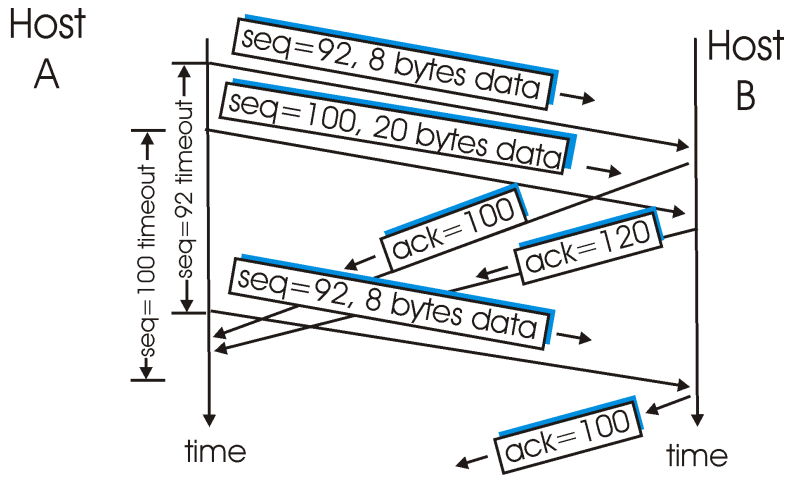

Figura 2 - Secuencia TCP

Habiendo predicho el número de secuencia del siguiente paquete que el objetivo espera de su host de confianza, el atacante prepara un paquete con la dirección IP de origen del sistema de

confianza y el número de secuencia esperado. Este paquete llegará a su destino antes que cualquier información legítima del host confiable (sobre el que generalmente se realiza un ataque DOS para mantenerlo ocupado y fuera de la atención). El paquete del atacante se puede usar como una vía para obtener acceso al sistema de destino, terminar a la fuerza una comunicación o entregar una carga maliciosa, comprometiendo fundamentalmente la disponibilidad de la información.

1.2.15 CAM Table Overflow

La tabla *CAM* (del inglés *Content-Addressable Memory,* en español “Memoria de Contenido Direccionable”) de una red Ethernet contiene información de red, como las direcciones *MAC* disponibles en los puertos físicos del conmutador y los parámetros de VLAN asociados. Los desbordamientos de la tabla *CAM* ocurren cuando una entrada de direcciones MAC se inunda en la tabla y se alcanza el umbral de la tabla *CAM*. Esto hace que el computador actúe como un concentrador, inundando la red con tráfico fuera de todos los puertos. La inundación causada por un desbordamiento de tabla *CAM* está limitada a la *VLAN* de origen. Por lo tanto, no afecta a otras *VLAN* en la red, pero compromete la disponibilidad de los datos.

Se conocen dos tipos de ataque de este estilo:

- Ataque de redireccionamiento *ICMP* y
- Ataque de transferencia de zona *DNS*

1.2.16 Inyección *SQL*

*SQL (*en inglés: *Structured Query Language,* en español: Lenguaje de Consulta Estructurado*) Injection* (Inyección) *es* un método de infiltración de código intruso que se vale de una

vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

El origen de la vulnerabilidad radica en la incorrecta comprobación o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL. Es, de hecho, un error de una clase más general de vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o script que esté incrustado en otro.

Se conoce como Inyección *SQL*, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código *SQL* intruso y a la porción de código incrustado, por lo que con ello, dependiendo el caso, se podría llegar a vulnerar las tres características de la seguridad de la Información: la confidencialidad, la integridad y la disponibilidad.

1.2.17 *Cross-site Request Forgery*

CSRF (del inglés: Cross-Site Request Forgery), en español: Falsificación de Petición en Sitios Cruzados, es un ataque que falsifica una petición a un servidor web haciéndose pasar por un usuario de confianza. Esto se puede hacer, por ejemplo, incluyendo parámetros maliciosos en una URL, después de un enlace que pretende redirigir a otro sitio.

Se trata de un tipo de exploit malicioso de un sitio web, mediante el cual se transmiten comandos no autorizados de un usuario en el que el sitio web confía. *CSRF* explota la confianza que un sitio tiene en el navegador de un usuario, vulnerando fundamentalmente la confidencialidad de la información, aunque dependiendo del script, podría llegar a alterar también la integridad y la disponibilidad.

1.2.18 Envenenamiento o Robo de *cookies*

Los ataques por envenenamiento de *cookies* implican la modificación de los contenidos de una *cookie* (información personal almacenada en la computadora de un usuario web) para eludir los mecanismos de seguridad. Al usar ataques de envenenamiento de *cookies*, los atacantes pueden obtener información no autorizada sobre otro usuario y robar su identidad, impactando sobre la confidencialidad y la integridad de los datos.

El robo de *cookies* se realiza mediante *scripts* del lado del cliente, como *JavaScript*. Cuando el usuario hace clic en un enlace, el *script* buscará la cookie almacenada en la memoria de la computadora para todas las cookies activas y las enviará al atacante, interfiriendo en la confidencialidad y la integridad de la información.

1.2.19 *Buffer overflow*

El desbordamiento de búfer, o el desbordamiento del búfer, del inglés: *Buffer overflow*, es una anomalía en la que un proceso almacena datos en un búfer fuera de la memoria que el programador reservó para ello. Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. Esta vulnerabilidad es completamente un error del Programador, que afecta a la integridad y la disponibilidad de los datos.

1.2.20 Exploración forzada

La exploración forzada es un ataque cuyo objetivo es enumerar y acceder a los recursos a los que la aplicación no hace

referencia, pero que aún son accesibles. Por ejemplo, directorios como *config*, *backup* o *logs,* a los que se puede acceder, pueden revelar mucha información sobre la aplicación en sí, como por ejemplo: contraseñas, actividades y servicios, entre otros. Este ataque impacta mayormente sobre la confidencialidad de la información, aunque dependiendo de la aplicación afectada, podría también afectar su integridad y disponibilidad.

1.2.21 Virus-Gusanos

Un virus informático es un programa digital que puede copiarse e infectar una computadora. El término "virus" también se usa comúnmente pero erróneamente para referirse a otros tipos de *malware*, incluidos, entre otros, los programas de *adware* y *spyware* que no tienen la capacidad reproductiva. Un virus verdadero puede propagarse de una computadora a otra (en algún tipo de código ejecutable) cuando el aplicativo o archivo infectado se lleva a la computadora de destino; por ejemplo, porque un usuario lo envió a través de una red o Internet, o lo llevó en un medio extraíble, como una unidad USB.

Un gusano informático es un programa digital de *malware* autorreplicante. Utiliza una red informática para enviar copias de sí mismo a otros nodos (computadoras en la red) y puede hacerlo sin intervención del usuario. Esto se debe a deficiencias de seguridad en la computadora de destino. A diferencia de un virus, no es necesario que se una a un programa existente. Los gusanos casi siempre causan al menos algún daño a la red, al consumir ancho de banda, por lo que estaría vulnerando en principio la característica de la disponibilidad de los datos, mientras que los virus casi siempre corrompen o modifican archivos en una computadora específica, siendo en este caso mayormente vulnerable la integridad de la información.

1.2.22 Malware-Adware-Spyware

1.2.22.1 Malware

Malware es una forma corta de software malicioso y responde a *"Malicious Software"*, en inglés. El *malware* no es lo mismo que el software defectuoso, es decir, el software que tiene un propósito legítimo pero contiene errores dañinos. El *malware* incluye virus informáticos, gusanos, caballos de Troya, *spyware, adware* deshonesto, software delictivo, la mayoría de los *rootkits* y otros softwares maliciosos y no deseados y su instalación o copiado se produce sin que el usuario legítimo lo autorice o si lo instala, lo hace a partir de un procedimiento engañoso, por lo que podría afectar a las tres características de la seguridad de la información: la confidencialidad, la integridad y la disponibilidad.

1.2.22.2 *Adware*

Del inglés *ad: advertising,* en español: publicidad y *ware,* en español: que alude a software o programa informático, es el software respaldado por publicidad, es cualquier paquete de *software* que reproduce, muestra o descarga publicidades en una computadora automáticamente después de instalar el *software* o mientras se usa la aplicación. Las funciones de publicidad se integran o se incluyen con el *software*, que a menudo está diseñado para indicar qué sitios de Internet visita el usuario y para presentar la publicidad pertinente a los tipos de productos o servicios que allí aparecen, alterando la disponibilidad de la información

1.2.22.3 *Spyware*

El *Spyware* (software espía, en español), es un tipo de software malicioso que se instala en las computadoras y recopila pequeñas porciones de información, a la vez, sobre los usuarios, sin su conocimiento. La presencia de *spyware* generalmente está oculta

para el usuario y puede ser difícil de detectar. Normalmente, el *spyware* se instala secretamente en el *PC* del usuario. A veces, sin embargo, los *spywares* como *keyloggers* son instalados por el propietario de una PC compartida, corporativa o pública a propósito, para monitorear en secreto a otros usuarios, interviniendo en la confidencialidad de los datos, aunque no se descarta que luego su accionar pueda afectar su integridad.

1.2.23 Troyanos-*Rootkit*

Un troyano, a veces denominado “caballo de Troya”, es un *malware* no auto-replicante que parece realizar una función deseable para el usuario, pero que en cambio facilita el acceso no autorizado al sistema informático del usuario.

Un *Rootkit* es un tipo de software que está diseñado para obtener el control de nivel de administrador sobre un sistema informático sin ser detectado. En prácticamente todos los casos, el propósito y el motivo es realizar operaciones maliciosas en un sistema informático host objetivo, en una fecha posterior, sin el conocimiento de los administradores o usuarios de ese sistema. Los *Rootkit* se pueden instalar en *hardware* o *software* dirigidos en la *BIOS*, hipervisores, cargadores de arranque, *kernel* o con menor frecuencia, bibliotecas o aplicaciones.

Estos tipos de ataque podrían comprometer a la confidencialidad, la integridad y la disponibilidad de la información, es decir, las tres características de la seguridad de la información.

2 NORMATIVA

En todo el mundo, en los últimos años y fundamentalmente a partir de la pandemia que vivimos, se han generado situaciones de riesgo informático e incrementado los ataques a los datos públicos de forma inédita, aumentando su frecuencia e impacto de manera sorprendente.

A raíz de ello y debido al avance de la tecnología informática en general, en el Estado Nacional de la República Argentina, los Organismos de Control y de Seguridad de la Información han dictado varias Disposiciones, Resoluciones y Decisiones Administrativas que ponen de manifiesto la importancia de la observación y el seguimiento de los aspectos vinculados a la protección de la información en los Organismos públicos del país, a efectos de prevenir y/o mitigar los incidentes de seguridad que pudieran ocurrir..

Algunas Normas son de cumplimiento obligatorio, otras son recomendaciones que indican los pasos a seguir para mitigar los riesgos que representan los ataques a los datos confidenciales en las Bases de Datos y Sistemas correspondientes al Estado Nacional.

Entre esas Normas, que están relacionadas con los Bancos de Datos personales y sistemas públicos nacionales, dictadas en los últimos años, se señalan a continuación las que -a criterio del autor- resultan ser fundamentales y necesarias para el tratamiento de la seguridad informática en el sector público nacional:

- Resolución N° 47/2018 - AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA: Se refiere al Tratamiento y conservación de los datos personales en medios informatizados.
- Disposición N° 1/2021 - DIRECCIÓN NACIONAL DE CIBERSEGURIDAD: Se crea en el ámbito de esta Dirección el Centro Nacional de Respuesta a Incidentes Informáticos (CERT.AR), con el objetivo de coordinar la gestión de incidentes de seguridad a nivel nacional y prestar asistencia.

- Decisión Administrativa N° 641/2021- JEFATURA DE GABINETE DE MINISTROS: Se aprueban los requisitos mínimos de Seguridad de la Información para los Organismos del Sector Público Nacional.
- Comunicación “A” 7266 de 2021 - BANCO CENTRAL DE LA REPÚBLICA ARGENTINA: Se establecen una serie de lineamientos para la respuesta y recuperación ante ciber incidentes con el fin de limitar los riesgos en la estabilidad financiera e impulsar la ciber resiliencia del ecosistema en su conjunto, en línea con las recomendaciones del Consejo de Estabilidad Financiera (*FSB*). Esta Circular obliga a las entidades financieras públicas y privadas a reportar incidentes de Seguridad.
- Resolución 75/2022 - MINISTERIO DE SEGURIDAD: Este plan incluye un proyecto que abarca desde el año 2021 al 2024 y deroga y actualiza la Resolución 977/2019 en la que se aprueba el “Plan Federal de Prevención de Delitos Tecnológicos y Ciberdelitos”.
- Resolución 86/2022 - MINISTERIO DE SEGURIDAD: Se crea en el ámbito de la Unidad de Gabinete de Asesores del Ministerio de Seguridad, el “Programa de Fortalecimiento en Ciberseguridad y en Investigación del Cibercrimen” (ForCIC) que tiene como objetivo coordinar, asistir y brindar asesoramiento en técnicas de seguridad de las infraestructuras digitales y en técnicas de investigación en materia de ciberdelitos y delitos con presencia de la tecnología y/o utilización de tecnologías.
- Resolución N° 87/2022 - SINDICATURA GENERAL DE LA NACIÓN (SIGEN): Se establecen Normas de Control Interno para Tecnología de la Información en los Organismos Públicos del Sector Nacional, indicando entre otros, la obligatoriedad de incorporar -en los Organismos Públicos- el Área de Seguridad Informática en sus organigramas, independiente del Área de TI, en los casos de Sistemas críticos y/o económicamente importantes. Reemplaza a la Resolución N° 48/2005 del mismo Organismo.
- Resolución N° 324/2022 - MINISTERIO DE SEGURIDAD: Se aprueba “El Plan anual de Ciberseguridad del Ministerio de Seguridad y de las Fuerzas Policiales y de Seguridad”.

- Resolución N° 326/2022 - MINISTERIO DE SEGURIDAD: Reglamenta el funcionamiento de la Comisión Asesora en materia de lucha contra el ciberdelito la cual estará conformada por representantes del ámbito público, del ámbito privado, la sociedad civil y expertos independientes.
- COMUNICACIÓN “A” 7724 de 2023 - BANCO CENTRAL DE LA REPÚBLICA ARGENTINA: Se establecen los Requisitos mínimos para la gestión y control de los riesgos de tecnología y seguridad de la información, derogando la norma anterior sobre “Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras”.

3 INCIDENTES EN ORGANISMOS PÚBLICOS ARGENTINOS

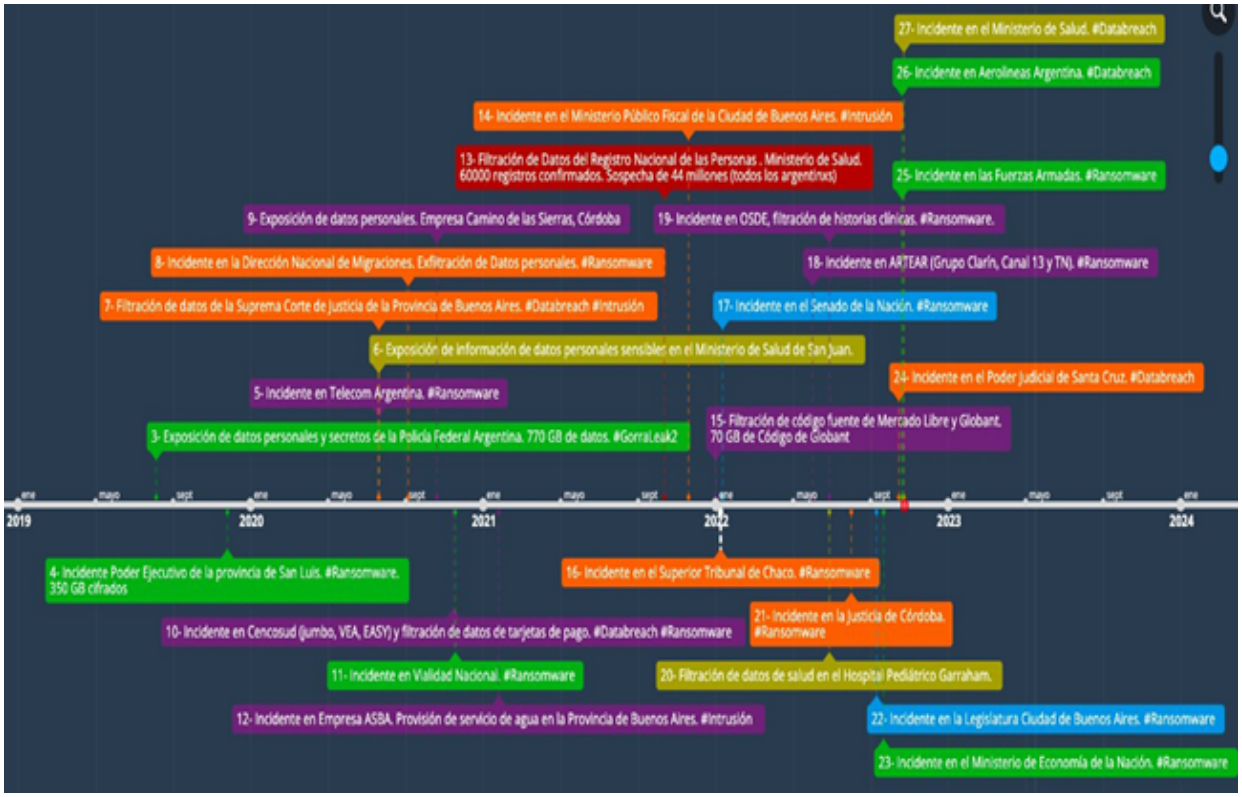

Figura 3 - Incidentes en Organismos Públicos Argentinos

Este gráfico, obtenido de la cuenta de Twitter de la Especialista Marcela Pallero, indica los principales incidentes de ataques informáticos ocurridos en la Argentina hasta abril de 2023. Fue tomado como referencia para efectuar el trabajo de clasificación, análisis y desarrollo correspondiente a este punto, relacionado con los ataques a organismos públicos argentinos que hubieran sido reflejados en algún medio de comunicación.

Sobre esta base, se indican de manera sucinta, los incidentes que reflejan ataques informáticos y en opinión del autor, son los más relevantes ocurridos en Organismos Públicos de la Argentina, en los últimos años:

3.1 Data breach en el Ministerio de Salud de la Nación

Este ciberataque ocurrido el 24/10/2022 provocó la circulación de noticias falsas difundidas desde un correo electrónico que tenía como remitente a la cartera que conducía la Ministra de Salud.

Ese incidente comenzó con la violación de las credenciales de la cuenta de una trabajadora de ese organismo, desde la cual se envió información falsa en una cadena de mails donde se citaba una supuesta reunión con funcionarios del área e importantes periodistas de renombre nacional. Además, se viralizó un correo electrónico difundiendo supuestas listas de portadores de VIH en la Argentina.

3.2 Ransomware en las Fuerzas Armadas

Este incidente, que tuvo lugar el 21/10/2022, consistió en un ataque de tipo *ransomware*, similar al que muchas veces se produce contra empresas y organizaciones privadas, mediante virus informáticos que bloquean los accesos a la información, pidiendo luego “un rescate económico”.

Así, el organismo militar confirmó la detección de “anomalías”, por lo que se tomó la decisión de desconectar los servidores como medida preventiva, luego de la intervención del Comando Conjunto de Ciberdefensa.

3.3 Data breach del Poder Judicial de Santa Cruz

Este incidente sucedió el 12/10/2022, a partir de un ingreso ilegal al servidor por lo que hubo una denuncia ante la justicia provincial, habiéndose advertido la filtración de datos luego de una publicación en *Twitter*, realizada por un *hacker* y experto en seguridad informática.

Se constató que no hubo descargas de información, ni se borraron datos. Tampoco se registraron cambios de claves de los usuarios. Sin

embargo, no se descarta que pueda ocurrir en el futuro un uso ilegal de los datos.

3.4 Ransomware en el Ministerio de Economía de la Nación

El 23/09/2022, una persona afirmó tener accesos a sistemas del Ministerio de Economía, ofreciendo la venta de la información en un foro especializado.

Estos accesos a sistemas, que contienen datos personales, confidenciales y privilegiados, estaban a la venta por un total de 15 mil dólares. No obstante, desde las áreas técnicas correspondientes, se afirmó que no se detectó el acceso ilegítimo a las bases de datos, ni la sustracción de claves o información en cuestión, por lo que el hecho quedó aparentemente desestimado, según fuentes periodísticas oficiales.

3.5 Ransomware en la Legislatura Porteña

El organismo legislativo fue víctima el 12/09/2022 de un ciberataque que comprometió sus “sistemas internos”. Las autoridades hicieron la denuncia ante la Unidad Especializada en Delitos y Contravenciones Informáticas de la Ciudad. Requirieron además a través de un comunicado difundido oficialmente, que no se utilizaran las computadoras ni el WiFi del organismo.

Asimismo, a través de una comunicación interna enviada a los coordinadores de las áreas, se solicitó que no se utilice ningún dispositivo, por cuestiones de seguridad.

3.6 Ransomware en la Justicia de Córdoba

El 14/08/2022 se produjo en la Justicia de Córdoba el "peor ataque informático en la historia a instituciones públicas", que afectó la página Web del Organismo, sus servicios digitales y las bases de datos. Los sistemas habrían sido víctimas de un ataque dirigido con una variante de *ransomware* denominada *".play*", un programa que copia y encripta la información. Usualmente, estos virus bloquean el acceso a la información a cambio de un rescate. Sin embargo, este incidente de seguridad de la información no habría tenido como objetivo un "pedido de rescate", sino la afectación del sistema mediante el cifrado de los datos.

3.7 Ransomware en el Senado de la Nación

El Senado de la Nación fue objeto de un ciberataque el 12/01/2022, realizado por piratas informáticos. Este accionar malicioso tuvo por fin el secuestro de datos de la Cámara Alta. El ataque fue realizado a las cuatro de la mañana del día antes mencionado y consistió en un secuestro de información, luego de lo cual, se solicitó un rescate para restablecer el acceso.

En el caso del Senado de la Nación, el organismo señaló que "toda la información sustraída es pública y se encuentra al alcance de todos y todas dentro del sitio Web correspondiente". No obstante, existieron indicios de que se vio afectada su operatoria habitual.

3.8 Ransomware en el Superior Tribunal de Chaco

El 08/01/2022 el Poder Judicial de la Provincia del Chaco sufrió un ataque de tipo Ransomware en sus servidores, afectando las bases de datos y la infraestructura tecnológica.

Entre las carpetas encriptadas que se encontraron, apareció un mensaje con indicaciones para acceder a la deep web. En esta ubicación, se encontró el pedido de rescate, un monto exigido como rescate y la forma de concretar el pago**.** Sin embargo**,** los jueces del máximo tribunal de Chaco decidieron frenar la avanzada y no proceder según lo solicitado por los malvivientes, aduciendo que por decisión política, no se iba a pagar dado que el organismo no estaba dispuesto a negociar con delincuentes.

De esta forma, gracias a que se pudo acceder a los backups, se logró recuperar un altísimo porcentaje de la información de las bases de datos y servidores atacados, en una ventana de tiempo razonable. Cabe acotar que este incidente tuvo lugar en el mes de enero, periódo de feria en el Poder Judicial.

3.9 Data breach del RENAPER

El 13/10/2021 en redes sociales circularon capturas de pantallas que mostraban un presunto hackeo a la base de datos del Renaper, que cuenta con información de los DNI de más de 45 millones de personas en el país. Sin embargo, el organismo aclaró que sus sistemas de seguridad informática no fueron vulnerados.

No obstante ello, se logró detectar que mediante el uso de claves otorgadas a otros organismos públicos, en este caso el Ministerio de Salud, se filtraron imágenes pertenecientes a trámites personales realizados en el Renaper. Desde el organismo dependiente del Ministerio del Interior se confirmó que se trató de un uso indebido de un usuario o del robo de su clave de acceso, y que la base de datos no sufrió vulneración o filtración alguna de datos.

3.10 Exposición de información en el Ministerio de Salud de San Juan

El 27/05/2021 la Dirección Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública realizó una investigación de oficio en el Ministerio de Salud de la provincia de San Juan, por una supuesta vulnerabilidad de la base de datos del portal de trámites de permisos de circulación por la Pandemia que emitía dicha jurisdicción. Esta vulnerabilidad permitía acceder a datos de salud alojados en el sistema sanitario "Andes Salud".

La Agencia resolvió aplicar sanciones por haber incurrido en dos infracciones graves ya que se mantenían bases de datos locales, programas o equipos que contenían información de carácter personal sin las debidas condiciones de seguridad, y por incumplir con el deber de confidencialidad exigido por el artículo 10 de la Ley 25.326 de Protección de Datos Personales.

3.11 Ransomware en la Agencia de Seguridad Vial

Este ataque de *ransomware* ocurrió el 26/11/2020 en la Agencia Nacional de Seguridad Vial, dependiente del Ministerio de Transporte. Por el ataque, que se caracterizó por el secuestro de los datos y archivos, a los cuales, no se podía acceder, los delincuentes pidieron una suma de dinero y amenazaron señalando que de no pagarse, publicarían la información en la *Dark Web* (web oscura, en español).

En la captura de pantalla con la amenaza de publicación, los atacantes incluyeron algunas carpetas que según *DarkTracer* -plataforma de Inteligencia Artificial que ofrece una ciberdefensa integral, protegiendo completamente el ecosistema digital de cualquier organización- pertenecen al sitio “argentina.gob.ar”. Sin embargo, esta información fue desmentida por distintas fuentes a las que se les consultó ya que todas, coincidieron al indicar que pertenecen a carpetas de la red interna de la Agencia. Además,

el organismo señaló que no iba a “abonar la cifra pretendida por los delincuentes" para evitar la filtración, según aseguraron en su momento. Más tarde y aún en la actualidad, no se pudo obtener más información al respecto, ni fue publicada novedad alguna.

3.12 Ransomware en la Dirección Nacional de Migraciones

El 27/08/2020, un *ransomware* denominado *NetWalker* vulneró los datos de la Dirección Nacional de Migraciones, dependiente del Ministerio del Interior. Un mensaje extorsivo señalaba que, si no se pagaba por recuperar la información secuestrada, harían públicos los datos.

En principio, Migraciones confirmó el ataque y aseguró que estaba contenido. Luego se supo que en rigor había puesto a funcionar un backup, por lo cual no necesitaba abonar el rescate para sacar el "candado" que tenían los documentos (descifrarlos para recuperar el acceso a ellos). Sin embargo, para evitar la "fuga" de archivos, los delincuentes, que ya tenían una copia en su poder, pedían la suma de 4 millones de dólares para evitar su difusión, dando una semana de aviso.

Oficialmente, la Dirección Nacional de Migraciones informó que logró contener ese intento de ciberataque al organismo, lo que ocasionó la caída de servicios, que se fueron restableciendo paulatinamente.

3.13 Filtración de información secreta de la PFA

El 12/08/2019 un Hacker, luego conocido como “La Gorra Leaks”, subió a la plataforma Twitter la información relacionada con una filtración de datos de 700 Gb., que llevó a cabo a través del hackeo de un portal web de la Policía Federal Argentina. Esa información fue subida por el delincuente a la *Deep Web* (web profunda, en español), lo que hacía necesario utilizar “el programa Tor” para visualizarla. Tor es una aplicación que toma los datos que entran y salen a través de una conexión a Internet

y los hace pasar a través de un circuito de servidores repartidos por todo el mundo. Eso consigue que el tráfico se vuelva totalmente anónimo.

A pesar de existir el riesgo de exponer a gente inocente, al filtrar en la Internet profunda -y, de allí, sacar a la superficie digital- información sensible e incluso personal relacionada con las Fuerzas Federales de Seguridad, el *Hacker* manifestó que eso no le interesa, que simplemente lo hizo como un “desafío personal técnico”, con la simple intención de “dar dolores de cabeza a las autoridades”, ya que la policía no es de su agrado.

Cabe acotar que no se pudo comprobar ninguna alteración de la información correspondiente. A partir de lo ocurrido, la Agencia de Acceso a la Información Pública realizó una investigación de oficio que, una vez finalizada, dió lugar al apercibimiento de la Policía Federal Argentina por incumplimientos a la Ley 25.326 de Protección de Datos Personales. La sanción se justificó en el hecho de que dicha institución no cumplió con los protocolos de seguridad ni con el deber de confidencialidad y por no haber dado respuesta a una intimación que envió con anterioridad la Dirección Nacional de Protección de Datos Personales.

3.14 Secuestro de cuentas del Ministerio de Seguridad de la Nación

El 26/01/2017 hackearon la cuenta de *Twitter* de la entonces Ministra de Seguridad de la Nación, por lo que se descubrió que su biografía -en esa plataforma- había sido modificada y también se publicaron desde su usuario polémicos *tweets*. Además se conoció que, en esa ocasión, más de 30 casillas de mail pertenecientes al personal del Ministerio de Seguridad habían sido vulneradas.

El 16/02/2017 se produce un segundo hackeo, en este caso a la cuenta principal de la PSA (Policía de Seguridad Aeroportuaria), dependiente del Ministerio de Seguridad.

Debido a estos incidentes, la Justicia -con la colaboración de la Policía Federal- dio con los responsables del *hackeo*, por lo que fueron

detenidos dos sospechosos, tras una tarea de inteligencia que siguió varias pistas.

Se desconoce en qué momento los *hackers* robaron las credenciales (las contraseñas), pero lo cierto es que la División Delitos Tecnológicos de la Policía Federal pudo detectar un ingreso a uno de los mails vulnerados desde un teléfono celular. Los investigadores pudieron conocer que el equipo pertenecía a un tal Mirco Milski, alias “El Niño Orsino”.

Al sospechoso se lo detuvo, por lo que brindó declaración indagatoria y se obtuvieron rastros y pruebas de que fue el autor del ataque al Twitter de la Ministra, de vulnerar las cuentas del Ministerio y además del hecho de la PSA.

Asesorado por sus abogados, el hacker hizo su descargo, al alegar que "no obtuvo datos de manera ilegal". Señaló que es un profesional que realiza asesoramiento en seguridad informática y que su objetivo era colaborar con la sociedad para exhibir la vulnerabilidad de los sistemas.

La Justicia días más tarde arrestó al segundo sospechoso, llamado Martín Horacio Trabucco y allanó su domicilio en La Plata. Se trata de un técnico informático que tenía antecedentes en otra causa por el mismo delito. Este sospechoso también brindó declaración indagatoria. Se sospecha la participación de más personas en los hechos. Ambos sospechosos fueron luego puestos en libertad.

Estos hechos impactaron en la confidencialidad y la integridad de la información almacenada en la cuenta de *Twitter* de la Ministra, en los mails del personal del Ministerio y en la cuenta principal de la PSA.

4 VULNERABILIDADES

En ese punto se indican las vulnerabilidades más comunes conocidas y detectadas, surgidas a partir de debilidades, errores, fallos de control o descuidos informáticos. En este trabajo se presentan agrupadas en Generales y Particulares.

Al respecto, existe una fundación sin fines de lucro denominada *OWASP* (*Open Web Application Security Project*, en español: “Proyecto abierto de Seguridad de Aplicaciones Web”), dedicada a mejorar la seguridad del software y evitar vulnerabilidades informáticas en el desarrollo web, que funciona bajo un modelo de "comunidad abierta". Es reconocida mundialmente por los desarrolladores como el primer paso hacia una codificación web más segura.

OWASP proporciona varias guías de desarrollo, testeo o pruebas unitarias para el desarrollo web y además, cada 2 o 3 años elabora un listado con el Top 10 de las vulnerabilidades informáticas web más explotadas, siendo el último correspondiente al año 2021. En las clasificaciones siguientes, se señalan algunas vulnerabilidades que aparecen en el listado citado:

4.1 Agrupamiento General

4.1.1 Vulnerabilidades no conocidas

También llamadas vulnerabilidad de día cero. En este caso nadie, ni siquiera la empresa desarrolladora, sabe frente a qué tipos de debilidades se está enfrentando, debido a que no han sido detectadas previamente. Por ello, resultan ser las más peligrosas, ya que los ciberdelincuentes las aprovechan para hacer ataques, encontrando desprevenidos a quienes deben tomar acciones para proteger los recursos. Esto además, permite que se genere un mercado ilegal de compra-venta de vulnerabilidades.

4.1.2 Vulnerabilidades de diseño

Se deben a fallos en el diseño de aplicaciones informáticas, mal diseño de protocolos de redes o deficientes políticas de

seguridad. Este tipo de vulnerabilidad fue informada en el cuarto lugar de mayor riesgo en seguridad en el TOP 10 de *OWASP* de 2021.

4.1.3 Vulnerabilidades de implementación

Se dan por errores de implementación de aplicativos o descuidos de los fabricantes de software, aunque también por presencia de “puertas traseras” en los sistemas informáticos

4.1.4 Vulnerabilidades por falta de mantenimiento

Se manifiestan cuando los softwares ya no reciben actualizaciones del fabricante o cuando nunca procedemos a verificar e instalar las actualizaciones correspondientes. Esta vulnerabilidad fue ubicada en el sexto lugar de mayor riesgo en seguridad en el TOP 10 de *OWASP* de 2021.

4.1.5 Vulnerabilidades por uso o causadas por factor humano

Son las menos consideradas, pero pueden tener mayor impacto que todas las anteriores. Se asocian con la falta de formación o conciencia en los usuarios o empleados de una entidad sobre prácticas de seguridad. Suelen incrementar su impacto por la configuración inadecuada de los sistemas informáticos, existencia de herramientas que facilitan los ataques y limitaciones en cuanto a la disponibilidad de componentes de tecnología de seguridad en la organización.

4.2 Particulares

4.2.1 Vulnerabilidades de desbordamiento de buffer

Esta situación se plantea cuando un programa no controla la cantidad de datos que se copian en el buffer. Esto implica que si dicha cantidad es mayor a la capacidad del buffer entonces los bytes sobrantes se van a almacenar en zonas de la memoria adyacentes, de manera que se sobreescriba contenido original. Esta vulnerabilidad es aprovechable para ejecutar códigos que otorgan privilegios de administrador. Este tipo de vulnerabilidades, relacionadas con la

pérdida de control de acceso, fue informada en el primer lugar de mayor riesgo en seguridad, en el TOP 10 de *OWASP* de 2021.

4.2.2 Vulnerabilidades de condición de carrera (*race condition*)

Se materializa cuando varios procesos acceden al mismo tiempo a un recurso compartido.

4.2.3 Vulnerabilidades de error de formato cadena (*format string bugs)*

Ocurren por aceptar, sin validación, la entrada de datos proporcionada por el usuario. Corresponde a un error de programación y el lenguaje más afectado es C/C++. Este ataque puede conducir inmediatamente a ejecutar código arbitrario y a revelar información. Esta vulnerabilidad fue situada en el quinto lugar de mayor riesgo en seguridad, en el TOP 10 de *OWASP* de 2021.

4.2.4 Vulnerabilidades de *Cross Site Scripting* (CSS)

Lo conforman todos los ataques que permitan ejecutar scripts como *VBScript* o *JavaScript*, en el contexto de otro sitio web. Pueden encontrarse en cualquier aplicación que tenga por objetivo final la presentación de información en un navegador web. Se usa, entre otros, para la realización de *phishing*, donde la víctima al ingresar a un sitio web, en la barra de dirección, ve una URL pero realmente accede a otra. A partir de este engaño, introduce su contraseña o sus datos personales, que son recepcionados por el atacante. Esta vulnerabilidad fue mencionada en el segundo lugar de mayor riesgo en seguridad, en el TOP 10 de *OWASP* de 2021.

4.2.5 Vulnerabilidades de Inyección *SQL*

Se da cuando se inserta o inyecta un código *SQL* invasor dentro del código *SQL* programado, con la finalidad de alterar el funcionamiento normal de dicho programa. Esta acción maliciosa se realiza para lograr que sea ejecutada la porción de código «invasor» incrustado dentro de la base de datos. Esta vulnerabilidad ocupa el

tercer lugar de mayor riesgo en seguridad, en el TOP 10 de OWASP de 2021.

4.2.6 Vulnerabilidades de denegación del servicio

Este tipo de vulnerabilidades causa que el recurso sea inaccesible para usuarios legítimos ya que produce la pérdida de conectividad de red debido al consumo de ancho de banda de la red o la sobrecarga de los recursos informáticos del sistema de la víctima.

4.2.7 Vulnerabilidades de ventanas engañosas (*Windows Spoofing*)

Son aquellas que se manifiestan a partir de un engaño, destinado a que el usuario entregue información confidencial. A manera de ejemplo, le hacen saber al usuario que es ganador de un determinado premio, información que es falsa, para que entregue datos personales. Pueden también existir también otro tipo de ventanas engañosas donde, al hacer clic e ingresar en ellas, el atacante obtiene datos del ordenador para posteriormente realizar el ataque.

4.3 Ejemplos

En función de lo anteriormente expuesto, se presentan a continuación algunos ejemplos más comunes de vulnerabilidades de seguridad informática:

1. Contraseñas débiles.
2. Software ya infectado con virus.
3. Bugs, es decir, fallos o errores de software.
4. Falta de cifrado de datos sensibles.
5. Transacciones no autorizadas.
6. Redireccionamiento de URL a sitios no confiables.
7. Falta de autenticación para una función crítica.

8. Carga sin restricciones de archivos peligrosos y descarga de códigos sin controles de integridad.
9. Dependencia de entradas no confiables en una decisión de seguridad.
10. *Cross-site scripting* y falsificación.
11. Errores de configuración.
12. Errores en la gestión de recursos.
13. Errores en los sistemas de validación.
14. Errores que permiten el acceso no autorizado a directorios.
15. Errores en la gestión y asignación de permisos.

5 FORMAS DE PREVENCIÓN

Debido a que los cibercriminales operan de manera encubierta y no son fáciles de detectar, puede pasar mucho tiempo antes de que los problemas sean visibles para cualquier organización, incluyendo las gubernamentales. Diversas publicaciones y expertos sostienen que algunas amenazas pueden ser detectadas, pero la gran mayoría pasará desapercibida. Por eso, una detección temprana siempre será necesaria.

Los siguientes son algunos pasos de prevención, a modo de recomendaciones destinadas al personal del Área de Sistemas o de Seguridad Informática del organismo, para estar preparados antes de que los ataques ocurran:

5.1 Supervisar el uso de correos electrónicos

Monitorear la aparición de mensajes sospechosos, así como las descargas de archivos anexos. Asimismo, educar al personal de la organización sobre el buen uso de este medio para que sea empleado sólo con fines laborales.

5.2 Estar alerta del tráfico anormal

Recolectar datos para establecer el comportamiento anormal de la red, referido a protocolos, aplicaciones o actividad de los usuarios. Prestar atención al volumen del tráfico y a los cambios inesperados en el uso del protocolo.

5.3 Identificar los códigos maliciosos

Los *malwares* y códigos maliciosos generalmente se esconden en formatos comunes de archivo (pdf, html, exe, zip, gif, etc.). Una buena práctica consiste en seleccionar un antivirus capaz de descubrir, decodificar y neutralizar estos códigos ocultos antes de que impacten en el puesto de trabajo.

5.4 Reconocer las conexiones sospechosas

Los cibercriminales a menudo usan direcciones IP, sitios web, archivos y servidores de correo electrónico, cuya actividad maliciosa ha sido registrada. Por ello, se recomienda utilizar herramientas capaces de examinar la reputación de fuentes no confiables ubicadas fuera de tu organización.

5.5 Supervisar la alteración de las aplicaciones

Cuando un atacante consiga ingresar a la red de la empresa, puede emitir comandos direccionados a aplicaciones clave. Para prevenirlo, se deberá crear una lista blanca (*whitelisting*) para especificar las aplicaciones que pueden ser ejecutadas.

Paralelamente, se deberá establecer una lista negra de programas no autorizados (*blacklisting*). De esa manera se podría prevenir cualquier intento de alteración en el sistema, ya sea en el servidor de correo electrónico, en los archivos, en los paquetes de software, etc.

5.6 Monitorear las Bases de datos

Los intentos no autorizados de acceso a datos críticos y de modificación de la estructura en el banco de datos son señales de alerta que indican que la red puede estar siendo amenazada. En estos casos, se deben usar herramientas para monitorear bases de datos y registrar intentos de acceso no autorizado. A continuación se indican algunas de estas herramientas:

- *Solarwinds DB Performance Analyzer*.
- *Idera SQL Diagnostic Manager*.
- *Lepide SQL Server Auditing*.
- *Heroix Longitude®*.
- *SQL Power Tools*.
- *Red-Gate SQL Monitor*.
- *Sentry One (SQL Sentry)*.

5.7 Vigilar las transferencias de datos

Monitorear la transferencia de información, especialmente cuando se trate de datos que sean propiedad intelectual de la empresa. Asimismo, prestar atención al movimiento poco común de datos, tráfico cifrado o transferencias de archivos sospechosos.

5.8 Mantener los sistemas actualizados

Si se trata de un computador personal, generalmente no es difícil suponer que el equipo tendrá un buen funcionamiento. Sin embargo, cuando no es uno, sino un volumen mayor de computadores, la tarea puede volverse compleja.

La mejor manera de enfrentar este desafío es haciendo un inventario de todo el hardware disponible en la organización porque permite gestionar todos los activos de información, así como los riesgos de seguridad a los que están expuestos.

Además, para realizar las actualizaciones que los equipos requieren, hay dos opciones: la primera es entrenar a los empleados para que las realicen periódicamente y la segunda, es automatizar el proceso a través de una herramienta que actualice automáticamente los sistemas. Esta última opción permitirá que se descarguen las actualizaciones de una sola vez y luego se vayan distribuyendo, según corresponda.

La ventaja de este método es que se tendrá la seguridad de que las actualizaciones están siendo instaladas en el momento en que se indique, sin tener que depender de intervención humana.

Asimismo, centralizar las actualizaciones permite ejecutar tareas de gerenciamiento de sistemas fuera del horario de trabajo, sin entorpecer las actividades diarias de los empleados.

5.9 Gestionar los riesgos de seguridad de la información

Por último y en forma general a todo lo antes citado, se recomienda contar con herramientas que permitan identificar, evaluar, controlar y monitorear los tipos de riesgos, a efectos de asegurar la confidencialidad,

integridad y disponibilidad de la información en las organizaciones públicas, es decir implementar la evaluación y el tratamiento de los riesgos de seguridad de la información en la organización. Si bien esta sección se incluye al final, su importancia es mayor que los puntos previamente citados, debido a que el tratamiento de los riesgos resulta ser la base fundamental al momento de analizar, desarrollar y clasificar cualquier tipo de medida de prevención descrita en esta sección 5.

6 CONCLUSIONES

La administración y manipulación de los datos personales implica la intervención de diferentes actores en su tratamiento. Las políticas de los datos hacen referencia a su gestión y cuidado integral, incluyendo su usabilidad y seguridad. Por ello es importante fomentar la adquisición de conocimientos y habilidades específicas en todos los intervinientes, especialmente en los encargados de procesar información y en los usuarios titulares de los datos.

En efecto, el tratamiento responsable de la información supone el trabajo conjunto y colaborativo de todos los participantes, así como de los especialistas en la materia. Por lo tanto, será necesario incluir a representantes de la sociedad civil, académicos especializados en seguridad de la información, investigadores, directivos de empresas públicas y privadas, especialistas en ética, técnicos informáticos y al público en general, ya que todos son titulares de los datos. En suma, la participación es multifactorial y requiere de la contribución de todos los involucrados.

Entre los ejes de las políticas de privacidad orientadas al tratamiento de los datos, es menester considerar la formulación de más y mejores políticas públicas en colaboración con el sector privado y con los especialistas en ciberseguridad. El objetivo será prevenir y mitigar los riesgos y hacer uso de las tecnologías informáticas disponibles para brindar una mayor seguridad a la información, y así fomentar una mayor protección de los datos personales y un incremento en la confianza de los usuarios.

A pesar de que existe un gran número de personas que han manifestado preocupación por el uso indebido de sus datos personales en las plataformas digitales, particularmente de las redes sociales, existen pocas evidencias de que las instituciones que tratan sus datos les hayan proporcionado un aviso previo de privacidad y de que adopten seriamente una política de protección de datos personales. Asimismo, se conocen muy pocos casos en los que exista un canal disponible y de uso sencillo para la presentación de quejas por uso indebido de datos personales. Podemos suponer que la cantidad y la calidad de la información recopilada a través de las plataformas digitales va más allá del nombre, la dirección, el teléfono o de otros datos que se requieren para el

registro o acceso en tales plataformas. No obstante, no se tiene un informe confiable de análisis del nivel de conocimiento de los ciudadanos ni tampoco del grado de preocupación que manifiestan respecto al tratamiento indebido de la información recopilada por las plataformas y de cómo ésto podría afectar sus intereses.

La participación ciudadana, de organismos públicos con competencias en la materia, entidades privadas y asociaciones civiles y de la industria informática en general, resulta relevante para fomentar un enfoque preventivo en el desarrollo de software seguro especialmente cuando trate datos personales. Esto se hace extensivo al uso de herramientas informáticas que promuevan una mayor protección a los datos, a la incorporación de protocolos seguros para el tratamiento de la información e incluso, para encarar una política de presión en el mercado con el fin de que las empresas cumplan con los mecanismos necesarios para el debido respeto de los derechos de privacidad y protección de datos.

Así, a efectos de minimizar o mitigar los ataques a los datos personales, deberían implementarse en cada organismo público (y también en entidades privadas) más y mejores políticas relacionadas con la seguridad de la información, por medio de las cuales se “eduque” e “instruya” al personal acerca de su importancia, sus riesgos y consecuencias. Si bien se registran algunos avances en este sentido, estos resultan insuficientes ya que el avance del ciberdelito resulta notorio. Además se debería tratar, consensuar e implementar más y mejores leyes y normas a partir de una política pública que promueva la protección de la privacidad. Esta política debe incorporar 3 conceptos fundamentales vinculados al desarrollo de la ciudadanía en general: la “prevención estatal”, la “educación virtual” y la “socialización informática”:

La “prevención estatal”:

Si bien existe en la legislación argentina normas, disposiciones y políticas que tienen como finalidad la prevención de las vulneraciones a los derechos de la privacidad, que incluye una serie de medidas tendientes a

prevenir que ello suceda, la simple existencia de la legislación y de políticas públicas y privadas, no conlleva necesariamente a su cumplimiento automático. En este sentido, es menester fortalecer los mecanismos efectivos de monitoreo en organismos públicos y privados y en especial, respecto a las plataformas digitales, para fomentar su cumplimiento. De esta forma, puede evaluarse si resulta necesario considerar modificaciones en leyes o normas, que involucren un tratamiento más estricto y que regulen, instruyan, prevengan y penalicen los casos indeseados y maliciosos de intrusiones a los datos personales.

La “educación virtual”:

Los datos anteriores exponen una fuerte urgencia al momento de fortalecer la alfabetización digital, a través de medidas que permitan el desarrollo de competencias para el uso de dispositivos informáticos de una manera responsable y segura. Una estrategia adecuada debería considerar el acercamiento a la población a través de diversos canales, con un mensaje que les permita detectar posibles riesgos y amenazas a su privacidad, así como desarrollar habilidades para adoptar medidas concretas con el fin de contenerlos y minimizarlos. A su vez, es necesario fortalecer una cultura de reporte y denuncia respecto a incidentes e ilícitos cometidos a través de dispositivos electrónicos, desarrollando mecanismos adecuados para su concreción.

La “socialización informática”:

Es necesario además, que los usuarios conozcan sus derechos y la forma de ejercitarlos, que las autoridades se encuentren preparadas para dar seguimiento a los procesos que se deriven de la aplicación de las normas en un ámbito digital. Además, se debe contar con mejores mecanismos para sancionar a los infractores y asegurar una reparación del daño equitativa para los afectados, así como medidas que impidan la repetición de la conducta violatoria de derechos de privacidad, considerando especialmente los grupos vulnerables.

Desde una perspectiva optimista y a través del tiempo, puede suponerse que con el avance de la tecnología, teniendo más y mejores técnicos y especialistas interesados en la seguridad de la información, preparados, egresados de carreras relacionadas con la disciplina y contando con una mejora en el consenso y la participación legislativa y ciudadana al respecto, estos objetivos, antes enunciados, se podrán paulatinamente lograr.

7 BIBLIOGRAFÍA

- “Protección de datos personales“ https://www.argentina.gob.ar/aaip/datospersonales
- “Resolución AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA Nº 47/2018”
- “Decisión Administrativa 641/2021”
- “Resolución SIGEN Nº 87/2022“
- “Ciberseguridad: todos podemos ser víctimas” https://iqlatino.org/ciberseguridad-todos-podemos-ser-victimas/
- “Vulnerabilidades Informáticas” https://ginzo.tech/blog/vulnerabilidades-informaticas-que-son-tipos/
- “Revista de Ciberseguridad y Seguridad de la Información para empresas y Organismos Públicos https://www.ciberseguridadpyme.es/
- “Tipos de Ataques informáticos y cómo prevenirlos” https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/
- “Consejos para prevenir ataques informáticos” https://www.piranirisk.com/es/blog/8-consejos-para-prevenir-ataques-informaticos
- “Datos personales: tus derechos” https://www.argentina.gob.ar/aaip/datospersonales/derechos

- “Ataques de Autenticación” https://www.segu-info.com.ar/ataques/ataques_autenticacion