Panorama general sobre la seguridad de la información, las vulnerabilidades y los incidentes en Argentina

DEMOCRACIA EN RED

O.D.I.A.

Fundación Vía Libre

Este trabajo es producto de la colaboración entre Democracia en Red, Fundación Vía Libre y el Observatorio de Derecho Informático Argentino (O.D.I.A), con el apoyo de Indela.
democraciaenred.org / vialibre.org.ar/ odia.legal / indela.fund

La presente versión fue escrita por Marcela Pallero.

DEMOCRACIA EN RED

O.D.I.A.

Fundación Vía Libre

Panorama general sobre la seguridad de la información, las vulnerabilidades y los incidentes en Argentina

Contenidos

Las vulnerabilidades

De manera general las vulnerabilidades son debilidades, condiciones que hacen vulnerable a una entidad, una organización, una infraestructura o a un sistema de información y, en consecuencia, donde hay vulnerabilidades hay posibilidad de que al ser aprovechadas un ataque tenga éxito.

La gravedad de una vulnerabilidad dada por el hecho de que pueda ser utilizada para realizar algún tipo de ataque será diferente dependiendo de la información que puede ser expuesta, la importancia de esa información para la organización afectada, así como el servicio o la infraestructura que pueda verse dañada. La diversidad de consecuencias negativas tiene tantas posibilidades que atenderlas y resolverlas es muy importante para la seguridad de la información en numerosos planos.

El impacto que las vulnerabilidades pueden tener en una sociedad es enorme, esto es en parte debido a que los sistemas de uso masivo cuentan con múltiples debilidades, y los programas de uso específico, en general, no siguen buenas prácticas en el desarrollo, y porque al mismo tiempo, existen una gran cantidad de programas destinados a aprovecharlas y causar daños; en este escenario los ataques constituyen un riesgo latente tanto para las personas en sus hogares como para cualquier organización, empresa como para el Estado.

Los incidentes que exponen datos personales en grandes cantidades, como las pérdidas económicas directas o la falta de disponibilidad de servicios esenciales podrían causar estragos, como ya lo están sufriendo distintos países a diferentes escalas, las organizaciones de todo tipo tienen sus riesgos y deben ser analizados para mitigarlos.

En seguridad de la información, una definición de vulnerabilidad se puede encontrar en la norma ISO/IEC 27000, estándar internacional con la terminología básica para la serie de documentos que trata sobre distintos aspectos de la seguridad de la información en el contexto de las organizaciones y extendiéndose a ciberseguridad para hablar de los países en el subconjunto ISO/IEC 27100. Entonces, una vulnerabilidad está definida como una debilidad en un activo o control de la que una o más amenazas pueden aprovecharse. Es decir, encontrada una debilidad en un sistema (o en cualquier tipo de programa), en una web o en un dispositivo o elemento físico los vuelve susceptibles de sufrir algún daño o de ser vulnerados.

En un sentido más amplio, en el ámbito de la administración de las organizaciones un control es una actividad o medida que se diseña e implementa para modificar un riesgo, para minimizarlo o para evitarlo, así una cerradura es un control, como método de autenticación tiene un factor de

autenticación (la llave) y un validador del factor, que es la cerradura en sí, para evitar accesos físicos no autorizados o esquemas de autenticación de usuario y contraseña para restringir accesos y asignar permisos, solo a registrados en ese sistema, plataforma o aplicación.

Este concepto de control es muy usado en la función de auditoría tradicional. Las medidas de seguridad de la información, de manera aún más general son controles..

La auditoría (informática o de sistemas) es el área dentro de una organización que debe verificar que el objetivo para el que fueron diseñados y la forma en que fueron implementados los controles establecidos sigan funcionando.

Estos conceptos y sus formalidades se utilizaron históricamente para la supervisión de las operaciones contables y sus disposiciones, así como a las funciones administrativas en general, y son los que se utilizan también para los aspectos técnicos. La particularidad es que los controles técnicos, en su gran mayoría, pertenecen al ámbito de conocimiento de la seguridad informática, es decir, controles sobre la tecnología.

Sin embargo no es un campo acotado, hoy la tecnología está integrada en casi todos los servicios, y éstos controles deben incluirse en cada sistema, al diseñarlos, codificarlos o programarlos, y en cada agregado de funcionalidad, en la infraestructura que les da soporte (hardware o telecomunicaciones), en las implementación, y en sus configuraciones, etc.. La falta o debilidad de controles pueden dar origen a una vulnerabilidad, por este motivo, la recomendación es cumplir con ciertos controles mínimos para reducirlas razonablemente.

Para cumplir con los objetivos de la seguridad de la información en una organización, hay un conjunto de procesos que se deben llevar adelante, algunos relacionados con los aspectos de administración, de riesgos y otros de carácter más técnicos.

Además, hay principios básicos para la asignación de permisos o derechos de accesos relacionados con las funciones que cada integrante tiene dentro de una organización. En ese sentido, el principio de "necesidad de saber" o "need to know" indica que solo debe tener acceso y permisos a un recurso informático[1] el usuario que lo requiere para cumplir sus funciones de acuerdo a sus responsabilidades en la organización y ninguno más.

Asimismo, otro de los principio, es el de "mínimos privilegios", que requiere que entre los tipos de permisos disponibles, como pueden ser sólo leer, o modificar, por ejemplo, únicamente deberá asignarse el menor de los derechos o permisos a ese usuario para ese recurso. Así el menor de los derechos es el de lectura, dado que no permite realizar alteraciones.

Estos dos principios son básicos en la seguridad de la información y están más relacionados con la administración en los controles de acceso, con el conocimiento de los procesos de la organización, la información que los sistemas gestionan, y con las funciones que las personas realizan más que con el funcionamiento de la tecnología. Sin embargo, una falla en la asignación de permisos puede hacer vulnerable a la organización.

De la misma manera, la identificación y la clasificación de la información son procesos necesarios para relevar cuál es la información que una organización gestiona, y cuáles son los riesgos a los que se encuentran expuestos y definir los requerimientos de seguridad y aplicar los controles de acuerdo a la clasificación y los riesgos.

Por otro lado, están las vulnerabilidades que se originan en las tecnologías, es decir en software o hardware, que requieren un análisis específico, porque pueden deberse a fallas en los diseños, en la implementación, en la programación de los sistemas, o por no atender a las actualizaciones o mantener tecnología obsoleta, entre otras.

En este sentido, la función de Seguridad de la información que debe atender los problemas derivados de las fallas de las tecnologías es el que se denomina gestión de las vulnerabilidades técnicas[2] o simplemente gestión de vulnerabilidades. Este proceso debe llevarse adelante de manera continua para identificar, evaluar, generar informes, administrar y remediar las vulnerabilidades de seguridad a fin de evitar que sean aprovechadas por atacantes.

A fin de entender este proceso y la importancia dentro de la seguridad de la información, es necesario definir también a la seguridad de la información. En este sentido la integridad, la confidencialidad y la disponibilidad son las tres propiedades básicas prioritarias a preservar en esta disciplina.

La integridad supone que debe resguardarse que la información no sea alterada, preservar su exactitud y completitud, o al menos tener información sobre su modificación. La confidencialidad resguarda que sólo accedan a la información, personas, sistemas o programas que están autorizados. Finalmente la disponibilidad debe asegurar que la información se encuentre a disposición cuando se la requiera y que pueda ser utilizada e interpretada.

[1] se denomina recurso informático a cualquier software y hardware de la organización.

[2] Gestión de las vulnerabilidades técnicas - Seguridad de las Operaciones en ISO/IEC 27002 https://normaiso27001.es/a12-seguridad-de-las-operaciones/

Otro concepto de importancia para brindar seguridad en los accesos a sistemas es conocido como el esquema de AAA correspondientes a: autenticación, autorización, y auditoría. (en inglés, authentication, authorization y accounting)[3].

La autenticación es el proceso que permite asegurar que se valide que la entidad (usuario o programa) es quien dice ser cuando intenta acceder. Luego, la autorización es el proceso por el que esa entidad tiene derechos o permisos para realizar determinadas acciones es la autorización. Por último, acá auditoría remite al concepto por el cual todas las acciones deben quedar registradas para revisiones posteriores para que, en caso de ser necesario, ante cualquier incidente se deba recurrir a esa información para identificar causas o causantes.

No obstante, los aspectos de gestión mencionados, muchas vulnerabilidades relacionadas con el acceso a sistemas de información se saltean estos procesos, ya sea por fallas en los diseños o en la implementación. Adicionalmente es de destacar que para evaluar el impacto de una vulnerabilidad en una organización es necesario identificar la funcionalidad que brindan el servicio o la información que se ve afectada en conjunto con la criticidad propia de la vulnerabilidad.

Descubrimiento de Vulnerabilidades

A fin de comprender aspectos puntuales del tema, hay que mencionar brevemente que existen distinciones entre las vulnerabilidades técnicas según el nivel de divulgación que se haya realizado por parte de quien la descubrió[4], si fue comunicada de manera pública, si fue comunicada al fabricante o a un tercero de confianza o si solo es conocida por quien la descubrió y nadie más conoce su existencia, en éste último caso, la vulnerabilidad se denomina, (zero) 0-day o vulnerabilidad de día cero.

Este último tipo de vulnerabilidades representa una situación grave, ya que tiene varias consecuencias negativas, primero que no habrá información para mitigar el riesgo de que sea utilizada por alguien más. Lo deseable y esperable es que cuando el fabricante o proveedor del sistema o servicio esté informado, elabore una solución y brinde una actualización del software o del servicio, en la que la vulnerabilidad se encuentre solucionada. Al menos esa es la situación ideal, aunque no siempre ocurre.

[3] CCN-CERT es el CERT Nacional de España, el equipo de respuesta ante ciberincidentes que es contacto nacional para ese país. https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=5.html

[4] Se asume que quien descubre la vulnerabilidad es una persona ajena o externa, sin vínculo con la organización que desarrolló el producto que tiene la vulnerabilidad.

Por otro lado, si existe una vulnerabilidad, significa que alguien más puede encontrarla y usarla para un ataque o venderla para que alguien más realice un ataque.

Por esta razón es absolutamente necesario que todas las vulnerabilidades, tanto en los casos de vulnerabilidad de día cero, que pueden ser muy peligrosas cuando afectan a sistemas de uso masivo, como vulnerabilidades conocidas en organizaciones de cualquier índole, puedan contar con una solución lo más rápido posible.

Dependiendo de las características de la vulnerabilidad y cómo afecta al producto o servicio, desarrollar una solución podría ser muy costoso para el fabricante u organización y sin obligaciones legales, ni otras presiones, la solución podría demorar demasiado. Por otro lado, una vulnerabilidad que pueda permitir un acceso rápido y fácil a sistemas de uso masivo, divulgada de manera pública, podría ser una oportunidad para que delincuentes la aprovechen. De ahí que la forma en que una vulnerabilidad es comunicada o "divulgada" es un aspecto importante a tratar y ha llevado a debates, y confusiones entre investigadores independientes y autoridades judiciales, desde hace muchos años.

En este sentido, cabe destacar el uso de herramientas para la detección de vulnerabilidades que constituye una industria en sí misma, desde software de código abierto, que van agregando código específico para comprobar la existencia de las nuevas vulnerabilidades o alguna forma de aprovecharlas, hasta servicios específicos, diseñados para brindar la información de manera segmentada a cada organización de acuerdo a las necesidades.

En cuanto a las personas que encuentran vulnerabilidades, estas pueden ser desde usuarios finales, personas que las encuentran de manera circunstancial por trabajar en los distintos ámbitos de las tecnologías de la información, practicantes de la seguridad informática, así como investigadores que han dedicado toda su vida a realizar análisis de seguridad que cuentan con diversas experiencias y conocimientos para descubrir debilidades ya sea de manera independiente como para empresas que desarrollan herramientas para descubrirlas.

En este contexto, la divulgación coordinada de vulnerabilidades sería una práctica que puede ayudar a garantizar la seguridad de los sistemas y de la información, y de quienes reportan , por lo que debería ser promovido y alentado por todas las partes interesadas, dado que la diversidad entre quienes pueden descubrir fallas hace que no todas las personas conozcan los pasos a seguir o buenas prácticas, así como los riesgos para sí.

En particular, se hace más complicado que cualquier persona reporte una vulnerabilidad cuando se penaliza el acceso indebido y se confunde o interpreta su reporte como una acción que merece una acusación penal. Situación que disuade y aleja a quienes conocen éstas circunstancias de la realización de los reportes correspondientes.

Los incidentes de seguridad de la información

El concepto específico para referirse a los problemas técnicos en seguridad de la información es "incidente". Un incidente por definición es un evento o conjunto de eventos no deseados que pone en peligro la integridad, la confidencialidad o la disponibilidad de la información, e incluye las transgresiones a una política de seguridad de la información, o política de uso aceptable, sin tener en cuenta si el evento fue intencional o no, ni si su origen es interno u externo. Ejemplos de transgresiones son compartir claves, utilizar recursos de una organización para fines personales, entre otros.

Es así que una vulnerabilidad que es aprovechada por un adversario dará origen a un incidente, muy posiblemente un ataque si hay intención de daño. Así se da una relación entre el tratamiento de una vulnerabilidad y la gestión de incidentes de seguridad de la información, otra de las especializaciones en materia de Seguridad de la Información, con un componente netamente técnico y aspectos relativos a los procesos y buenas prácticas, que deben llegar hasta los más altos niveles de decisión de una organización.

Entre los objetivos del proceso de gestión de incidentes se encuentran la elaboración de análisis de amenazas y vulnerabilidades y contar con información para prevenirlos o evitarlos, plantear escenarios posibles aún con todos los controles preventivos dispuestos. El otro gran objetivo es mitigar los efectos de los incidentes, preparar a una organización para un conjunto de amenazas concretas, proceso que se denomina respuesta ante incidentes. Cuando esta función existe, los procesos están implementados y probados, cuando existe un plan de respuesta y recuperación, las organizaciones están cumpliendo con requisitos mínimos e implementando las salvaguardas para las amenazas actuales.

Un acceso no autorizado, un phishing[5], un ransomware[6] o una denegación de servicio, así como un corte de conectividad, serán todos incidentes para la organización que deberían ser atendidos de acuerdo a un plan, con respuestas analizadas y preestablecidas o al menos planificadas, en sus generalidades que minimicen la incertidumbre.

Éstos tipos de incidentes se encuentran estandarizados[7] y tienen una terminología común a fin de poder compartir las amenazas que circulan en un momento determinado. Lo que no se puede establecer a priori es cómo cada uno de esos incidentes puede afectar a una organización o a quienes las organizaciones dan servicio, esto es de particular interés cuando se trata del Estado. Ese es un enorme trabajo de coordinación interna de la organización o, en particular, de cada Estado.

La gestión de incidentes de seguridad también tiene la finalidad de analizar la causa origen o raíz que produjo el incidente para que no vuelva a ocurrir, y en esta investigación de las causas suelen utilizarse los registros de auditorías de los sistemas, o logs[8] de sistemas y dispositivos. Ésta misma información es la que se utilizará en caso de que el incidente pueda además entenderse como un ataque o delito. En este sentido, cuando el objetivo es identificar las acciones, el orden y los rastros de usuarios, interviene el análisis forense que es otra de las disciplinas utilizadas en la gestión de incidentes. Así, analizar técnicamente un incidente requiere de procedimientos y estándares específicos que suelen denominarse DFIR (Digital forense and Incident response).

En síntesis, la gestión de la seguridad de la información forma parte de las actividades necesarias para mantener bajo control los riesgos derivados del uso de la tecnología. Un organismo, empresa u organización que no contemple una gestión de riesgos planificada, ordenada y que atienda a los procesos críticos, analizando las amenazas a las que se encuentra expuesta estará en severas dificultades al sufrir un incidente. En particular, porque para una gestión efectiva de estos procesos se requieren conocimientos, habilidades y capacidades específicas con las que se debe contar, tanto para las actividades que se denominan de gobierno (quien asigna recursos y administra los riesgos al más alto nivel), como en la gestión (para la coordinación de acciones con el resto de las áreas, con las

[5] Phishing es un mensaje que intenta engañar al destinatario para obtener información confidencial o lograr que el destinatario haga una acción específica como clic en un adjunto o un link.

[4] Ransomware es un tipo de código que extorsiona al destinatario, cifra archivos generalmente con el objetivo de que la organización o persona destinataria realice una acción, como un pago para luego entregar las claves y permitir el descifrado.

[7] Tabla de incidentes del Cert Nacional de Chile: https://www.csirt.gob.cl/eng/incident-classification-taxonomy, el Real Decreto de España Nro 43/2021, también tiene su tabla de incidentes: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192, Clasificación de Incidentes de Seguridad de ENISA (Agencia Europea para la seguridad de la información y las redes) https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

[8] Registros de auditorías o logs es información que los sistemas guardan para identificar a usuarios, acciones, fechas, objetos afectados y demás información técnica para rastrear errores o fraudes.

autoridades y el personal operativo) y en la operación (personal técnico calificado y con actualización permanente sobre las amenazas).

Es así que los incidentes pueden verse como la unidad a analizar en materia de seguridad de las organizaciones y también de los países en el ámbito en el que interactúan los sistemas de información, redes informáticas y de telecomunicaciones, los procesos, los datos y las personas y así es que poner los esfuerzos en prevenir, detectar, responder y recuperarse de los incidentes resulta central para medir la ciberseguridad de los países.

En los últimos estándares desarrollados en la serie de ISO/IEC 27100[9] del año 2020, se ha definido ciberseguridad como la salvaguarda de las personas, la sociedad, las organizaciones y las naciones de los ciberriesgos y a un ciberataque como intentos maliciosos de explotar vulnerabilidades en los sistemas de información o sistemas físicos en el ciberespacio[10] y dañar, interrumpir u obtener acceso no autorizado a estos sistemas.

Incidentes de seguridad de la información que afectan a datos personales

Un caso particular que merece resaltarse es cuando el incidente de seguridad de la información afecta a datos personales. En estos casos el incidente puede ser conocido como *personal data breach*[11] o *data breach*, en inglés, con nombre propio dado la frecuencia con que han aparecido y las implicancias negativas que pueden tener para los titulares de los datos.

Analizados desde la seguridad de la información, prevenir éste tipo de incidentes requiere de todos los procesos, procedimientos y tecnología que requiere la protección de la información corporativa, aunque el análisis de riesgos en la protección e inversión viene generalmente derivado del cumplimiento legal en el marco de la legislación en Protección de datos personales, en Argentina, la Ley 25326 y sus normas reglamentarias y complementarias.

Por otro lado, la respuesta ante éste tipo de incidentes requiere de un componente técnico para conocer cuál fue la causa raíz que permitió la ocurrencia del incidente, identificar responsabilidades y verificar que la organización tomó las acciones para que no vuelva a ocurrir. Además, los aspectos de debida diligencia hacia los titulares de los datos, como informarlos del incidente y asistirlos en las medidas que pueda tomar respecto de la protección de su información, en caso de corresponder, tal como se menciona en la Resolución del 17 de septiembre de 2021 de la Agencia de Acceso a la Información pública en la que sanciona a la empresa Cencosud[12]. Por ejemplo, si existiera una exposición pública de claves y cuentas de correo, utilizadas para acceder a un servicio, la recomendación debería ser cambiar la clave de inmediato.

Los equipos de respuesta ante incidentes de seguridad de la información

Con una finalidad similar a la que pueden adoptar la función de gestión de incidentes en una organización, pero distinto alcance en sus funciones, existen desde ya hace más de 30 años los Equipos de Respuesta ante incidentes de seguridad de la la Información que atienden a una comunidad en particular. Estos equipos se denominan CSIRT (Computer Security Response Team) o CERTs[13]® (Computer Emergency Response Team); los más antiguos con autorización del titular de la marca, dan atención y tratamiento a los incidentes que pueden afectar a un conjunto de organizaciones que pertenecen a un determinado sector, por ejemplo a una comunidad de Universidades, o a una comunidad de Instituciones financieras o alguna industria en particular.

Es así que son los CERTs o CSIRTs[14], las instituciones que suelen ser los canales idóneos para recibir los informes de quienes encuentran las vulnerabilidades debido al trabajo que realizan y a que cuentan con personal técnico calificado en seguridad informática que comprenden las variables y los peligros potenciales en que puede derivar una vulnerabilidad. Adicionalmente, es de destacar que como parte de los servicios básicos, éstos equipos cuentan con el tratamiento, el análisis y la respuesta a las vulnerabilidades.

[9] ISO/IEC 27100 Tecnología de la información — Ciberseguridad — Visión general y conceptos https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27100:ed-1:v1:en

[10] Ciberespacio, se define en ISO/IEC 27100 como el entorno digital interconectado de redes, servicios, sistemas, personas, procesos, organizaciones y lo que reside en el entorno digital o lo atraviesa.

[11] En el Reglamento General de Protección de Datos se define:"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; https://gdpr-info.eu/art-4-gdpr/

[12] https://www.argentina.gob.ar/sites/default/files/rs-2021-146-apn-dnpdpaaip_censurado.pdf

[13] CERT es una Marca Registrada de CERT CC, el primer Equipo de Respuesta ante Incidentes, que depende la Universidad de Carnegie Mellon.

[14] CERT y CSIRT al pie del cañón. Servicios que pueden brindar https://www.first.org/newsroom/releases/FIRST-Press-Release-20201118.pdf

Qué servicios básicos ofrecen los CERTs / CSIRTs

Servicios Reactivos	Servicios Proactivos	Servicios de Gestión de la Calidad de la Seguridad
• Alertas y advertencias • Tratamiento de incidentes • Análisis de incidentes • Respuesta a incidentes *in situ* • Apoyo a la respuesta a incidentes • Coordinación de la respuesta a incidentes • Tratamiento de vulnerabilidades • Análisis de vulnerabilidades • Respuesta a vulnerabilidades • Coordinación de la respuesta a la vulnerabilidad • Asistencia remota a vulnerabilidades e incidentes	• Comunicados y anuncios • Observatorio de tecnología • Evaluaciones o auditorías de la seguridad • Configuración y mantenimiento de la seguridad • Desarrollo de herramientas de seguridad • Servicios de detección de intrusos • Difusión de información relacionada con la seguridad • Programas de gestión de listas de configuración segura de sistemas TIC • Monitorización de redes	• Análisis de riesgos • Continuidad del negocio y recuperación ante desastres • Consultoría de seguridad • Sensibilización • Educación / Formación • Evaluación o Certificación de productos

Para los aspectos técnicos, en materia de incidentes que afectan a datos personales la OCDE[15], en un documento sobre Seguridad Digital publicado en 2014, incluía recomendaciones a los CERTs o CSIRTs, para que participen en las acciones sobre prevención de incidentes que afecten a la privacidad y la protección de datos.

Algunas de las recomendaciones son las siguientes (Recuadro 14.5):

- Se recomienda a los CISRTs participar activamente en los debates de políticas que resulten pertinentes, tanto a nivel nacional como internacional.
- Cualquier gobierno tiene derecho a crear los CSIRT que necesite, aunque conviene tomar una decisión fundada que tenga en cuenta las posibles consecuencias.
- En lo referente a los CSIRT la privacidad y la seguridad han de ir de la mano para que resulten realmente eficaces.
- El término protección de datos se entiende mejor en un sentido general que el de privacidad, por lo que es aconsejable optar por el contexto de CSIRT al ser mucho más concreto.
- El núcleo de la labor de los CSIRT debe ser la protección de los datos.

[15] OCDE 2014, Un manual para la economía digital: Gestión de Riesgos en Seguridad Digital, https://read.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe/gestion-de-riesgos-de-seguridad-digital_9789264259027-17-es#page12

- Un CSIRT bien gestionado es parte esencial de la protección de datos y la seguridad en una sociedad.
- Se aconseja un estudio más profundo de la forma en que los CSIRT y las fuerzas de seguridad puedan aumentar la cooperación de manera significativa en el marco de sus respectivas misiones.

Las vulnerabilidades en la Seguridad a nivel nacional

El análisis de las vulnerabilidades ha sido una preocupación para la seguridad de los sistemas desde que los sistemas existen. En el documento "Análisis de seguridad y mejoras de los sistemas operativos informáticos" de 1976[16] disponible en el repositorio de MITRE, esta organización sin fines de lucro fundada en 1958 para brindar asistencia técnica y de ingeniería al gobierno federal de Estados Unidos, ya se advertía el crecimiento de los riesgos por el impacto que podían alcanzar las vulnerabilidades en los sistemas operativos utilizados por el gobierno, que por ese entonces eran mayoritariamente dos. El documento se centraba en tres sistemas operativos, dos de los que mayormente utilizaba en ese momento el gobierno federal y un tercero que se analizó, teniendo información detallada y para prevenir problemas que se podían encontrar en sistemas similares.

MITRE, es la organización que lleva una de las bases centralizadas de vulnerabilidades más conocidas del mundo desde 1999[17]. Esta base conocida como CVE (Common Vulnerabilities and Exposure) es una lista de vulnerabilidades específicamente desarrollada para obtener una clasificación y categorización preliminar de las vulnerabilidades, los ataques y las fallas entre otros conceptos para ayudar a definir las debilidades habituales del software, pero no fue suficiente.

Durante el tiempo en que se elaboraba la clasificación de CVE se observó que los criterios adoptados para clasificar eran poco precisos para identificar y categorizar a las debilidades y poder evaluar la seguridad de los distintos sistemas, para realizar una evaluación efectiva se requería más información, sobre los efectos de las debilidades, los sistemas afectados, los desarrollos, etc.

[16] "Security Analysis and Enhancements of Computer Operating Systems" de MITRE, 1976. MITRE es una organización sin fines de lucro fundada en 1958 para brindar asistencia técnica y de ingeniería al gobierno federal. http://cwe.mitre.org/documents/sources/RISOSProjectFinalReport.pdf

[17] La descripción del contenido de las publicaciones de las CVE, están desarrolladas como antecedentes para la publicación de la Lista de debilidades comunes, "Common Weakness Enumeration" de MITRE, https://cwe.mitre.org/about/history.html

Fue así que, para mejorar la evaluación, MITRE hizo una revisión de las categorías CVE para su uso en la industria de evaluación de código en 2005 como parte de la participación de MITRE en el Instituto Nacional de Estándares y Tecnología (National Institute Standard and Technology, NIST en adelante) patrocinado por el Departamento de Seguridad Nacional (Department of Homeland Security, DHS) de EEUU, en el Proyecto SAMATE (Software Assurance Metrics and Tool Evaluation). Ello dio como resultado una lista preliminar de ejemplos de vulnerabilidad para investigadores, éste nuevo listado fue denominado PLOVER, (Preliminary List Of Vulnerability Examples for Researchers).

Este listado enumera más de 1500 ejemplos diversos de vulnerabilidades conocidas por su identificación bajo CVE. Las vulnerabilidades en PLOVER están organizadas dentro de un marco conceptual detallado que actualmente enumera 290 tipos individuales de debilidades y fallas de software, con una gran cantidad de ejemplos. PLOVER representó el primer intento de un esfuerzo verdadero para clasificar los casos reales, y luego realizar las abstracciones necesarias y agruparlas en clases comunes que representen vulnerabilidades potenciales más generales que podrían existir en la programación o codificación de los sistemas, y luego, finalmente para organizarlos en una estructura relativa adecuada para hacerlos accesibles y útiles para un conjunto diverso de audiencias para un conjunto diverso de propósitos.

Después de PLOVER, el siguiente paso fue establecer definiciones y descripciones aceptables de estas debilidades en el marco del proyecto SAMATE de NIST, y así se llegó a la creación de la primera publicación de la Lista de CWE (Common weakness exposure) "Enumeración de debilidades comunes" y la taxonomía de clasificación asociada en 2006. El listado de CWE no solo abarcó una gran parte de las entradas de CVE, ahora son más de 168000, sino que también incluyó detalles, descripciones y estructura de clasificación de un conjunto diverso de otras fuentes académicas y de la industria.

Este esfuerzo que implicó identificar debilidades comunes, bajo la lista CWE en sistemas de información, desde su programación o codificación tiene la intención de prevenirlos en los nuevos desarrollos, de ahí su valor y también el hecho de contar con la experiencia y conocimiento del camino recorrido hasta su creación para notar que fue necesario mucho tiempo y dedicación de especialistas, así como el involucramiento de diversas instituciones para su conformación.

Las actualizaciones a lo largo de los años fueron mejorando las descripciones y su clasificación, y también se agregaron contenidos. Por ejemplo, en el año 2014 cuando se incorporaron debilidades encontradas en aplicaciones móviles y en 2020, vulnerabilidades en el hardware, ya que los problemas de seguridad del hardware (p. ej., LoJax, Rowhammer, Meltdown/Spectre) se observaron cada vez más importantes tanto para la industria de TI como para la OT (Operational technology) y también en IoT (Internet of thing).

Se llama tecnología de operaciones (OT) a los sistemas de información e infraestructuras tecnológicas utilizadas en las fábricas industriales así como en la distribución de energía e IoT (Internet of Thing) o Internet de las cosas, a los dispositivos hogareños o de oficina que se pueden conectar y administrar en forma remota a través de Internet. Se incluyen dentro de éstas denominaciones, sistemas de control industrial y dispositivos médicos hasta automóviles y tecnologías portátiles.

En la actualidad, la actualización de la Lista CWE sigue siendo un esfuerzo de la comunidad. El mantenimiento de la lista es un proceso continuo, ya que la comunidad CWE ajusta regularmente los tipos de debilidades de software y hardware existentes y sus árboles de clasificación, desarrolla y agrega nuevas definiciones de tipos de debilidades y contenido relacionado según sea necesario para las nuevas tecnología. Además, descubre nuevas formas para que la comunidad aproveche los contenidos de CWE, como el nuevo enfoque basado en datos para generar el CWE Top 25, la lista de las 25 debilidades más frecuentemente encontradas.

Para hacer una síntesis, los investigadores y especialistas de MITRE primero conformaron la base de datos de CVE como una lista de que identifica problemas conocidos en sistemas y productos específicos de uso masivo y luego en conjunto con NIST (National Institute Standards and Technology), desarrollaron otra base de datos con CWE que clasifica los tipos de vulnerabilidades de software, de manera general y conceptual para que esos errores puedan evitarse y prevenir que alguien más los aproveche.

Estas nociones elementales sobre el tratamiento de debilidades y exposiciones de los sistemas y productos conocidos expone en sí misma una especialidad, por lo que resulta que la notificación de una vulnerabilidad pueda no ser comprendida cuando se informa a personas no entrenadas aún cuando la vulnerabilidad pueda dejar expuesta a la organización a un gran daño.

Desde otro punto de vista, entender cómo la vulnerabilidad puede afectar a la misión de una organización y tener previstos los recursos para atenderla en función al riesgo tiene como prerrequisito una comprensión general de los sistemas y sus procesos críticos, que no siempre está al alcance del personal técnico, cuando los procesos no están adecuadamente gestionados.

Un sistema para clasificar vulnerabilidades por su peligrosidad

Se ha mencionado que hay un listado CVE que identifica productos afectados por determinadas vulnerabilidades, luego la lista CWE que contiene las vulnerabilidades más frecuentes que se actualiza periódicamente. Además, la Agencia de Ciberseguridad y Seguridad de la Infraestructura (Cybersecurity & Infrastructure Security, CISA) de Estados Unidos ha creado un nuevo listado, esta vez para difundir los CVE más utilizados en incidentes, es decir las vulnerabilidades en productos que están siendo más aprovechados, este nuevo listado ha han denominado KEV[18] (Known exploited vulnerability).

Es así que los esfuerzos para promover las medidas que permitan mitigar los efectos, ya sea divulgando este tipo de debilidades, o publicando las más frecuentemente utilizadas en ataques, así como alertar a las organizaciones para que apliquen actualizaciones o medidas de mitigación cuando no existan soluciones son en definitiva todas medidas tendientes a evitar que los incidentes sucedan.

En otro proyecto para informar y concientizar sobre la peligrosidad de las vulnerabilidades existe la puntuación CVSS, que brevemente se comenta a continuación y cuya documentación y actualización se encuentra a cargo de FIRST[19], organización internacional sin fines de lucro que agrupa a la mayor cantidad de CSIRT del mundo.

Esta iniciativa trata de ayudar en la comprensión de los riesgos específicos de una vulnerabilidad estandarizando los parámetros que deben ser tenidos en cuenta a la hora de conocer el peligro que representa.

Este índice conocido como CVSS (Common Vulnerability Scoring System)[20] o Sistema común de puntuación de vulnerabilidad proporciona una forma de definir las características principales de una vulnerabilidad y permite generar una clasificación numérica que refleje su gravedad. La puntuación numérica se puede traducir a una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidades. CVSS es un estándar que utilizan organizaciones de todo el mundo.

Para definir la puntuación, es decir la gravedad, el índice se basa en tres grupos de características, el primer grupo se relaciona con la vulnerabilidad en sí misma, con seis aspectos a evaluar donde cada uno tiene distintos valores para asignar donde éstos valores no van a cambiar con el transcurso del tiempo y se llama "grupo base".

El segundo grupo, que tiene tres características que cambian en el tiempo y por este motivo se llama "grupo de métricas temporales", son: la explotabilidad, que refiere a la disponibilidad y características del código de explotación (Exploit) que aprovecha la vulnerabilidad con objetivo de acceder inadvertidamente o eliminar un archivo, etc., el nivel de remediación que se relaciona con la disponibilidad de una posible solución y el nivel de confianza relacionado a la credibilidad de la fuente que publica la vulnerabilidad. Este grupo de características da a la puntuación CVSS una condición de temporal porque con el correr del tiempo las características cambian. Por ejemplo, una vulnerabilidad que cuenta con una prueba de concepto[21] tiene una puntuación más baja que una que cuenta con un exploit que permite alguna acción que pueda utilizarse para dañar o acceder a un sistema.

Finalmente el último grupo a las que denomina "métricas del entorno" son las características que evalúan la importancia del activo de TI afectado para la organización medido en términos de controles de seguridad, sean complementarios o alternativos, implementados sobre la confidencialidad, la integridad y la disponibilidad de la información.

Es decir, que para la evaluación de la gravedad que brinda la puntuación CVSS es necesario analizar catorce características, divididas en los tres grupos mencionados, que abarcan desde la disponibilidad del código que la aprovecha y el entorno de controles que se encuentra en una infraestructura específica, hasta saber y comprender a cuál de las propiedades de seguridad de la información afecta.

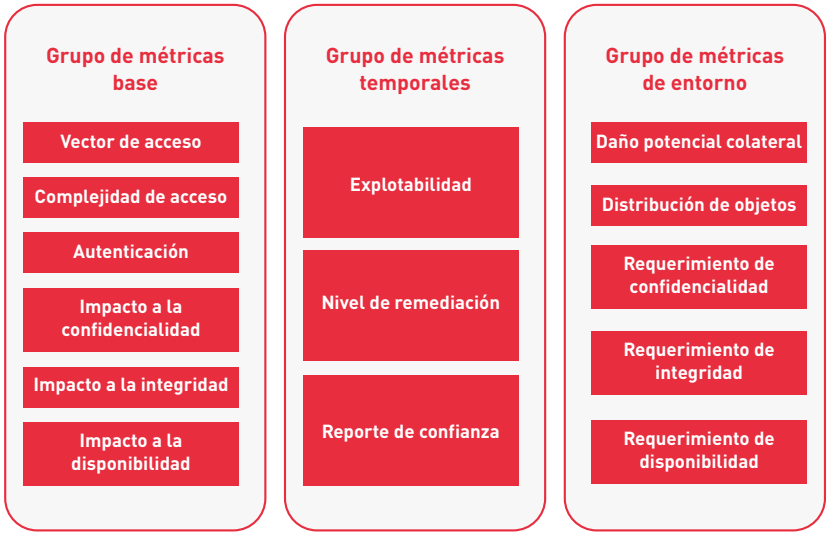
[18] KEV, Known Exploited Vulnerabilities, Vulnerabilidades conocidas que están siendo aprovechadas. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[19] FIRST. https://www.first.org/about/ FIRST se fundó en 1990 sus miembros han resuelto un flujo casi continuo de ataques e incidentes relacionados con la seguridad, incluido el manejo de miles de vulnerabilidades de seguridad que afectan a casi todos los millones de sistemas informáticos y redes en todo el mundo conectados por Internet en constante crecimiento. Febrero de 2022, 608 miembros.

[20] FIRST. Documento de las especificaciones para la puntuación del impacto de las vulnerabilidades. https://www.first.org/cvss/specification-document

[21] Prueba de concepto, en inglés PoC o proof of concept, se refiere a una explicación teórica de cómo podría aprovecharse una vulnerabilidad, también puede ser un programa cuyo objetivo es mostrar que la vulnerabilidad existe.

Gráfico de los grupos de características para la puntuación en criticidad[22] en CVSS.



Entre las características contenidas en el grupo base, la necesidad de requisitos de autenticación del usuario, puede tener tres valores: si la vulnerabilidad no requiere autenticación para ser aprovechada, si requiere permisos de usuario común, o permiso de administración. La segunda característica es la explotabilidad, que refiere al nivel de disponibilidad del código que se aprovecha de la vulnerabilidad que puede adoptar cinco valores posibles, desde la falta de información pasando por el conocimiento de que existe un código que funciona en cualquier condición, o cuando existe una prueba de concepto, hasta cuando no hay código que explote o aproveche.

Cada una de esas catorce características puede adoptar distintos valores y así se obtiene el valor final que orientará en la peligrosidad de una vulnerabilidad en un momento dado.

En el sitio de FIRST, la organización que mantiene este sistema de manera abierta, pública y gratuita; y donde se puede obtener la información completa, la versión CVSS 3.1 de éste índice tiene cinco niveles de puntuación

[22] Publicación en el blog de ESET "We live security". Vulnerabilidades: ¿qué es CVSS y cómo utilizarlo? https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

final que se corresponden con el índice de 0 a 10 de menor a mayor criticidad de la siguiente manera:

Escala cualitativa de calificación de severidad

CLASIFICACIÓN	PUNTAJE CVSS
Ninguna	**0.0**
Bajo	**0,1 - 3,9**
Medio	**4,0 - 6,9**
Alto	**7,0 - 8,9**
Crítico	**9,0 - 10,0**

Un índice alto o crítico da la categoría de una vulnerabilidad que puede afectar con cierta facilidad y de manera grave a una organización y que debe ser inmediatamente atendida para evitar un incidente.

Las vulnerabilidades y la seguridad de la información

En el marco de las buenas prácticas para la seguridad de la información de los sistemas, y en el contexto de una organización, los estándares se imponen lentamente en tanto los servicios y la digitalización se expanden. Los estándares internacionales en materia de seguridad de la información y de servicios de tecnología de la información, así como otros sobre "gobierno del dato", tienen décadas, por ejemplo, la norma BS 7799-1[23] antecedente de la ISO/IEC 27001 sobre los requisitos para un Sistema de Gestión de Seguridad de la información fue publicada en 1995.

Los institutos y organismos de normalización a nivel internacional aportan ordenamientos conceptuales, principios, modelos de procesos y consensos sobre prácticas efectivas para distintos aspectos en tecnologías de la información y las comunicaciones. En tanto todo este conjunto de recomendaciones que hacen a la normalización contribuyen a la solidez y confianza de los servicios y las tecnologías de la información como recomendaciones de la industria junto a representantes de Estados en los

[23] Seguridad de la información e ISO/IEC 27001 https://www.itgovernance.co.uk/files/Infosec%20101v1.1.pdf

foros como los de la Organización Internacional de Estándares ISO y sus grupos de trabajo.

En este sentido, entre los procesos que figuran en la mayoría de estándares internacionales de seguridad de la información, la gestión de vulnerabilidades siempre está presente, junto a la gestión de actualizaciones y la realización de distintas pruebas orientadas a la mitigación de los riesgos que se originan en vulnerabilidades.

En este sentido, la gestión de las vulnerabilidades, se encuentra vinculada a la gestión de parches que consiste en el análisis, pruebas e instalación de actualizaciones de plataformas y sistemas utilizados, que contienen nuevas funcionalidades o que también arreglan fallos de seguridad.

Sin embargo, buscar de manera sistemática vulnerabilidades, identificarlas, y mitigarlas de manera continua no siempre suele ser un proceso estándar, en algunos casos las empresas reguladas deben hacerlo por cumplimiento, en un sector regulado, o alguna norma de orden administrativo o legal.

En la actualidad, las prácticas utilizadas por las organizaciones para realizar éstas actividades son las pruebas denominadas, test de intrusión o escaneo de vulnerabilidades[24], realizadas de manera periódica, por ejemplo, anualmente. Este hecho se relaciona también con el nivel de madurez de la sociedad en estos temas[25], y de los esfuerzos de los Estados en la adopción de los diferentes estándares, que en su mayoría viene con los análisis de riesgos para evitar incidentes y en otros casos por la ocurrencia de incidentes graves que afectaron con pérdidas económicas significativas.

Como se ha mencionado, las vulnerabilidades pueden ser una puerta para el acceso a datos o sistemas, para obtener información o causar daños, en este sentido hay que mencionar que la posibilidad de que se encuentre una vulnerabilidad es más alta cuanto mayor sea el incentivo encontrarlas. En el caso de que sean descubiertas por terceros independientes, lo mejor que podría suceder es que sean reportadas a la organización y que ésta las gestione, es decir reciba, clasifique, evalúe su gravedad y las mitigue.

[24] Un escaneo de vulnerabilidades se basa en utilizar una herramienta, un software que permite probar la presencia de vulnerabilidades conocidas.

[25] Puede consultarse el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones como referencia. https://www.itu.int/es/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx

Los reportes de vulnerabilidades a nivel nacional

En un reciente estudio publicado, la OCDE[26] analiza los obstáculos para un tratamiento oportuno que brinde seguridad a todas las partes interesadas en la que se aborda expresamente la problemática de las vulnerabilidades y quienes reportan, en el marco del Grupo de Trabajo sobre Seguridad en la Economía Digital de la Comisión de Política de Economía Digital de la Dirección de Ciencia y Tecnología e innovación. En el documento se abordan los gravísimos problemas económicos que derivan de la explotación de las vulnerabilidades y los problemas judiciales en los que se han visto involucrados algunas de las personas que reportaron vulnerabilidades por una legislación que no contempla la actividad.

En el marco de la Unión Europea, es también por el lado de una nueva Directiva comunitaria, denominada "Seguridad de la Información y de las redes 2"[27] (*Network and Information Security* versión 2, NIS2), con el objetivo de elevar los niveles de seguridad de la Unión Europea que ya fueron establecidos por la primera edición de la Directiva NIS[28] en vigencia desde 2018 que contempla la obligatoriedad de coordinar la divulgación de las vulnerabilidades como una práctica para fortalecer la seguridad de la Unión.

En Europa, fue la Agencia europea para la Seguridad de la Información y las Redes *(European Network information Security Agency, ENISA),* creada en 2004, la oficina que promueve capacidades en la unión en materia de ciberseguridad y quien se encargó de los estándares sobre Divulgación Coordinada de vulnerabilidades[29], publicada ya desde 2018.

Mientras que en Estados Unidos, la Orden Ejecutiva de mayo de 2021[30] que trata sobre "La mejora de la Ciberseguridad de la Nación" estableció directivas para el tratamiento de las vulnerabilidades en varios aspectos, instaurándose luego desde la Agencia de Ciberseguridad y Seguridad de la Infraestructura (*Cybersecurity & Infrastructure Security, CISA*) un progra-

[26] OCDE, febrero 2021, Fomentar el tratamiento de las vulnerabilidades: Descripción general para los responsables de formación de políticas. https://www.oecd.org/fr/numerique/encouraging-vulnerability-treatment-0e2615ba-en.htm

[27] Proyecto de Directiva NIS2, Network Information Security https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[28] Directiva europea NIS, 2016. Un Marco para la ciberseguridad https://www.enisa.europa.eu/topics/nis-directive

[29] ENISA. Guía de Divulgación Coordinada de Vulnerabilidades (CVD) https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf

[30] Executive Order on Improving the Nation's Cybersecurity, may 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

ma para que las agencias del gobierno federal atiendan los reportes de vulnerabilidades como una forma de mejorar la seguridad de la información para el gobierno. Este programa[31] se pone en práctica a través de la Agencia de Ciberseguridad para las Infraestructuras (CISA) quien coordina la atención y la divulgación pública de vulnerabilidades (*Coordinated Vulnerability Disclosure, CVD*) en productos y servicios con las empresas que desarrollan los productos o servicios o afectados.

Estos ejemplos de regulaciones surgen después de muchos años de falta de atención del problema de las vulnerabilidades como parte de la seguridad hacia el público general.

Desde la Organización internacional de estándares (ISO) en conjunto con la Comisión Electrotécnica Internacional (IEC) ya en el estándar ISO/IEC 29147[32] Divulgación de vulnerabilidades es un documento que proporciona requisitos y recomendaciones a los proveedores y destaca "La divulgación de vulnerabilidades permite a los usuarios realizar una gestión de vulnerabilidades como se especifica en ISO/IEC 27002:2013[33], 12.6.1[1]. La divulgación de vulnerabilidades ayuda a que los usuarios a proteger sus sistemas y datos, priorizar sus inversiones en prácticas defensivas y evaluar mejor el riesgo. El objetivo de la divulgación de vulnerabilidades es reducir el riesgo asociado con la explotación de vulnerabilidades. La coordinación de divulgación de vulnerabilidades es especialmente importante cuando se ven afectados varios proveedores."

Cabe mencionar que la norma anterior ISO/IEC 29147 es citada tanto en el proyecto de Directiva europea NIS2 para abordar el tema desde las organizaciones, como por ejemplo en Ley 116-207[34] (Public Law 116–207) de Estados Unidos, de diciembre de 2020 para establecer estándares mínimos de seguridad para dispositivos de "Internet de las Cosas" de propiedad o en control del Gobierno Federal.

[31] Programa de divulgación coordinada de CISA Cybersecurity & Infraestructure Security Agency, Estados Unidos, https://www.cisa.gov/coordinated-vulnerability-disclosure-process

[32] Visualización introductoria de la norma ISO/IEC 29147 Divulgación de Vulnerabilidades, desde el repositorio de Comisión Electrotécnica Internacional, organismo que emite la publicación en conjunto con la Organización Internacional de Estándares. https://webstore.iec.ch/preview/info_isoiec29147%7Bed2.0%7Den.pdf

[33] ISO/IEC 27002 es un conjunto de buenas prácticas en materia de controles para la gestión de seguridad de la información en una organización que ISO y IEC han definido como buenas prácticas y lograr un mínimo de prácticas que hacen a la seguridad de un Sistema de información. Esta norma es una más de la serie de normas ISO/IEC 27000. https://www.iso.org/standard/54533.html

[34] "Internet of Things Cybersecurity Improvement Act of 2020" or the "IoT Cybersecurity Improvement Act of 2020". https://www.congress.gov/116/plaws/publ207/PLAW-116publ207.pdf

En este sentido, el Instituto Nacional de Estándares y Tecnología (NIST) es responsable de desarrollar estándares y guías de seguridad de la información, incluidos los requisitos mínimos para los sistemas de información federales, dependiente de la Oficina de Comercio de Estados Unidos para la economía y tiene en desarrollo un estándar de la serie 800, que corresponde a ciberseguridad sobre la divulgación vulnerabilidades en etapa de borrador.

En esta propuesta de guía se destaca "El reporte de vulnerabilidades de seguridad conocidas o sospechadas en productos digitales es una de las mejores maneras para que los desarrolladores y los servicios se den cuenta de los problemas. La formalización de acciones para aceptar, evaluar y administrar los informes de divulgación de vulnerabilidades puede ayudar a reducir problemas de seguridad conocidos. El documento tiene la intención de recomendar y orientar en la implementación de medidas para establecer un marco federal de divulgación de vulnerabilidades y destacar la importancia del manejo adecuado de los reportes de vulnerabilidades y la comunicación para minimizar y eliminar vulnerabilidades. El marco permite el apoyo a la resolución local mientras proporciona supervisión federal y debe aplicarse a todo el software, hardware y servicios digitales bajo control federal".

La gestión de vulnerabilidades y la divulgación coordinada

Como se ha mencionado, las organizaciones deberían tener su proceso de gestión de vulnerabilidades. En la actualidad, como parte del proceso para asegurar también los estándares promueven los programas de recompensas (bug bounty, en inglés) que incentivan la búsqueda de vulnerabilidades por parte de investigadores independientes, e inclusive algunos gobiernos, como en Estados Unidos o en el Proyecto de Directiva europea NIS2 están estableciendo sus programas de coordinación de vulnerabilidades (CVD en inglés).

En particular a nivel nacional o regional, éstos programas tienen la finalidad de que los organismos del Estados atiendan los reportes de investigadores puedan analizarlos y mitigarlos. La explotación de esas vulnerabilidades, en éstos últimos años por parte de atacantes, están provocando pérdidas multimillonarias como en caso de Equifax[35], espionaje a las máxi-

[35] Equifax says data breach has cost it nearly $2 billion so far https://www.bizjournals.com/atlanta/news/2020/02/13/equifax-says-data-breach-has-cost-it-nearly-2.html

mas autoridades de un país como fue en el incidente de SolardWind[36], o impedir el funcionamiento de la empresa más grande distribución de gas de Estados Unidos como en el caso de Colonial Pipeline[37].

Los programas de recompensas o Bug Bounty son instrumentos de las organizaciones más grandes y maduras para encontrar esas vulnerabilidades que aún la propia organización no ha podido encontrar pero sabe que pueden existir. Empresas como Google[38], Microsoft y muchas otras, pagan cuando alguien les reporta una vulnerabilidad y lo hacen de acuerdo a la criticidad.

Para que los programas sean efectivos, todas las prácticas básicas de seguridad de la información deben ser implementadas y gestionadas, porque si, por ejemplo, existen en uso sistemas obsoletos, o la falta de pruebas seguramente la debilidades serán múltiples.

Desde otra perspectiva, están las acciones que una persona puede realizar cuando se encuentra una vulnerabilidad. En este sentido, si decide publicar toda la información relacionada se menciona como Full disclosure, puede ser que no publique o divulgue ninguna información (non- disclosure), que intente comunicarse con la organización que tiene la vulnerabilidad o también puede contactarse con una tercera entidad para coordinar la atención de la vulnerabilidad con quien comparte la información de la vulnerabilidad. Esta última modalidad se denomina Divulgación Coordinada de vulnerabilidades, Coordinated Vulnerability Disclosure, CVD.

Una divulgación coordinada es lo deseable en tanto, como se ha comentado, las circunstancias pueden variar muchísimo y los riesgos son grandes, por estos motivos un tercero de confianza que pueda entender las complejidades técnicas es un escenario que puede beneficiar a todas las partes.

Si bien como se ha comentado las entidades deseables para coordinar son los CERT o CSIRT, las organizaciones de la sociedad civil que puedan entender tales circunstancias y el aporte que pueden brindar la atención de las vulnerabilidades al fortalecimiento de la ciberseguridad son también terceros de confianza que pueden ejercer como un punto de confianza.

[36] Un sofisticado ciberataque contra SolarWinds enciende las alarmas: el proveedor del Pentágono y decenas de grandes compañías ha sido comprometido https://www.xataka.com/seguridad/sofisticado-ciberataque-solarwinds-enciende-alarmas-proveedor-pentagono-decenas-grandes-companias-ha-sido-comprometido

[37] How a major oil pipeline got held for ransom https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices

[38] Condiciones para el reporte de vulnerabilidades de Alphabet, empresa global dueña de Google. https://bughunters.google.com/about/rules/6625378258649088

Incidentes y vulnerabilidades en el sector público nacional de Argentina

En la Administración pública Nacional de la Argentina, las primeras normas administrativa que mencionan la necesidad de dar tratamiento a las vulnerabilidades puntualmente son, por un lado, la Decisión Administrativa 669/2004[39], en la que se establecía que los organismos del Sector Público Nacional debían dictar o adecuar sus políticas de seguridad de la información, conformar Comités y asignar funciones responsabilidades en relación con la seguridad y, por otro lado, la Disposición 6/2005[40] que contenía el modelo de Política de seguridad de la información en la que puntualmente menciona:

> *2.6. Incidente de Seguridad*
>
> *Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la informaci*ón. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Cabe mencionar que las prácticas se han actualizado y ampliado, es así que recientemente la Publicación de la Decisión Administrativa 641/2021[41] deroga la 669/2004 mencionada, siguiendo las pautas de los estándares internacionales y en la que el tratamiento de las vulnerabilidades continúa presente. De la misma manera y luego de varias versiones, se ha publicado una actualización del Modelo de política que debería tomarse de referencia en la Disposición 1/2022[42] de la Dirección Nacional de Ciberseguridad y en la que también sugiere su tratamiento, en el marco de la Seguridad operativa:

[39] DA 669/2004. Solicita que los organismos del sector público nacional Aprueben su política de Seguridad de la Información en base a la Política de Seguridad Modelo, http://servicios.infoleg.gob.ar/infolegInternet/anexos/100000-104999/102188/texact.htm

[40] Disposición 6/2005 de la ex Oficina Nacional de las Tecnologías de la Información que aprueba la Política Modelo de Seguridad de la Información para organismos de la APN. http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/108672/norma.htm y https://www.unpa.edu.ar/sites/default/files/descargas/Administracion_y_Apoyo/4.%20Materiales/2018/RECT/Vigentes/124-T053-P/PSI_Modelo%20de%20Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Inf_Jul-15.pdf texto de la política Modelo.

[41] Decisión Administrativa 641/2021, Requisitos mínimos de Seguridad de la Información para organismos. https://www.argentina.gob.ar/normativa/nacional/decisi%C3%B3n_administrativa-641-2021-351345

[42] Disposición 1/2022, Modelo referencial de Política de Seguridad de la Información", https://www.boletinoficial.gob.ar/detalleAviso/primera/257620/20220216

Seguridad operativa

Las operaciones del organismo se desarrollan en forma segura, en todas las instalaciones de procesamiento de información, asignándose las debidas responsabilidades y desarrollando procedimientos acordes. Se adoptan medidas para minimizar los riesgos de acceso y cambios no autorizados o pérdida de información y para proteger las instalaciones y plataformas tecnológicas contra infecciones de código malicioso. Las vulnerabilidades son gestionadas de manera apropiada y se controla la actividad de administradores y operadores.

Asimismo, esta última Decisión Administrativa, la 641/2021, de fecha junio de 2021, es reconocida por la Sindicatura General de la Nación, órgano de control interno del Poder Ejecutivo Nacional como el marco en materia de Seguridad de la Información mediante la Resolución 87/2022[43].

Como antecedente general vale mencionar que en materia de gestión de incidentes, la normativa origen puede remontarse a la Resolución 81/1999[44] de la ex- Secretaría de la Función Pública, por la que se creaba una Unidad para la coordinación de los organismos de la Administración Pública Nacional para la atención de incidentes de seguridad, denominada ArCERT.

El reconocimiento de la importancia que debe darse a la atención de vulnerabilidades en la prevención de incidentes de seguridad se evidencia también en la "Guía introductoria a la Seguridad para el Desarrollo de Aplicaciones WEB", que publicó la Dirección Nacional de ciberseguridad mediante la Disposición 8/2021[45], de noviembre de 2021, en la que figuran tanto los principios para una codificación segura, algunas consideraciones para su mantenimiento y pruebas que ayudan a evitar los efectos de las vulnerabilidades.

A continuación se mencionan algunas prácticas que se han venido mencionando como estándares en la materia, en particular: 1 de las 5 vulnerabilidades mencionadas en la guía, asimismo se indica que tomaron como base los "Top de OWASP"[46], un proyecto que, como CWE, realiza un listado de las vulnerabilidades más utilizadas para realizar ataques.

[43] Resolución 87/2022 SIGEN, https://www.boletinoficial.gob.ar/detalleAviso/primera/257108/20220204

[44] Creación de ArCERT. Coordinación de Emergencia en Redes Teleinformáticas. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-81-1999-58799/texto

[45] Disposición Nro 8/2021 de la Dirección Nacional de Ciberseguridad, Guía introductoria para el Desarrollo seguro, https://www.boletinoficial.gob.ar/detalleAviso/primera/252690/20211111

[46] Top Ten de OWASP, Proyecto abierto y gratuito, reconocido por la comunidad de seguridad informática que contiene una lista de vulnerabilidades conocidas más utilizadas para realizar ataques. https://owasp.org/www-project-top-ten/

Ataque	*[Uso de] Componentes con vulnerabilidades conocidas.*
Descripción	*Ocurren cuando no hay aseguramiento de que se usen componentes y librerías actualizadas. O cuando hay dependencias desconocidas entre componentes.*
Amenaza	*Puede facilitar todo tipo de ataque: de inyección, xss, controles de acceso rotos, etc. Puede resultar en compromiso total del host y robo de datos*
Mitigaciones	*Inventariar continuamente las versiones de los componentes utilizados. Monitorear bases de datos de vulnerabilidades en busca de componentes utilizados. Analizar componentes instalados y evaluar si son necesarios. Aplicar actualizaciones y parches de seguridad provistos por el fabricante del componente.*

Entre las pruebas que se sugieren para mejorar la seguridad figuran:

10.4 Pruebas de Penetración

Se evalúa la seguridad del sistema desde la perspectiva de un atacante. Cumple la función de detectar vulnerabilidades que escaparon a todos los otros controles de seguridad anteriores.

Por sí sola, este tipo de pruebas no es suficiente para garantizar la seguridad de una aplicación. Corregir fallos detectados mediante pruebas de penetración, suele ser mucho menos económico que prevenirlos en etapas tempranas del ciclo de desarrollo.

10.6 Pruebas Tercerizadas y Confidencialidad

En caso de que las pruebas sean realizadas por personal ajeno a la organización se recomienda documentar las condiciones de las actividades de prueba, definiendo: alcance, objetivos, tipos de pruebas, y horarios permitidos.

Entre las actividades de mantenimiento figuran:

12.3 Reporte de incidentes y vulnerabilidades

Se recomienda ofrecer un canal de contacto para el reporte de fallos, errores y vulnerabilidades. Se deberá implementar una Base de Conocimientos para facilitar el seguimiento de cada caso.

Será necesario suscribirse a las notificaciones de seguridad del fabricante de cada componente utilizado en la aplicación. En caso de recibir información de terceros sobre vulnerabilidades que afecten a nuestra aplicación, se recomienda recabar la información necesaria para solucionar lo reportado.

12.4 Ventana de vulnerabilidad

Es el plazo de tiempo desde que se toma conocimiento de la existencia de una vulnerabilidad hasta que se produce una nueva versión o parche correctivo. Se debe minimizarla para reducir el riesgo de ataques. Se recomienda establecer procesos especiales para casos que requieran corrección urgente. Algunos dispositivos permiten mitigar temporalmente las vulnerabilidades mediante la aplicación de "parches virtuales".

12.5 Actualizaciones de seguridad

Se deberá verificar que las actualizaciones reparen efectivamente la vulnerabilidad o fallo. También deberá probarse que los cambios no generan nuevas vulnerabilidades. En caso de que las actualizaciones se instalen manualmente deberá corroborarse que no queden instancias con versiones vulnerables. Es una buena práctica publicar reportes describiendo información técnica y la criticidad de la actualización. Dependiendo del tipo de aplicación, puede ser necesario notificar a los usuarios de los cambios aplicados.

Estos antecedentes del marco administrativo nacional demuestran que la seguridad de la información cuenta con un lugar dentro de la Administración Pública Nacional desde hace tiempo, aunque sin embargo ese espacio no ha acompañado el crecimiento que la digitalización de la vida de las personas ha tenido en éstos últimos años, en el que prácticamente la vida social, económica, y política está mediada por servicios digitales, además del ámbito laboral y hasta el educativo, impulsado fuertemente por la pandemia de COVID-19 y la necesidad, en todo el mundo de distanciamiento social obligatorio.

Por otro lado deben mencionarse dos aspectos fundamentales y que van unidos indisolublemente. En primer lugar, los requisitos mínimos, las políticas de seguridad y los procedimientos son los aspectos formales y organizativos necesarios para una gestión ordenada y transparente, en la que puedan plasmarse las actividades y que, eventualmente, se pueda auditar de manera regular y sistemática, hecho sumamente necesarios en cualquier ámbito pero aún más en sector público que depende de fondos públicos.

El segundo aspecto, básico y esencial, es el del desarrollo de las capacidades técnicas necesarias para hacer frente a los riesgos, el de las habilidades y conocimientos de las personas y las herramientas a utilizar. En este sentido es clave la preparación para una respuesta desde la investigación, el desarrollo de las personas, la inversión y el análisis de los riesgos y las medidas más eficientes para mitigarlas.

En éste último sentido se debe resaltar que el desconocimiento en la toma de decisiones en este campo de conocimiento puede llevar a errores en las interpretaciones de hechos, efectos e impactos de los incidentes, afectando desde los derechos de las personas cuando son acusados por reportes de vulnerabilidades hasta por la falta de ciberseguridad para el país.

Para asistir en la adopción de las medidas técnicas más eficientes, en el uso de las mejores herramientas con el objetivo de la protección del país y su soberanía ya no es posible el asesoramiento de especialistas ad-hoc, se debe pensar en el desarrollo de instituciones dedicadas a la seguridad de la información de sus ciudadanos. De la misma manera debe promoverse el desarrollo de la formación en todos los niveles.

También es deseable el interés por los aspectos públicos desde el sector privado, tanto desde las instituciones educativas, como de formación práctica y transferencia hacia la industria, ya que forman parte del desarrollo de nuestra economía, que necesariamente requieren de la mejor formación para mejorar las capacidades internas como para la exportación de productos y servicios.

ANEXO - Incidentes de seguridad de la información con trascendencia nacional

Durante los últimos años, Argentina ha sufrido incidentes graves que afectaron tanto al sector público como al privado, con distinto tratamiento.

A continuación un breve listado de incidentes graves, en orden cronológico, con repercusión en medios de alcance local, nacional e internacional:

1. **Enero 2017: Incidente Gorra Leaks**
   Acceso no autorizado a la cuenta de Twitter, a la correo electrónico de la Ministra de Seguridad de la Nación y filtración de datos de Fuerzas de Seguridad. Enero de 2017

2. **Agosto 2019: Incidente Gorra Leaks 2**
   Filtración de datos de personal policial de la PFA, 700 GB.

3. **Agosto 2020: Incidente en la DN Migraciones.**
   Filtración de datos personales de ciudadanos registrados en la Dirección Nacional de Migraciones argentina. Ransomware.

4. **Agosto de 2020: Incidente en el Ministerio de Salud de San Juan.**
   Exposición de datos personales en el Ministerio de Salud en la provincia de San Juan.

5. **Noviembre 2020: Incidente en la Empresa CENCOSUD**
   Filtración de datos personales y financieros en la Empresa Cencosud en Argentina. Ransomware

6. **Octubre 2021: Incidente RENAPER**
   Filtración de datos personales en el Registro Nacional de las Personas RENAPER.

7. **Enero 2022: Incidente en la Justicia de Chaco**
   Filtración de datos en la Justicia de la provincia de Chaco. Ransomware

8. **Enero 2022: Incidente en el Senado de la Nación**
   Filtración de datos y denegación de servicios en el Senado de la Nación. Ransomware

Se exponen algunos artículos periodísticos de los incidentes con una breve reseña extraída de la información de conocimiento público.

1. Enero 2017: Incidente La Gorra Leaks

Reseña:

Según las publicaciones en medios y en las redes sociales, mediante un phishing engañaron y suplantaron la identidad de la Ministra de Seguridad en su cuenta de Twitter y realizaron publicaciones no autorizadas que la ridiculizaban. También accedieron a cuentas de correo electrónico del Ministerio de Seguridad, en el que se recibía información de denuncias de narcotráfico.

Artículos periodísticos:

- **Ciberataque Cómo hackearon la cuenta de Twitter de la ministra Patricia Bullrich.**
  Desde el entorno de la funcionaria hablan de "pishing". Te contamos de qué se trata esta técnica de hackeo que violenta todo tipo de datos personales.
  https://www.clarin.com/tecnologia/hackearon-cuenta-twitter-ministra-patricia-bullrich_0_ryHIoXcDx.html

- **Bullrich, tras el hackeo: "Trabajamos en ciberseguridad, pero falta"**
  La ministra de Seguridad habló con periodistas acreditados al salir del acto en el que estaba presente mientras su cuenta de Twitter era usada por hackers. Adelantó que van a iniciar acciones judiciales.
  https://www.cronista.com/economia-politica/Bullrich-tras-el-hackeo-Estamos-trabajando-en-ciberseguridad-pero-nos-falta-20170126-0101.html

- **También habrían hackeado el correo oficial de Bullrich**
  La ministra denunció la intervención ilegal de su cuenta de Twitter; podría ampliar la presentación si se comprueba que además espiaron sus mails.
  https://www.lanacion.com.ar/politica/tambien-habrian-hackeado-el-correo-oficial-de-bullrich-nid1979802/

- **Habrían usado un correo de la Embajada de Bolivia**
  Hackeo al Ministerio de Seguridad: además del Twitter de Patricia Bullrich, violaron 40 cuentas de mails.
  Una pericia de la Policía Federal confirmó que los correos electrónicos habrían sido capturados, entre ellos, el de la propia Patricia Bullrich. A la ministra le tomaron su cuenta y publicaron tuits ofensivos.
  https://www.clarin.com/politica/hackeo-ministerio-seguridad-ademas-twitter-patricia-bullrich-violaron-40-cuentas-mails_0_S1O2GiCwx.html

2. Agosto 2019: Incidente La Gorra Leaks 2

Reseña:

Una publicación en un grupo de Telegram alertó sobre la exposición de 700GB de información personal de integrantes de las Fuerzas de Seguridad, en su mayoría de la Policía Federal, exponiéndolos, como así también una gran cantidad de lo que serían archivos de escuchas de causas judiciales.

En la resolución de la Agencia de Acceso a la información pública, se menciona como una de las causas de la filtración la explotación de una vulnerabilidad por uso de una versión no actualizada de un producto.

Artículos periodísticos:

- **"La Gorra Leaks": qué hay en los archivos secretos de la Policía filtrados por hackers**.
  La gorra leak 2, Fecha de la publicación 16/8/2021
  https://www.infobae.com/sociedad/policiales/2019/08/16/la-gorra-leaks-que-hay-en-los-archivos-secretos-de-la-policia-filtrados-por-hackers

- **Se archivó la causa por una de las mayores filtraciones de datos en la Policía Federal**
  La Justicia llegó a la conclusión de que las personas sospechadas, entre las cuales figuraba el técnico informático riocuartense Javier Smaldone, no fueron responsables de la intromisión. Fecha de publicación 28 de noviembre de 2021.
  https://www.perfil.com/noticias/cordoba/se-archivo-la-causa-por-una-de-las-mayores-filtraciones-de-datos-en-la-policia-federal.phtml

- **Resolución de la Agencia de Acceso a la Información Pública. Sanción a la Policía Federal Argentina, Febrero de 2020:**
  https://www.argentina.gob.ar/sites/default/files/rs-2020-30-apn-aaip.pdf
  ARTÍCULO 1º.- Aplícase a la POLICÍA FEDERAL ARGENTINA la sanción de TRES (3) apercibimientos, configurados de la siguiente forma: UN (1)

apercibimiento por haber incumplido el deber de seguridad contenido en el artículo 9 de la Ley N° 25.326; UN (1) apercibimiento por haber incumplido el deber de confidencialidad contenido en el artículo 10 de la Ley N° 25.326; y UN (1) apercibimiento por no haber proporcionado en tiempo y forma la información solicitada por la DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES en el ejercicio de las competencias que tiene atribuidas, de conformidad a la Disposición DNPDP N° 7/05 y modificatorias.

3. Agosto 2020: Incidente Migraciones.

Reseña:

El jueves 27 de agosto de 2020 un ransomware (un software malicioso) afectó los servicios de la Dirección Nacional de Migraciones, dejando a esta Dirección sin poder brindar algunos servicios en la entrada y salida de personas del país, y con gran cantidad de información interna y datos personales de quienes salieron o entraron del país fueron expuestos.

En particular, en el artículo del diario "La Nación", se indica:

"Entre los más de 1,8 gigas de información para descargar, figuran datos personales de 25.723 argentinos repatriados, incluyendo nombre completo, DNI, domicilio, domicilio de cuarentena, lugar por donde ingresaron, desde dónde venían, número de teléfono. Según algunos especialistas que accedieron a los documentos, "no se trata de la base de datos entera de la SiCaM, sino las carpetas compartidas en la red". Todo lo que hay es aquello que era compartido en la red por diferentes empleados y partes que fueron exportadas de esa base de datos."

Artículos periodísticos:

- **Quiénes están detrás del hackeo a Migraciones y cómo funciona Netwalker, el software malicioso utilizado.**
  Secuestro de datos, extorsiones millonarias e indicios que conducen a Rusia. Cómo se lleva a cabo uno de los ciberdelitos más frecuentes. Fecha de publicación 5/9/2020.
  https://www.infobae.com/tecno/2020/09/05/quienes-estan-detras-del-hackeo-a-migraciones-y-como-funciona-netwalker-el-software-malicioso-utilizado/

- **Migraciones: cómo fue el ataque del ransomware Netwalker** y qué tipo de datos revela.
  El ransomware es un tipo de software malicioso que encripta datos de una computadora y exige un pago para descifrarlos; una nueva versión, NetWalker, también hace una copia para extorsionar a sus dueños. 10/9/2020.
  https://www.lanacion.com.ar/tecnologia/migraciones-como-fue-ataque-del-ransomware-netwalker-nid2446451/

Comunicación del organismo:

4. Agosto de 2020: Incidente Salud de San Juan.

Reseña:

Un problema de configuración dejó expuesta información de aproximadamente 100000 registros de personas en un sistema de Salud, esta información fue descubierta por una empresa que realiza servicios

de ciberseguridad que intentó alertar al Ministerio de Salud y no obtuvo respuesta. Comunicándose con el CERT Nacional dependiente de la Dirección Nacional de Ciberseguridad, quien se comunicó con la Agencia de Acceso a la Información Pública y la Dirección Nacional de Protección de Datos.

Artículos periodísticos:

- **Salud culpó a un empleado por la filtración de datos que generó un castigo de Nación.**
  San Juan recibió dos apercibimientos por infracciones graves al exponer a más de 110 mil perfiles. Fecha de publicación 01/06/2021
  https://www.diariodecuyo.com.ar/politica/Salud-culpo-a-un-empleado-por-la-filtracion-de-datos-que-genero-un-castigo-de-Nacion-20210531-0123.html

- **Escándalo internacional: se filtraron datos sensibles de 100.000 argentinos con la app del coronavirus.**
  Se conoció que hubo una brecha de seguridad en los datos personales de quienes usaron la app del gobierno. Qué pasó y qué datos están en peligro.
  https://www.cronista.com/infotechnology/online/Escandalo-internacional-se-filtraron-datos-sensibles-de-100-000-argentinos-con-la-app-del-coronavirus-20200807-0006.html

***Resolución de la Agencia de Acceso a la Información Pública sancionando al Ministerio de Salud de la Provincia de San Juan, mayo de 2021*:**

https://www.argentina.gob.ar/sites/default/files/2021/05/rs-2021-45161366-apn-dnpdpaaip_ministerio_de_salud_san_juan.pdf

ARTÍCULO 1º.- Aplícase al MINISTERIO DE SALUD de la PROVINCIA DE SAN JUAN la sanción de DOS (2) APERCIBIMIENTOS por haber incurrido en DOS (2) infracciones graves consistentes en: "[m]antener bases de datos locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen", e "[i]ncumplir el deber de confidencialidad exigido por el artículo 10 de la Ley N° 25.326 sobre los datos de carácter personal incorporados a registros, archivos, bancos o bases de datos", de conformidad con los puntos 2, incisos k) y j), respectivamente, del Anexo I a la Disposición DNPDP Nº 7/05 y modificatorias.

5. Noviembre 2020: Incidente CENCOSUD

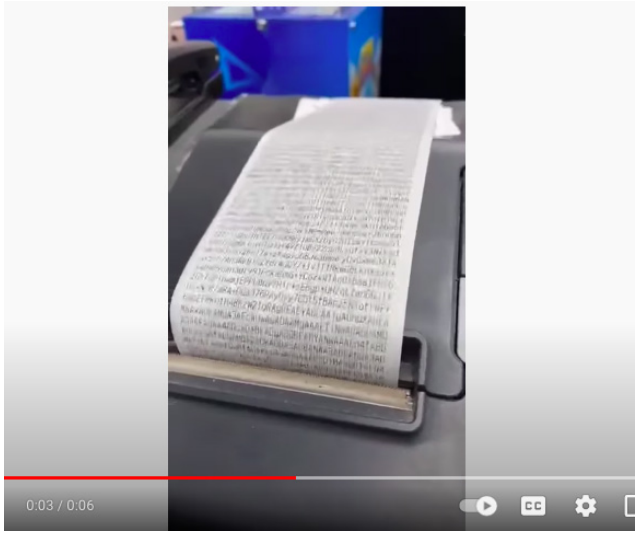
Reseña:

Cencosud, es un consorcio empresarial chileno, propietario de Jumbo, Easy, Vea y Disco, fue afectado, en noviembre de 2020, por un ransomware impidiendo su funcionamiento en varias sucursales por varios días y que sirvió para extorsionar a la firma pidiendo millones de dólares a cambio de no difundir la información de clientes comprometida en el incidente.

Este incidente fue informado primero por algunos usuarios de Twitter que publicaban que algunas de las impresoras de Jumbo, un gran supermercado imprimía en sus cajas la nota de rescate.

Ataque Ransomware Egregor a CencoSud imprime directamente la nota de rescate

- Video en el que se muestra la impresión que generaba el malware, en el artículo de Elhacker.net: https://blog.elhacker.net/2020/11/ataque-de-ransomware-egregor-hace-que-las-impresoras-nota-de-rescate-cencosud.html



https://www.youtube.com/watch?v=28bbUGeJTAc&t=6s

Artículos periodísticos:

- **Hackeron Cencosud y piden millones de dólares para no revelar la información privada.**
  Entre lo recolectado por los hackers habría "movimientos de compras y ventas de la empresa" así como datos de clientes. La multinacional tiene su propia tarjeta de crédito. Fecha de publicación 16/11/2020
  https://www.ambito.com/informacion-general/hackers/hackeron-cencosud-y-piden-millones-dolares-no-revelar-la-informacion-privada-n5148493

- **Hackeo masivo a Jumbo: es un "secuestro virtual" y hay millones de tarjetas argentinas en peligro.**
  La seguridad de la multinacional del retail chilena fue vulnerada. Qué pasó, qué es un ransomware y cómo protegerse.
  https://www.cronista.com/infotechnology/online/Hackeo-masivo-a-Jumbo-es-un-secuestro-virtual-y-hay-millones-de-tarjetas-argentinas-en-peligro-20201116-0001.html

- **Resolución de la Agencia de Acceso a la Información Pública. Sanción a la empresa Cencosud, Septiembre de 2021:**
  https://www.argentina.gob.ar/sites/default/files/rs-2021-146-apn-dnpdpaaip_censurado.pdf

  ARTÍCULO 1º.- Aplícase a la empresa CENCOSUD S.A. CUIT 30'59036076-3, con domicilio en Suipacha 1111, Piso 18 de la Ciudad Autónoma de Buenos Aires, la sanción contemplada en artículo 31 de la Ley N º 25326, normas reglamentarias y complementarias; consistente en una multa por la suma de PESOS DOSCIENTOS NOVENTA MIL ($ 290.000,00), por haber incurrido en DOS (2) infracciones graves y DOS (2) infracciones muy graves, de acuerdo con el detalle expresado en los considerandos de la medida.

6. Octubre 2021: Incidente RENAPER. Registro Nacional de las Personas.

Reseña:

Varias imágenes de personalidades de Argentina (famosos, autoridades políticas y algunos usuarios que hablan de incidentes), en particular fueron 44 imágenes de las caras, fueron publicadas en Twitter por un usuario que decía tener toda la base de datos del REGISTRO NACIONAL DE LAS PERSONAS -RENAPER-, posteriormente publicó información de fichas de del Registro, que pudo ser verificada por periodistas.
En posteriores encuentros con periodistas, quien decía ser autor de la filtración y ser el mismo del Incidente de la Gorra Leak, amenaza con publicar mucha más información de ciudadanos argentinos, mencionando que tiene la base completa de ciudadanos argentinos.

Los datos extraídos del Registro Nacional de las Personas a los que el periodismo e investigadores pudieron acceder llegan a 60000 registros con información de ciudadanos. Lo cuál constituye un enorme riesgo para la población.

Comunicado oficial del RENAPER: 13 de octubre de 2021.

https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo

Artículos periodísticos:

- **Ingreso no autorizado. Filtración del Renaper: difunden datos sensibles de 60.000 argentinos y piden cerca de 17 mil dólares por todos los DNI.**
  Desde el Gobierno investigan quién es el autor del robo de información.
  https://www.clarin.com/tecnologia/filtracion-renaper-difunden-datos-sensibles-60-000-argentinos-piden-cerca-17-mil-dolares-dni_0_2eE_kXXBo.html

- **Hackean RENAPER: habló el hacker y asegura tener copia de los datos, planea venderlos y filtrarlos.**
  El robo tuvo lugar el mes pasado. Ya filtró información sensible en Twitter y vende todos los datos en la darknet. Fecha de publicación 19/10/2021
  https://eleconomista.com.ar/tech/hackean-renaper-hablo-hacker-asegura-tener-copia-datos-planea-venderlos-filtrarlos-n47003

- **El Ministerio de Salud denunció ante la justicia la filtración de datos sensibles.**
  La cartera de Vizzoti hizo una presentación judicial en paralelo a la que había hecho el Renaper; se pidió el cambio de claves, limitaron el uso de información y habrá una fuerte inversión en ciberseguridad
  https://www.cronista.com/economia-politica/el-ministerio-de-salud-

denuncio-la-filtracion-de-informacion-que-involucra-a-mas-de-964-millones-de-datos/

- **Hacker steals government ID database for Argentina's entire population**
  A hacker has breached the Argentinian government's IT network and stolen ID card details for the country's entire population, data that is now being sold in private circles.
  https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/

7. Enero 2022: Incidente Justicia Chaco

Reseña:

Un ransomware afectó a la infraestructura tecnológica y a la información del superior tribunal causando una suspensión de servicios hacia las partes que no tenían previsto.

Los medios han reportado la falta de capacidad para asistir en los expedientes durante la afectación y la solicitud de asistencia tanto al sector público, como al privado para el análisis del incidente como para los pasos a seguir.

Artículos periodísticos:

- **Un grupo cibercriminal secuestró la base de datos de la Justicia de Chaco y ahora pide rescate**
  Hive Ransomware infectó los servidores del Poder Judicial de Chaco, afectando a más de 3.500 computadoras en toda la provincia. Aún no se conoce la completa extensión del daño. Fecha de publicación 20/01/2022
  https://tn.com.ar/tecno/2022/01/20/un-grupo-cibercriminal-secuestro-la-base-de-datos-de-la-justicia-de-chaco-y-ahora-pide-rescate/

- **Hackearon al Poder Judicial de Chaco y piden un rescate por la información**
  El Superior Tribunal se negó a negociar con los atacantes, declaró la feria hasta el lunes próximo y confía en que la pérdida de información sea, al final, "mínima". Fecha de publicación 8 /2/2022
  https://www.lanacion.com.ar/politica/hackearon-al-poder-judicial-de-chaco-y-piden-un-rescate-por-la-informacion-nid08022022/

- **Un informe confirmó la peligrosidad del virus que atacó al Poder Judicial de Chaco y se sigue buscando a los hackers**
  Infobae había detallado a inicios de enero el ataque a los servidores. La Corte chaqueña recibió los datos de un estudio que precisa cómo se generó el sabotaje. Fecha de publicación 20 de febrero de 2022.
  https://www.infobae.com/politica/2022/02/20/un-informe-confirmo-la-peligrosidad-del-virus-que-ataco-al-poder-judicial-de-chaco-y-se-sigue-buscando-a-los-hackers/

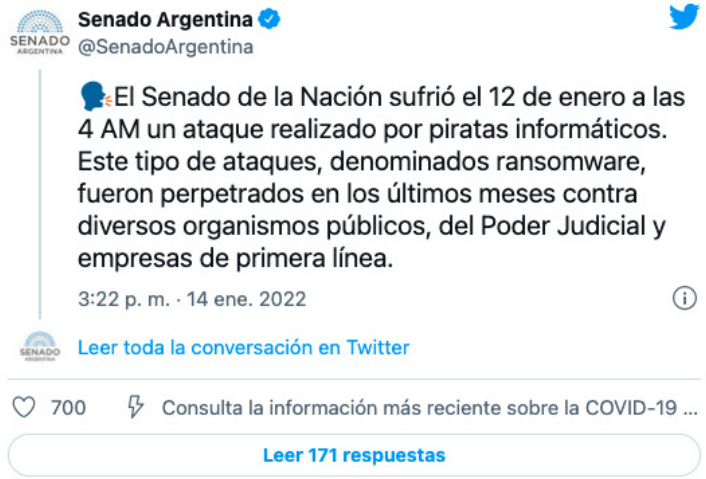
Resolución del Superior Tribunal de Justicia de la Provincia de Chaco con acciones derivadas del incidente.

https://www.diariojudicial.com/public/documentos/000/100/418/000100418.pdf

8. Enero 2022: Incidente Senado de la Nación

Reseña:

Un ransomware afectó al Senado de la Nación Argentina, y ésto fue publicado en la cuenta oficial de la siguiente manera.



Por el mismo canal, el Senado informó que el incidente no comprometió información confidencial, no obstante según se publicaron algunos medios informaron que no pudieron restablecerse un mes después.

Artículos periodísticos:

- **Hackearon los sistemas del Senado y secuestraron información**
  La Cámara alta informó que en las últimas horas sus sistemas fueron atacados por "piratas informáticos" bajo la modalidad de "ransomware". Fecha de publicación 14/1/2022.
  https://www.cronista.com/economia-politica/hackearon-los-sistemas-del-senado-y-secuestraron-informacion/

- **Hackeado hace casi un mes, el Senado todavía intenta recuperar su funcionamiento normal**
  Los ciberdelincuentes encriptaron casi toda la información de los servidores de la Cámara alta y pidieron un rescate; cientos de computadoras quedaron inutilizadas y hay documentos aún no recuperados. Fecha de publicación 9 de febrero de 2022.
  https://www.lanacion.com.ar/politica/hackeado-hace-casi-un-mes-el-senado-todavia-intenta-recuperar-su-funcionamiento-normal-nid09022022/

Comentarios generales sobre los incidentes

Los incidentes sucederán cada vez con más frecuencia y los habrá de mayor impacto, la diferencia la harán los esfuerzos en prevenirlos y actuar de la manera más planificada ante la ocurrencia.

En ninguno de los incidentes mencionados, se ha dado una explicación pública de qué falló, de cómo eran los procedimientos para prevenir incidentes para demostrar que no había más que hacer, es decir, demostrar una debida diligencia por parte de los organismos involucrados. En la mayoría de los casos, se delega en la investigación penal la única función que el Estado podría hacer ante un incidente. Luego de lo expuesto en el presente documento creemos que la investigación penal, que es necesaria y un paso, en general obligatorio, no ataca el principal aspecto de este tema, que es dotar de todas las medidas técnicas y organizativas y de infraestructura necesarias para evitar y mitigar las consecuencias gravísimas que tienen éstos incidentes, hecho en el que la investigación penal no incide en absoluto.

La atención adecuada de las vulnerabilidades es una parte muy importante, sin embargo para comprender los impactos que pueden causar, debe comprenderse el lugar de la tecnología en los servicios y cómo afecta una construcción e interconexión donde abundan las debilidades. Mejorar las capacidades de las organizaciones y el país es esencial, promover una cultura de la ciberseguridad fortaleciendo la capacitación y la concientización en seguridad informática, los procesos correspondientes y asignando las responsabilidades tanto a nivel Estatal, municipal, provincial y nacional y así como en el sector privado. La coordinación requiere pautas normativas, recursos humanos y técnicos pero también tiene una dimensión política en la que el centro debe ser la protección de las personas.

Acrónimos

CVE. Common Vulnerabilities and Exposures. Exposición y vulnerabilidades habituales.

CCN-CERT. Equipo de Respuesta ante Emergencias del Centro Criptológico Nacional (de España)

CERT. Computer Emergency Response Team. Equipo de Respuesta ante emergencias informáticas.

CISA. Cybersecurity and Infrastructure Security Agency. Agencia de seguridad de la infraestructura y la ciberseguridad.

CSIRT. Computer Security Incident Response Teams. Equipo de Respuesta ante incidentes de seguridad informática.

CWE. Common weakness exposure. Listado de debilidades habituales.

CVD. Coordinated Vulnerability Disclosure. Divulgación de vulnerabilidades coordinada.

CVSS. Common Vulnerability Scoring System. Sistema de puntuación de vulnerabilidades habituales.

DHS. Department Homeland Security.

DFIR. Digital forensic and incident response. Forensia Digital y respuesta ante incidentes.

ENISA. European Networks and Information Security Agency. Agencia Europea para la ciberseguridad.

FIRST. Forum of Incident Response and Security Teams. Foro de Equipos de Seguridad y Respuesta ante incidentes.

ISO. International Standard Organizations. Organización internacional de estándares

IoT. Internet of Things. Internet de las cosas

IEC. International Electrotechnical Commision. Comisión Electrotécnica Internacional

INCIBE. Instituto Nacional de Ciberseguridad Español.

NIST. National Institute Standards and Technology (de Estados Unidos).

NIS. Network and Information Systems. Redes y Sistemas de Información.

TO. Tecnologías de operación

TI. Tecnologías de la información