Annual Report 2022

NIVEL

ÍNDICE

INTRODUCCIÓN

Avanzar para crecer en ciberseguridad ha sido una de las experiencias más desafiantes, pero enriquecedoras, que hemos desarrollado como innovadores en tecnologías de la información en los últimos 8 años.
En este tiempo hemos aprendido que la ciberseguridad es un reto permanente, para nosotros, así como para nuestros clientes y el ecosistema en el que nos desenvolvemos.

Chile y América Latina, en general, están por detrás de las sociedades más desarrolladas en ciberseguridad. Ello, pese a que las personas adoptan las transformaciones tecnológicas al mismo ritmo que en el resto del mundo.

La consecuencia de ese ritmo de cambios sin reparos en la ciberseguridad hace que el desafío de quienes tenemos que hacernos cargo de este tema sea doble: por una parte, las organizaciones tienen que cerrar las brechas de profesionales, tecnologías y trabajar en concientización, y mientras lo hacen, también deben enfrentar riesgos que significa la adopción de más y nuevas tecnologías. Y para quienes innovamos e implementamos los cambios del futuro, hoy, la misión no es solo asegurar que nuestro mercado tenga suficientes tecnologías y herramientas en materia de ciberseguridad disponibles, sino que hacer que las organizaciones comprendan que invertir en ellas no es un gasto, sino una inversión estratégica y, en muchos casos, críticas para la continuidad operacional de los negocios, reputación de las marcas, y la integridad de las cadenas de suministro.

Los líderes de la ciberseguridad en todas las organizaciones, públicas y privadas, están en una encrucijada histórica. Deben por un lado conciliar los cambios necesarios para que sus negocios y servicios no queden obsoletos y sean comercialmente competitivos, y por otro lado, deben cuidar sus activos informáticos y los de sus clientes y usuarios frente a las amenazas cibernéticas, como las filtraciones de datos, los intentos de ataques dirigidos, o los correos de phishing con suplantaciones a marcas nacionales, por dar unos ejemplos.

La integración en la aldea global ha derribado las fronteras naturales y ha creado un espacio digital abierto a todos los usuarios de internet. Pero también ha aumentado la superficie de ataque y nos ha hecho más vulnerables, especialmente con la adopción de la remotización del trabajo, los estudios, y un sinfín de otros aspectos de la vida cotidiana que fueron la más importante consecuencia de la pandemia global.

En este mundo de cambios y adaptaciones, nace NIVEL4. Y hoy somos una empresa consolidada dedicada a la ciberseguridad y que se destaca por ser un early-adopter de las nuevas tecnologías y tendencias de seguridad informática, las que ponemos a disposición de nuestros clientes, siempre enfocándonos en las necesidades de sus negocios y servicios.

Las organizaciones que confían en nosotros saben que tienen a su disposición una serie de desarrollos y servicios que están a la vanguardia del mercado, pero también saben que detrás de esas tecnologías tenemos un equipo de profesionales y expertos altamente preparados y que están al frente de la implementación de los cambios de ciberseguridad que los negocios deben adoptar, y en la medida de sus necesidades.

En este largo camino, NIVEL4 ha desarrollado herramientas de uso interno que permitan facilitar la operación y mejorar la calidad de servicio hacia nuestros clientes, como plataformas para el registro y gestión de vulnerabilidades, plataformas para ejercicios de awareness y concientización y simulación de pruebas de phishing, entre otras.

Toda la información que hemos recopilado en avanzar y hacer madurar la ciberseguridad en nuestro ecosistema la hemos sintetizado en este informe, que reúne la experiencia de un trabajo con más de 250 clientes en rubros tales como la banca, el retail, el retail financiero, el gobierno, la fintech, la salud y la minería, entre otros.
Este informe busca ser un fiel reflejo Equipo NIVEL4del trabajo constante y dedicado, y creemos que dará mayor visibilidad sobre la situación actual de ciberseguridad en nuestro país y la proyección de ella para el futuro.

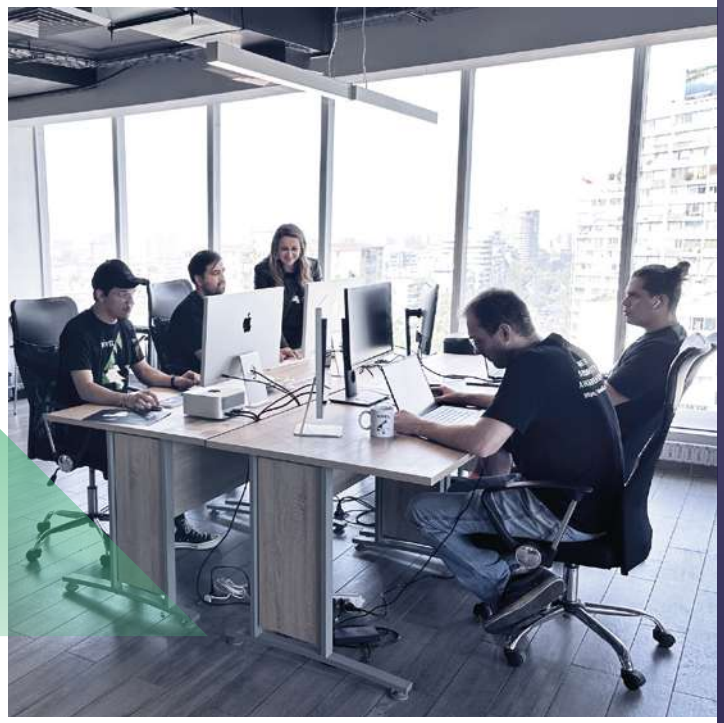
El Annual Report 2022 de NIVEL4 comparte la experiencia de varios años de trabajo, y resume estadísticamente los resultados de los servicios ejecutados por nuestros especialistas en áreas de Ethical Hacking, Red Team, Phishing Test, Ejercicios de crisis, Concientización, Forense Digital, Incident Response y Monitoreo de fuga de datos.

Con este documento, que es un valioso trabajo multidisciplinario, y que ponemos a disposición de nuestros clientes, las instituciones de gobierno, la comunidad de ciberseguridad y los medios de comunicación, también comenzamos a despedir este exitoso año 2022, pero con grandes metas y desafíos para este 2023.

Los invitamos a revisar este valioso trabajo y seguir confiando en los cambios inspirados en el uso de las tecnologías de la información, pero siempre y cuando adoptemos esos cambios con ciberseguridad.

Equipo NIVEL4

QUIENES SOMOS



NIVEL4 es una empresa chilena que nace en el año 2015, fundada por dos expertos y apasionados por el hacking, Fernando Lagos y Hernán Möller. Centrada en prestar asesoría & consultorías especializadas y dedicadas de ciberseguridad, poniendo a disposición de los clientes nuestra experiencia y conocimiento, entregando un servicio de calidad desarrollado por profesionales de primer nivel.

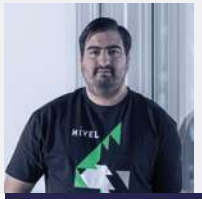
Tenemos la misión de convertirnos en un socio estratégico de nuestros clientes, ayudándolos a proteger y resguardar los activos de información y plataformas digitales frente a los distintos tipos de amenazas existentes en el ciberespacio y es con esta premisa como hemos ido ganando su confianza, sustentada en relaciones de largo plazo y desarrollando nuestras distintas áreas de negocio, las cuáles se unen transversalmente bajo las buenas prácticas y la ética.

En los últimos 8 años, NIVEL4 se ha posicionado como una empresa líder en el mercado nacional y referente en la región, con la visión de fortalecer las capacidades, procesos y la ciberseguridad de organizaciones pública, privadas, sociedad civil, instituciones militares y sectores que formen parte de la infraestructura crítica.

Hoy somos un grupo humano conformado por más de 40 expertos en diferentes áreas y tenemos más de 120 clientes que dan cuenta de nuestro compromiso, la excelencia de nuestro trabajo y cercanía en Chile y en la región, desarrollando proyectos en Perú, Colombia, Ecuador, Paraguay y Argentina.

Asimismo, potenciamos el crecimiento sostenido de la empresa y el desarrollo profesional de nuestros colaboradores.
Nuestro equipo es nuestro principal activo y el negocio de nuestros clientes es nuestra preocupación.

NUESTRO EQUIPO DE TRABAJO



Fernando Lagos Berardi
CEO y socio fundador de NIVEL4.

Durante su vida laboral previa a NIVEL4 se desarrolló como programador, administrador de sistemas GNU/Linux y Especialista de Seguridad en distintas organizaciones públicas.

Desde siempre ha sido un referente en el mundo informático y de seguridad reconocido nacional e internacionalmente por sus investigaciones, descubrimientos y publicaciones. Constantemente es invitado a exponer en eventos de ciberseguridad, además de aparecer regularmente en entrevistas para la TV o medios de prensa escritos.

Hoy está a cargo de liderar desde una visión global los objetivos y propósitos estratégicos de la empresa convirtiendo su gestión en un ejemplo que se refleja en el crecimiento sostenido de NIVEL4 de más de un 50% anual desde sus inicios.

Katherina Canales Madrid
CSO de NIVEL4.

Reconocida como mujer destacada en Ciberseguridad en Chile, y Top 25 Women in Cybersecurity en Latinoamérica.

Ex Directora operacional del CSIRT de gobierno de Chile, líder en la implementación de políticas y estrategias de ciberseguridad, con especial énfasis en la creación, implementación y maduración de los equipos de respuesta ante incidentes de seguridad informática. Co autora de la ley de delitos informáticos, normativas sectoriales y el proyecto de ley marco de ciberseguridad.

Hoy está a cargo del diseño e implementación de la estrategia corporativa que busca fortalecer el reconocimiento y crecimiento sostenido de la empresa con miras a su internacionalización.
de la empresa con miras a su internacionalización.

Hernán Möller Zavalla
COO y socio co-fundador de NIVEL4.

Antes de NIVEL4 trabajó muchos años como Especialista de Seguridad para una empresa Española, cuando en Chile la ciberseguridad aún no era un rubro establecido formalmente.

Participa en la fundación de la empresa con el objetivo de trabajar en un ambiente no corporativo, en el cual se valorará a las personas por sus habilidades y no por sus títulos académicos.

Hoy está a cargo de liderar el equipo de Operaciones y de velar por la correcta entrega de todos los servicios a los clientes de la empresa, con un sello muy propio que es posicionar a NIVEL4 como el partner de ciberseguridad de todos sus clientes y evitar que la seguridad de la organización sea una preocupación, para no perder el foco del negocio.

"CÓMO NACE NIVEL4"

Fernando Lagos Berardi
CEO y socio fundador de NIVEL4.

REMONTEMONOS A LOS INICIOS

Soy conocido como Zerial en el ciberespacio. Durante mucho tiempo estuve investigando y divulgando mis investigaciones. Estas no siempre estaban relacionadas al hacking o a la ciberseguridad, ya que muchas de las cosas que investigaba y publicaba tenían como foco Linux, open source y software libre.

Mi primer computador lo tuve aproximadamente a los 12 años. Era el típico de familia, donde se podía usar con horarios restringidos. Hasta que cambié mis cartas Magic por uno propio, por fin era mío y solo mío. Con él hice y deshice, muchas veces lo eché a perder, le rompí piezas, pero logré armar mi propio servidor en casa y en monté mi sitio web y correo. Aprendí a programar pegado las 24 horas a IRC.

Nunca trabajé en algo que no tuviera relación con la informática. Vendí mi primer software cuando tenía 20 años, era un programa de inventario para una bodega. Pasé por trabajos donde me espiaron, en una start-up muy buena, donde aporté harto y aprendí mucho (ProactiveOffice/Fidelizador) y luego de esto, a mis 23 años y gracias a mis investigaciones, me ofrecieron mi primer trabajo de ciberseguridad en CONICYT.

REFERENTE DEL BOOM DE LA CIBERSEGURIDAD

Siempre aprendiendo, investigando, escribiendo y divulgando, tanto en IRC como en foros y listas de correo de distintas índoles. Una vez que llegaron las redes sociales y se empezó a masificar el uso de internet, las empresas e instituciones comenzaron a tener mayor presencia en la red, permitiendo realizar cada vez más trámites, compras, pagos de cuentas, etc. Esto llamó mi atención y empecé a dedicarle más tiempo a las investigaciones de hacking y ciberseguridad. Como yo ya tenía conocimientos de administración de sistemas y programación, se me hacía muy fácil encontrar debilidades y vulnerabilidades. Debido a que el tema estaba tan inmaduro, inicialmente intentaba reportar a los encargados, pero nunca obtenía respuesta, y luego de meses de espera me animé a publicar la información en mi blog, lo cual empezó a tener una repercusión e interés público gracias a las redes sociales.

Mis investigaciones comenzaron a aparecer en los diarios y televisión, lo que gatilló un boom. Antes nadie hablaba de ciberseguridad y en algún momento, Zerial era sinónimo de ciberseguridad. Muchas entrevistas, muchas oportunidades de trabajo, hasta que empezaron a contactarme para asesorías y consultorías.

NIVEL4 UNA VISIÓN DE UN MERCADO NACIENTE

De aquí en adelante, cuando decidí comenzar este proyecto, sabía que no podía seguir exponiendo a las empresas, por lo tanto tenía un gran desafío: ganarme la confianza de esas empresas a las que alguna vez había expuesto o criticado.

En un principio todo fue esporádico, tenía mi trabajo full time y me dedicaba en mis ratos libres a asesorar a empresas. A medida que los requerimientos iban aumentando me faltaba tiempo, hasta que tome la decisión de dedicarme a esto. En un principio formé una empresa la cual no prosperó por falta de experiencia y conocimientos en estos temas. Sin embargo, en 2014 gracias al empuje y motivación de algunos amigos, formé NIVEL4, teniendo pleno conocimiento que la ciberseguridad iba a ser un nicho al menos durante los próximos 15 años, ya que conocía muy detalladamente cómo era la seguridad de las empresas y del gobierno y estaba dispuesto a prestar asesorías y trabajar en ello.

ENCONTRANDO UN PARTNER

Cuando comencé con este proyecto, hubo personas que se acercaron pero cuando quise pedir compromiso en el proyecto me encontré con las típicas "es que no me puedo arriesgar", hasta que le conté sobre esto a Hernán, a quien había conocido 6 años antes en un evento llamado "WebPrendedor". Creo que nos contactamos por twitter y ahí coordinamos, fue como una cita a ciegas.

El fue el único, en ese momento, que me apoyó 100%, y no nos quedó otra que tirar pa' delante. Renuncié a mi trabajo, y por varios meses no recibimos sueldo. No fue hasta 8 o 9 meses aproximadamente que logramos “estabilizarnos”. Teníamos una oficina en un zócalo, era un piso -1 que estaba entre la calle y un subsuelo, teníamos una ventana en la oficina por la que se veían las ruedas de los autos. En esta oficina se crearon varias cosas, fue donde hicimos crecer a NIVEL4 hasta que nos pudimos cambiar a una oficina un poco más decente en la calle Serrano.

PENSANDO EN GRANDE Y SUS RESULTADOS

En un principio la empresa era para ser independientes y trabajar haciendo lo que más nos gusta, sin embargo, nadie dimensionó el desafío que significaba, tener que aprender otras cosas más allá de la informática, como, contabilidad, asuntos comerciales, tributarios, finanzas, administración de empresas, etc. Cuando más del 50% de nuestro tiempo lo consumía la burocracia, es cuando empezamos a pensar en grande y crecer como equipo.

Hoy tenemos dos oficinas en Providencia, somos un equipo de más de 40 personas, atendemos a más de 100 clientes y somos reconocidos como una de las mejores empresas de ciberseguridad del país.

NIVEL4 tiene una proyección de crecimiento del 100% para el próximo año. Buscamos atender al doble de clientes, duplicar el equipo de trabajo y consolidarnos como la mejor empresa de ciberseguridad del país, con miras a una expansión en la región.

"SERVICIOS"

Los servicios de NIVEL4 se agrupan en los 4 pilares fundamentales de la defensa de la ciberseguridad, lo que nos permite satisfacer con una mirada integral las necesidades de las organizaciones en materia de ciberseguridad.

Seguridad ofensiva: Tiene por objeto atacar sistemas y romper defensas, buscando puntos débiles en personas, procesos y tecnologías, lo que permite identificar de una forma proactiva el grado exposición y las vulnerabilidades que tiene una organización con servicios como Ethical Hacking, RedTeam, Phishing Test, Cybersecurity Assessment y Ejercicios de Crisis.

Seguridad defensiva: Es la especialidad dentro de la ciberseguridad que se ocupa de proteger a una organización y garantizar la efectividad de los controles y protocolos de seguridad. Está dada por acciones de defensa interna de la organización contra ciberataques y amenazas, cuando las organizaciones buscan "fortalecer los muros del castillo" para que nadie pueda comprometer las defensas, requieren tomar acciones que les permitan protegerse, responder y concientizar ante ciberataques, con servicios como Awareness, Forense digital, Hardening, Incident Response y Monitoreo de fuga de datos.

Cumplimiento normativo: Nuestra experiencia y conocimientos los ponemos al servicio de nuestros clientes para ayudarlos en el cumplimiento e implementación de marcos normativos, regulaciones y normativas en materia de ciberseguridad.

Células ágiles: Uno de los retos a los que se enfrentan las organizaciones es la demanda de nuevos perfiles tecnológicos, que se integren con el fin de formar o integrar células de trabajo para un proyecto en particular o diversas iniciativas del negocio y para ello puedes contar con nuestros especialistas para hacer frente a las necesidades de tu organización.

1 Seguridad Ofensiva

Ethical Hacking
RedTeam
Phishing Test
Ejercicios de Crisis
Cybersecurity Assessment

2 Seguridad Defensiva

Awareness & Entrenamiento
Forense Digital
Hardening
Incident Response
Monitore de Fuga de datos

3 Células ágiles

Célula ágil de Ethical Hacking
Célula ágil de Arquitecto de seguridad
Especialista de Cumplimiento
de ciberseguridad
Especialista DevSecOps
Especialista Técnico Ciberseguridad OT
Security Advisor

4 Cumplimiento Normativo

DevSec0ps / Ciberseguridad en el SDLC
Consultoría ISO 27001
Consultoría CIS

SEGURIDAD OFENSIVA

1.- Ethical Hacking

Los ataques informáticos son cada vez más sofisticados, dañinos y difíciles de prevenir, es por ello que a la hora de llevar a cabo un adecuado sistema de prevención y respuesta a ciberataques, es fundamental tener en cuenta las auditorías y análisis a los sistemas, aplicativos, infraestructura y redes.

El Ethical Hacking es el mecanismo que utilizan las organizaciones para evaluar sus entornos TI en busca de vulnerabilidades que les permita identificar por un lado los riesgos de ciberseguridad y la gestión de los mismos, evaluando vulnerabilidades, analizando y categorizando las debilidades explotadas, además de proveer recomendaciones en base a las prioridades de la organización, y por último eliminar dichas vulnerabilidades para garantizar que están protegidos frente al continuo aumento de las ciberamenazas.

La protección de los sistemas y redes actuales requiere una comprensión amplia de las estrategias de ataque y un conocimiento profundo de las tácticas, herramientas y motivaciones de los ciberdelincuentes. Para abordar esto NIVEL4 cuenta para la prestación de este servicio con profesionales expertos y de primer nivel, los cuales utilizan las mismas técnicas que los ciberdelincuentes, con el fin de descubrir si existen vulnerabilidades de seguridad, y explotarlas de forma segura y controlada.

Tipos

1. Ethical Hacking Web (Aplicaciones Web):

El servicio de Ethical Hacking a aplicaciones o plataformas web consiste en detectar, enumerar, validar y documentar las debilidades y vulnerabilidades que puedan existir en ellas. Este análisis se basa en pruebas manuales realizadas en base a la experiencia y conocimiento de nuestros especialistas con el apoyo de herramientas automatizadas, lo que permite abordar una mayor superficie de ataque frente al objetivo. Las pruebas de seguridad web se pueden ejecutar bajo las modalidades Blackbox, Graybox y Whitebox.

Para poder realizar las pruebas de seguridad, las plataformas son sometidas a distintos tipos de pruebas que permitan detectar vulnerabilidades que puedan afectar la integridad, confidencialidad y disponibilidad de la información, las cuales se realizan de manera transversal a las aplicaciones así como las pruebas específicas dependiendo del tipo de aplicación, ello con el fin de garantizar una mirada integral de la seguridad.

Las pruebas de seguridad son realizadas de acuerdo a OWASP Testing Guide, catalogadas según OWASP TOP 10 Web y CWE, y una evaluación de riesgo e impacto en base a CVSSv3.

2. Ethical Hacking Mobile (Android / iOS):

Las aplicaciones móviles, se han transformado en un recurso muy usado y valioso de las organizaciones de cara a los usuarios, de ahí la importancia de descubrir las vulnerabilidades de ellas, tomando en consideración, que la mayoría de los ataques exitosos a las aplicaciones móviles tiene como vector de entrada las vulnerabilidades de las aplicaciones móviles generados por errores de configuración de los desarrolladores.

El servicio de Ethical Hacking a aplicaciones móviles permite evaluar de manera efectiva la seguridad de estas, y detectar, enumerar, validar y documentar las debilidades y vulnerabilidades que puedan existir realizando pruebas de intrusión, que sirven para verificar y evaluar la seguridad de las aplicaciones operativas, buscando la verificación de ella.

Este análisis se basa en pruebas manuales con el apoyo de herramientas automatizadas, lo que permite abordar una mayor superficie de ataque frente al objetivo. Estas pruebas se pueden ejecutar en entornos iOS y Android y en la modalidad de análisis estático o dinámico.

Las pruebas de seguridad son realizadas de acuerdo a OWASP Testing Guide, catalogadas según OWASP TOP 10 Mobile y CWE, y una evaluación de riesgo e impacto en base a CVSSv3.

3. Ethical Hacking API

Las APIs cumplen un rol fundamental en el funcionamiento de las aplicaciones web y móviles, por este motivo, los análisis realizados por NIVEL4 consideran las últimas tecnologías del mercado como: GraphQL, Rest API, XML y SOAP.

El servicio de Ethical Hacking a APIs o WebServices consiste en detectar, enumerar, validar y documentar las debilidades y vulnerabilidades que puedan existir. Este análisis se basa en pruebas manuales con el apoyo de herramientas automatizadas, lo que permite abordar una mayor superficie de ataque frente al objetivo. Las pruebas de seguridad web se pueden ejecutar bajo las modalidades Blackbox, Graybox y Whitebox.

Para poder realizar las pruebas de seguridad, se definen una serie de pruebas que se realizan de manera transversal a las aplicaciones y también pruebas específicas dependiendo del tipo de aplicación, que permitan detectar vulnerabilidades que puedan afectar la integridad, confidencialidad y disponibilidad de la información.

Las pruebas de seguridad son realizadas de acuerdo a OWASP Testing Guide, catalogadas según OWASP TOP 10 Web y CWE, y una evaluación de riesgo e impacto en base a CVSSv3.

4. Ethical Hacking de Infraestructura

El proceso de análisis de infraestructura incluído dentro del servicio de ethical hacking, permite realizar una revisión general sobre la infraestructura que soporta la aplicación web: como los puertos y servicios expuestos, análisis de implementación SSL/TLS, cabeceras de seguridad, entre otros.

Los hallazgos detectados mediante el análisis de infraestructura pueden requerir mitigación por el área de sistemas para realización de hardening a nivel de configuración.

Las pruebas consideradas bajo este análisis de infraestructura son las siguientes:

- **Comunicación**
- **Cabeceras**
- **Puertos y servicios**

5. Ethical Hacking a Infraestructuras Críticas, SCADA, ICS, IoT

La seguridad, confiabilidad y disponibilidad en las industrias modernas se pone en riesgo con la explosión de la conectividad de los sistemas OT como PLC, ICS y SCADA con el mundo IT. La complejidad aumenta para las industrias ya que cada sistema, sensor y red debe evaluarse y protegerse de ciberataques.
Los actores de amenazas tienen mucho que ganar cuando atacan a los ICS. Un ataque exitoso tiene impactos serios en cualquier organización, los que incluyen la paralización de las operaciones, el daño en equipos, pérdidas financieras, robo de propiedad intelectual, además de riesgos sustancias para la salud y la seguridad.
Los actores de amenazas tienen diferentes motivos al elegir una empresa como blanco de ataque, a menudo motivados por ganancias financieras, una causa política o incluso un objetivo militar. Los ataques pueden ser patrocinados por el estado o también pueden provenir de competidores, personas internas con un objetivo malicioso e incluso hacktivistas.

NIVEL4 contribuye a la mejora de la ciberseguridad de la infraestructura industrial esencial tanto de empresas públicas y privadas, al identificar brechas y vulnerabilidades que pueden afectar la continuidad operacional, en los procesos de integración, adopción de nuevas tecnologías que pudieran afectar la disponibilidad, integridad y seguridad de datos.

Expertos:

Diego Gallegos
Especialista en Ciberseguridad

¿Qué tan necesario es realizar auditorías de seguridad?

La respuesta directa es sencilla, realizar actividades de análisis de seguridad siempre es necesario, no solo orientado al cumplimiento de procedimientos, ya que las normativas ISO 27001 o PCI-DSS exigen la realización de pruebas de seguridad en los aplicativos o activos que puedan ser desplegados para una solución, si no que también es necesario desde la filosofía de mantener una intención de resguardo sobre los datos que son administrados por alguna de las plataformas/soluciones/aplicaciones disponibles, por ejemplo, ya sea porque contienen información sensible del negocio, manejan datos de clientes, contienen información bancaria, etc.

Por otro lado, también es importante considerar el ámbito reputacional de la organización, dada la visibilidad actual de la seguridad informática al nivel de usuario promedio, ahora existe la consideración por parte de la población de preferir organizaciones que sean, al menos reputacionalmente, seguras. Hoy por hoy, la gente entiende, al menos de forma básica, el término "protección de datos personales".

Dado lo anterior, es que podemos decir que realizar pruebas de seguridad es un requisito fundamental a la hora de disponibilizar cualquier activo en la red, ya sean recursos internos o expuestos públicamente a internet.

¿Cada cuanto tiempo se recomiendan?

En este punto es importante tener en cuenta el grado de madurez de la solución, no es lo mismo una plataforma web que se encuentra en desarrollo, que un aplicativo que ya lleva años expuesto públicamente.

Un aplicativo que se encuentra en desarrollo, requiere de ser analizado a medida que se vayan realizando los despliegues de funcionalidades para detectar de forma temprana, posibles brechas importantes además de evitar que posibles vulnerabilidades se repliquen en diferentes secciones de la solución, por lo que las actividades de análisis pasan a formar parte de la célula de desarrollo, acompañando la tarea de despliegue.

Por otro lado, los proyectos que ya han sido desplegados con consideraciones de desarrollo seguro, y que cuentan con implementaciones de seguridad, vale decir, que ya se encuentran en un estado más "pulido", requieren de realizar actividades de análisis de forma continua para acreditar que el estado actual de seguridad coincide con los esfuerzos dedicados para ello.

Adicionalmente, es muy importante mencionar, que cada vez que se realiza un nuevo despliegue sobre una plataforma existente, el estado de seguridad actual puede cambiar, debido a que existe la posibilidad de lograr detectar vulnerabilidades asociadas a estos nuevos componentes.

En general la realización de auditorías de seguridad suelen ser incómodas para proveedores o clientes, ya que cuentan con ventanas de tiempo acotadas para el desarrollo de soluciones y despliegue a producción, por lo que se recomienda que sean realizadas teniéndose en consideración en los tiempos previstos, de modo que forme parte de un trabajo colaborativo, no solo para poner a disposición de los usuarios funcionalidades que puedan simplificar sus necesidades, sino que también, asegure la confidencialidad de sus datos.

Ronald Herrera
Especialista en Ciberseguridad

¿Qué significa que las pruebas de seguridad que realiza NIVEL4 sean realizadas de acuerdo a OWASP Testing Guid, catalogadas según OWASP TOP 10 Web y CWE y una evaluación de riesgo e impacto en base a CVSSv3?

Se traduce en que seguimos una metodología internacional de la industria de la ciberseguridad, lo cual nos permite mantener los altos niveles requeridos en las revisiones que realizamos, asegurando la calidad de cada pentest. Abarcamos el rango de pruebas indicados en dicha metodología (OWASP) y su debida categorización (CWE) como guía en cada prueba/control realizada(o), de esta manera podemos reflejar lo más fehacientemente posible la realidad de cada hallazgo indicando su alcance y posibles vías de mitigación al cliente.

Dado que el CVSSv3 es una de las formas de catalogar los riesgos/impactos de cada vulnerabilidad, es necesario acotar cada hallazgo a la realidad del proyecto, de esta manera ajustamos el valor de la criticidad según corresponda a cada ambiente/aplicación. En NIVEL4 nos preocupamos de catalogar los hallazgos de manera correcta para que nuestro cliente pueda entender el real impacto de lo reportado.

2.- Red Team

La seguridad ofensiva se está convirtiendo en tendencia al considerarse como un paso más allá de la seguridad tradicional. Mediante el empleo de un enfoque proactivo basado en el análisis de cuándo, dónde y cómo es probable que se produzca un ciberataque.
Por otro lado, los ataques informáticos son cada vez más avanzados y sofisticados, y las organizaciones no siempre cuentan con expertos dentro de sus equipos para enfrentarse a esos desafíos, ya que se necesita pensar y meterse en la mente de un atacante siendo lo más creativo posible.

Un ejercicio de red team consiste en hackear una empresa sin importar el punto de entrada. Es decir que puede ser la infraestructura expuesta a internet, mediante un proveedor, realizando ataques de ingeniería social, pruebas físicas desde sucursales, entre otros.

El objetivo principal del servicio de RED TEAM, es utilizar todas las técnicas disponibles para encontrar puntos débiles en personas, procesos y tecnologías para obtener acceso no autorizado a los activos críticos del negocio.

Como resultado de estos ataques simulados, se realizan recomendaciones y planes sobre cómo fortalecer la postura de seguridad de una organización. Ello dado que las organizaciones tienen dificultades para detectar nuevas tácticas y técnicas empleadas por los ciberdelincuentes que buscan romper sus defensas. La única forma segura de frustrar las posibles amenazas cibernéticas es descubrir las debilidades y vulnerabilidades desconocidas en los sistemas y las defensas existentes.

En los ejercicios de RED TEAM se utiliza una variedad de técnicas y herramientas para aprovechar las brechas dentro de la arquitectura de seguridad, que pueden ir desde pruebas de penetración como el Ethical Hacking, hasta técnicas de Ingeniería social como un Phishing Test o mezcla de distintos ejercicios para lograr el objetivo final, incluyendo pruebas presenciales y pruebas remotas.

Experto:

Ignacio Espinosa
Especialista en Ciberseguridad

¿Qué habilidades requiere un experto en RED TEAM?

Los ejercicios de Red Team se caracterizan por buscar un propósito claro: vulnerar la seguridad de una organización y llegar tan lejos como se pueda para evaluar la existencia y efectividad de los controles de seguridad. Como en la mayoría de los casos, un objetivo así de abstracto conlleva mucho desarrollo en el diseño de las tareas que permitan cumplir la meta. Es por esto que un experto en ejercicios de Red Team no sólo debe ser una persona con experiencia y conocimiento técnico avanzados, sino que debe ser:

Organizado: es de suma importancia que el profesional pueda definir claramente un camino a seguir durante el ejercicio, realice una documentación constante de sus hallazgos y tenga siempre a disposición la información recolectada para poder responder ante las dudas del cliente.

Paciente y Perseverante: la cantidad de pruebas y focos que puede tomar un ejercicio de Red Team son variados y muy numerosos, donde muchas veces los resultados no permiten vulnerar de manera inmediata una organización. Es por esto que el experto debe realizar todas las pruebas necesarias, sin caer en juicios anticipados de la seguridad de una organización, ni descartar tareas por lo difícil que puedan parecer los escenarios del análisis.

Creativo: a pesar de contar con una gran experiencia, existen casos en que el experto no tendrá vectores de ataque claros e inmediatos desde el inicio de un actividad, forzandole a realizar un proceso de análisis y creatividad que le permita unir puntos que, aunque aparentemente distantes, determinen el éxito en la detección y vulneración de fallas de seguridad que existen en la organización.

Interesado y con facilidad para el aprendizaje continuo: a medida que las tecnologías se desarrollan, también se expande su adopción por las empresas y organizaciones. Es por eso que un experto debe estar siempre en conocimiento de las tendencias en el uso de sistemas y plataformas empresariales, así como de las novedades que existan respecto a técnicas y vulnerabilidades que las puedan afectar.

Adaptable a distintos escenarios: son incontables la cantidad de plataformas y tecnologías utilizadas por las diversas industrias que puedan necesitar un ejercicio de Red Team. Es por eso que el experto debe estar siempre dispuesto a aprender y lidiar con los sistemas utilizados por la organización, encontrando en cada uno de ellos un potencial vector de ataque en vez de verlos como limitaciones del ejercicio.

Excelente en su capacidad comunicativa: si bien en el ejercicio de Red Team se puede evaluar si se logró o no vulnerar la seguridad de una organización, es crítico que el cliente entienda claramente qué y cómo sucedió. De esta manera el experto debe ser capaz de explicar claramente los alcances del ejercicio, las pruebas realizadas, los controles de seguridad correctamente implementados, los problemas detectados, los impactos que puedan generar las vulnerabilidades que fueron explotadas y las recomendaciones para prevenir que estos ataques puedan ser realizados por un actor malicioso. De esta manera la organización podrá tener toda la información necesaria para realizar las acciones correctivas de sus sistemas y proteger de manera adecuada sus recursos.

3.- Phishing Test

El phishing, y sus variantes como vishing y smishing, son unos de los ataques más prevalentes en el mundo y tienen el potencial de atacarnos a todos: desde empresas grandes y pequeñas, hasta instituciones e incluso a personas naturales. Sus objetivos pueden ser muy amplios, como distribuir malware, robar contraseñas y datos personales, extraer información confidencial o cometer fraudes. Esto lo convierte en una amenaza de primera categoría.
Los phishing son ataques que avanzan a pasos agigantados, imitando grandes marcas, copiando la voz y estilo de mensajes, así como implementando técnicas para que el usuario no tenga dudas del correo que está abriendo. Estar conscientes de los métodos que utilizan los atacantes, como también los peligros que estos presentan para las personas y las organizaciones, nos ayudará a crear un ecosistema seguro.

El servicio de Phishing Test permite planificar, ejecutar y medir una simulación de ataque de phishing de manera controlada y dinámica. Mediante un Phishing Test, una organización puede medir y tener conocimiento sobre las brechas existentes al momento de identificar un correo malicioso, de esta manera es posible conocer el nivel de susceptibilidad que tiene la organización a recibir un ataque masivo de phishing, o bien un ataque dirigido en un contexto real por parte de un ciberdelincuente.

El objetivo de una simulación de ataque de phishing es identificar a las personas que no cuentan con los conocimientos ni habilidades necesarias para detectar un ataque de este tipo, con el fin de poder realizar sesiones de concientización y de esta forma mitigar el riesgo

Características principales del servicio

- **Gestión 360:** Nos encargamos de preparar la campaña de phishing, enviarla y generar el reporte.
- **Campañas personalizadas:** Preparamos cada ejercicio de phishing de manera personalizada, abordando temáticas acordes al contexto actual.
- **Simulamos un ataque real:** Nuestros ejercicios de phishing se realizan en base a situaciones reales
- **Reportes de análisis de comportamiento:** Realizamos comparaciones con campañas de phishing anteriores entregando métricas en base a estudios de comportamiento.
- **Resultados segmentados:** Nuestros reportes pueden ser segmentados con diferentes variables como el cargo, tipo de usuario, ubicación, entre otros.
- **Garantizamos un alto porcentaje de no repudio de los usuarios.**

Junto al servicio de Phishing Test, NIVEL4 ha desarrollado una plataforma que permite acceder en tiempo real a los datos de comportamiento de los usuarios mientras se esté ejecutando la campaña de phishing. Podrás obtener información como:

Estado de envío de la campaña: Cantidad de correos enviados y cuántos faltan por enviar.

Apertura del correo: Usuarios que abrieron y leyeron el correo malicioso.

Clics: Usuarios que ingresaron a una url dentro del mail.

Ingreso de información: Usuarios que cayeron en el phishing e ingresaron sus datos en un sitio falso.

Descarga los resultados: Exporta los resultados obtenidos hasta ese momento.

Experto:

Diego Vargas
Especialista en Ciberseguridad

¿Cuándo podrían no ser efectivas las pruebas de Phishing en una organización?

Las pruebas de Phishing Test se utilizan para encontrar falencias en la cultura y concientización de seguridad de los colaboradores de una organización. Se busca mostrarle a las personas las distintas formas que tienen los atacantes de tratar de engañarlas, desde correos muy genéricos hasta mensajes totalmente dirigidos y personalizados. De esta forma, se genera la costumbre de revisar y validar el origen y el contenido de la información que nos llega, confirmar dominios y enlaces, y finalmente, reportar cualquier mensaje potencialmente sospechoso.

Sin embargo, muchas organizaciones no lo ven de esta manera. Consideran que hacer caer a muchas personas con un mensaje dirigido no es bueno, por lo que intentan facilitar su detección por medio de errores de ortografía, uso de recursos de mala calidad y una mala redacción del mensaje, cosa que un atacante dedicado no hará. A fin de cuentas, el riesgo más alto lo suponen los ataques personalizados y más difíciles de detectar.

Otra área que suele perjudicar el rendimiento de las pruebas de Phishing Test es la política interna de la organización o su sindicato de trabajadores. Estos normalmente restringen las actividades que puedan engañar a los colaboradores a entregar información personal o privada, incluso en ambientes controlados, lo cual no permite preparar a las personas contra ataques reales, ya que no tendrán dichas restricciones. Estas decisiones, aunque bien intencionadas y necesarias en muchos casos, pueden terminar perjudicando a la persona individualmente, como también a la organización completa.

4.- Ejercicios de crisis

Durante el estado previo a la declaración de un ciberincidente es necesario que toda organización esté preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo pueden ser la diferencia entre una gestión eficaz de un incidente o un desastre absoluto, ya que, en el momento en que se declare un incidente ya será tarde para comenzar a planificar.

Un ejercicio de crisis permite situar a la empresa en una situación en la cual se hayan visto vulnerados sus sistemas, permitiendo evaluar el comportamiento del SOC, correcta ejecución de los protocolos de seguridad y procedimientos de actuación, la cadena de mando, entregando una visión de cómo se comportaría la empresa bajo la materialización de un ciberataque.

El principal objetivo de un ejercicio de crisis es poner en evidencia las falencias que puedan tener los mecanismos de protección, la eficacia de los procedimientos y el actuar de los equipos, con fin de poder mejorarlos y estar debidamente preparados frente a un escenario real de ataque.

Los ejercicios de crisis que realiza NIVEL4 son estratégicamente planificados tomando en consideración el tipo de empresa, amenazas principales del rubro en que opera, cantidad de usuarios, infraestructura y la amenaza de riesgos latentes.

Los ejercicios pueden consistir en:

- **Simulaciones de ataques de phishing**
- **Ataques DoS/DDoS**
- **Infección por malware como ransomware, cryptominner, etc**
- **Filtración de información sensible, entre otros.**

Experto:

Ignacio Espinosa
Especialista en Ciberseguridad

¿Cuáles son las claves para el éxito de un ejercicio de crisis?

Los Ejercicios de Crisis se caracterizan por enfocarse en la validación de procesos de detección, alerta y mitigación de potenciales ataques a los que se pueda ver objeto una organización. A diferencia de otros tipos de actividades, los Ejercicios de Crisis no tienen como objetivo comprometer la seguridad de los clientes, sino evaluar su capacidad de respuesta. Es por esto que entre los puntos más importantes para llevar a cabo un Ejercicio de Crisis efectivo están:

Definición clara de los controles a evaluar: es de suma importancia tener claridad sobre qué sistema se está poniendo a prueba y qué reacciones deberían generarse por parte de la organización ante la acción de los expertos de seguridad. Esto tiene un impacto directo en la expectativa que se genera del ejercicio y la evaluación de los resultados.

Diseño de tareas y límites de la actividad: así como el objetivo de un Ejercicio de Crisis no es la vulneración de sistemas, es vital acordar las pruebas y acciones a realizar durante la actividad, tomando en consideración cuáles serán los límites aceptables para la organización de manera de no afectar la continuidad del negocio. En general un Ejercicio de Crisis no debería significar una pérdida productiva real para la organización, sino sólo ser una ventana que refleje la preparación que esta tiene ante potenciales amenazas.

Coordinación durante la actividad: es imprescindible realizar la actividad en coordinación con una contraparte de la organización, de manera que esta pueda alertar ante posibles problemas y pueda entregar la retroalimentación necesaria pasar de una tarea a otra dentro de la actividad o modificar la intensidad con la que se realiza la simulación del ataque.

Documentación: al final de un Ejercicio de Crisis, y si se realiza correctamente coordinado, el cliente ya tendrá una idea general del resultado de la actividad. Sin embargo, sin un reporte final que indique claramente las tareas realizadas y con qué parámetros fueron llevadas a cabo, la organización no podrá realizar las afinaciones de sus controles de seguridad de manera adecuada.

5.- Cybersecurity Assessment.

El servicio Cybersecurity Assessment de NIVEL4 consiste en una evaluación general de ciberseguridad en la que se encuentra una organización y se ejecuta en virtud de una serie de pruebas y evaluaciones técnicas que permiten identificar y evaluar el riesgo cibernético, el Cybersecurity Assessment no es un análisis completo de la ciberseguridad organizacional, sino que es un levantamiento inicial que permite conocer el estado del arte y conocer los riesgos inmediatos frente a las amenazas latentes que hay hoy en día en internet.

El Assessment se compone de una serie de pruebas técnicas que se ejecutan, como ataques de phishing, evaluación de exposición organizacional, búsqueda de vulnerabilidades de las plataformas tecnológicas, entre otros.

Este servicio permite medir a nivel general el nivel de riesgo, mediante un indicador (cybersecurity risk score), evaluación que refleja las acciones necesarias para elevar el nivel de ciberseguridad desde una mirada agnóstica, transversal a la compañía y acorde al negocio.

Adicionalmente, este servicio es una simulación de un ciberataque controlado y supervisado, por lo que permite evaluar los controles de seguridad existentes. Este ataque debería ser detectado por los equipos especializados, permitiendo evaluar la detección y reacción frente a este tipo de incidentes.

Experto:

Fernando Lagos
CEO NIVEL4

¿Cuál es el valor que entrega el servicio a la gerencia o al directorio?

Un ciberataque puede poner en riesgo la continuidad operacional de una compañía, dañar su reputación e incluso afectar económicamente mediante multas, ventas o la caída del valor de las acciones. En los últimos cinco años hemos sido testigos como caen las acciones de las empresas después de un ciberataque o cómo este provoca pérdidas en la continuidad operacional teniendo un impacto directo en el negocio.

Las compañías han estado creando departamentos o áreas de ciberseguridad, generando grandes inversiones. El servicio de Cybersecurity Assessment ayudará a dar visibilidad sobre la efectividad de estas decisiones mediante un proceso que dura tres semanas, donde se entrega una visión general de todas las pruebas ejecutadas, junto con las recomendaciones necesarias para mejorar.

Mediante un Cybersecurity Assessment nos ponemos en los zapatos de un ciberdelincuente para planificar y ejecutar un ciberataque controlado, y de esta forma poder agregar valor a la gestión en ciberseguridad que se está realizando actualmente. En la práctica consiste en la búsqueda de información expuesta de la compañía en redes sociales, foros relacionados con ciberdelitos, deep o dark web, data breaches de otras compañías que pudieron haber afectado, recopilación de información relacionada a los colaboradores o empleados, con el fin de realizar ataques de phishing, búsqueda y análisis de vulnerabilidades en los sistemas más críticos.

¿Cual es el resultado de un Cybersecurity Assessment?

Una vez finalizado el Cybersecurity Assessment, una organización podrá conocer su indicador de riesgo cibernético, permitiendo responder cuatro interrogantes:

1. Phishing: ¿Cual es la susceptibilidad de la organización a recibir un ataque de phishing y enfrentarse a una posible fuga de datos o ciberataque que pueda poner en riesgo la continuidad operacional?

2. Vulnerability: ¿Existen vulnerabilidades en las plataformas que puedan poner en riesgo la confidencialidad, integridad o disponibilidad de la información, generando un daño reputacional o afectar a la continuidad operacional?

3. Exposure: ¿Qué tipo de información correspondiente a la organización hay hoy en internet accesible por cualquier persona y que pueda significar una amenaza cibernética al ser utilizada por alguien para realizar un ciberataque?

4. Data Breach: ¿Los activos tecnológicos o las personas han sido afectadas por alguna filtración o divulgación de información de manera involuntaria, poniendo en riesgo la privacidad, continuidad operacional y la reputación de la compañía?

Finalmente, permite responder una gran pregunta:

¿Estamos preparados para recibir un ciberataque?

SEGURIDAD DEFENSIVA

1.- Awareness y concientización

Hoy en día, las empresas y organizaciones están invirtiendo en tecnologías, políticas y servicios para garantizar su ciberseguridad. Pero no importa cuántos esfuerzos sean destinados para contar con las más rápidas, eficientes y sofisticadas soluciones cibernéticas del mercado. Si los usuarios que acceden a la información no tienen conciencia sobre la ciberseguridad al gestionar los activos informáticos, podrían realizar acciones riesgosas que pondrán en peligro la continuidad del negocio.
La educación de los usuarios en materia de ciberseguridad y fraudes digitales, ayuda a evitar la mayor parte de los incidentes que ocurren comúnmente en las organizaciones. El 90% de las brechas de seguridad comienzan por un error humano. Si las personas que utilizan la información lo hacen aplicando medidas simples pero eficientes, o si tienen los suficientes conocimientos como para advertir sobre situaciones sospechosas, los equipos de seguridad TI pueden actuar a tiempo para contener y mitigar incidentes.

Crear concientización entre los grupos de usuarios es esencial en las empresas y organizaciones, porque son las personas quienes usan la información para poner en marcha el negocio.

Nivel4 es especialista en la concientización de usuarios en ciberseguridad y fraudes digitales a través de estrategias de contenido y gestión de la cultura organizacional, con el objetivo de disminuir potenciales brechas de seguridad.

Para implementar de manera efectiva nuestro plan de concientización, diseñamos una metodología que consta de 6 etapas: 1. Sensibilización, damos a conocer un problema, contexto o situación; 2. Educación: entregamos la información específica; 3. Conocimiento: colaboradores retienen el material entregado; 4. Habilidades: construcción de estas en base al conocimiento y la práctica; 5. Hábito: las habilidades obtenidas se ponen en práctica y forman parte del día a día; 6. Cambio cultural: Un número suficiente de personas incorporan los nuevos hábitos.

Las estrategias de concientización que desarrollamos identifican a los distintos segmentos de colaboradores y sus insights, ejecutando planes específicos para cada uno de ellos y logrando permear de manera efectiva en la cultura organizacional. Hay 3 grupos que siempre están presentes en una organización: Dirección/gerencia, equipos técnicos y usuario general.

En relación a los equipos técnicos, es indispensable educarlos con contenido específico sobre la gestión técnica, regulaciones, controles y normativas específicas del sector.

Este servicio consta de diversas acciones y actividades tales como:

Cursos e-learning: Cursos para todo usuario de niveles básico, intermedio y avanzado, adaptados a la identidad de marca de cada organización y elaborados en los formatos actuales requeridos por las principales plataformas de enseñanza online. A nivel personalizado diseñamos cursos para equipos técnicos que requieran adquirir o actualizar conocimientos (Owasp, CIS, NERC CIP, Gestión técnica de ciberseguridad), así como cursos para directivos que requieran interiorizar temas específicos.

Charlas: A través de casos reales y ejemplos prácticos introducimos a los participantes de cada sesión en el mundo de la ciberseguridad, mostrándoles los riesgos a nivel personal y laboral. Trabajamos distintos enfoques de acuerdo al público objetivo, llevándolos de lo general a lo particular. Las charlas son una buena instancia para mostrar qué está haciendo el equipo de ciberseguridad de la organización, cuáles son sus políticas y normativas internas, así como canales de ayuda y reporte de incidentes o fraudes.

Videos y cápsulas digitales: El material audiovisual permite entregar información a los usuarios de forma rápida, sencilla e inteligente, facilitando el aprendizaje y la experiencia de los colaboradores de una organización. Desarrollamos micro-cápsulas con animaciones que explican diversas temáticas, ideales para compartir en boletines, charlas o pantallas en oficinas. Un punto a destacar es la posibilidad de personalizar el contenido en base a los lineamientos de la marca, de modo que este no produzca rechazo o los usuarios lo desconozcan.

Boletines: Son una herramienta de email-marketing que permite mantener informados a los usuarios acerca de diversos temas relacionados con ciberseguridad. Mediante la generación periódica de boletines es posible establecer un vínculo y disponibilizar un canal para acercar a los colaboradores con los equipos de ciberseguridad, permitiendo difundir el material gráfico y audiovisual que se haya generado, así como también noticias y actualidad. La clave de los boletines, es que nos permiten obtener estadísticas de apertura, reapertura y clics, además de poder segmentar el contenido por grupos o enviarlo a todos los usuarios, convirtiéndose en una herramienta sumamente útil a la hora de agregar KPIs.

Gráficas digitales y Afiches Impresos: La difusión de contenidos gráficos, permite concientizar con educación, traspasar buenas prácticas y recomendaciones sobre ciberseguridad no sólo a los equipos técnicos, sino que también transversalmente a todos los colaboradores de una organización con el fin de prevenir e informar sobre los riesgos que existen en el ciberespacio. Con los modelos de trabajo híbridos, muchos colaboradores reparten su tiempo entre la oficina y el teletrabajo, por lo que integrar una estrategia de contenido online y offline ayudará a la retención del contenido de manera rápida.

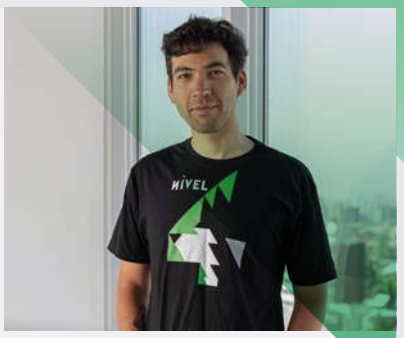
Wallpapers: Piezas gráficas con recomendaciones sobre ciberseguridad y fraudes digitales. Concientizar a través de diversos elementos es clave, por lo que utilizar el escritorio de nuestras estaciones de trabajo debe ser parte de nuestra estrategia.

Trivias y quiz: Aprender jugando, permite intencionar un juego para provocar una enseñanza-aprendizaje, potenciando el conocimiento, facilitando el aprendizaje y generando un momento de distracción positivo. Cuando uno juega, se de cuenta o no, siempre aprende algo. Los quiz, en tanto, nos permitirán medir el nivel de madurez en ciberseguridad de una organización, ya sea como evaluación inicial en un plan de concientización, como para medir su avance e identificar puntos débiles.

Pruebas de Ingeniería Social: Realizamos diversas pruebas de ingeniería social, con el fin de complementar, a través de ejercicios prácticos, el plan de concientización. 1. Vishing: Consiste en simular una llamada telefónica fraudulenta, previo estudio de la víctima, con el objetivo de recopilar información o lograr que la persona realice una acción. 2. Pruebas físicas: Ingresar a un recinto corporativo, vulnerando medidas de seguridad con el fin de obtener información o realizar baiting.

Phishing Test: El servicio de concientización funciona de manera conjunta con el servicio de phishing test, ya que ambos se complementan, aportando este último la parte práctica a través de los ejercicios de correos maliciosos. Es por esto que, al diseñar una estrategia de concientización, sugerimos integrar ambos servicios.

Experto:



Augusto Oporto
Security awareness

¿Cuáles son los atributos de las campañas efectivas de awareness?

A través de múltiples campañas realizadas, hemos podido determinar puntos claves para que una estrategia de concientización sea efectiva: Deben ser persistentes en el tiempo, transversales en la organización o compañía, ir de lo general a lo particular sin asumir el conocimiento de las personas, sino que evaluándolo e identificando los puntos débiles, y su diseño debe ser 360, es decir que abarque múltiples aristas como: la creatividad del contenido, los canales de comunicación, las acciones offline, enfocándose en todos los colaboradores, ya que el riesgo de ciberseguridad no es 100% tecnológico.

¿Cómo podría fallar una campaña de awareness?

Las campañas de concientización son una pieza clave en la estrategia de ciberseguridad de una organización, que requieren otorgarles la suficiente importancia de modo que cumplan su rol en la gestión del cambio del capital humano. Uno de sus beneficios es que ayuda a que los colaboradores dejen de ser los vectores de entrada y se conviertan en la primera línea de protección.
Pero para que no fallen y se cumplan los objetivos, las campañas de awareness deben integrar a las diversas áreas de la organización que podrían estar involucradas, como el equipo de ciberseguridad, TI, comunicaciones internas, recursos humanos y gerencias. Cuando los altos cargos y jefaturas son concientizados sobre los nuevos riesgos digitales, estos traspasarán la información a sus equipos de trabajo, facilitando el proceso de sensibilización.

2.- Forense digital

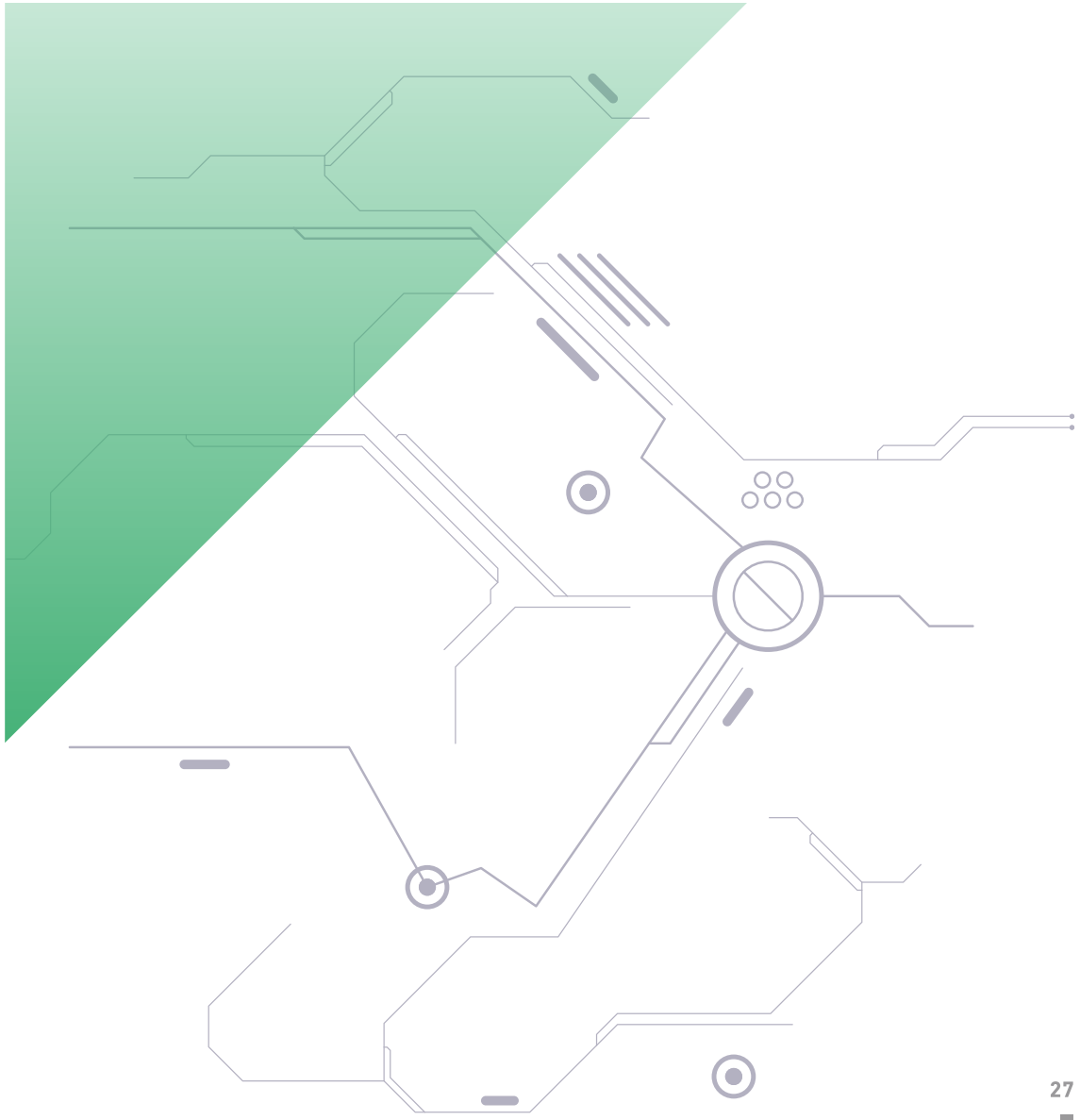
La informática forense es la rama de la ciencia forense que se ocupa de recuperar, almacenar y analizar datos electrónicos que pueden constituir evidencias que ayuden en las investigación criminal.
Durante la investigación forense digital, los especialistas forenses enfrentan desafíos como extraer datos de dispositivos dañados o destruidos, ubicar elementos de evidencia individuales entre grandes volúmenes de datos y garantizar que sus métodos capturen datos de manera confiable sin alterarlos de ninguna manera.

El proceso de análisis forense digital suele ser complejo, ya que en cada peritaje el analista se enfrenta a un escenario desconocido como sistemas operativos con distintas versiones, kernels diferentes, exploits y efectos que varían entre uno y otro archivo de evidencia.

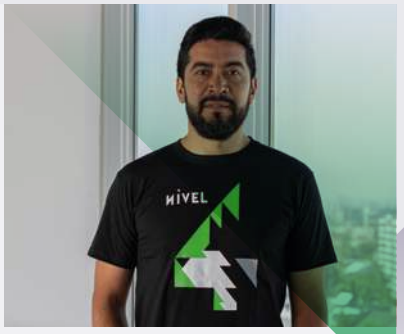
El servicio de forense digital que presta NIVEL4, se caracteriza por el análisis exhaustivo a distintos tipos de componente o dispositivos y se realiza en dos modalidades a fin de cumplir con dos objetivos de valor para las organizaciones:

Forense digital con fines probatorios: consiste en la extracción y recolección de información que pueda constituir una evidencia digital que pueda servir como prueba ante un proceso judicial si es que el incidente reviste las características de delito . Esta información puede permitir llegar a descubrir a él o los causantes de un delito informático.

Respuesta forense que corresponde al análisis exhaustivo que tiene por objeto poder determinar las causas de un incidente de seguridad, búsqueda de indicadores de compromiso, documentar el incidente, análisis de artefactos, datos borrados, vectores de explotación que sirvan para fines de documentación y análisis posterior.



Experto:



Andres Godoy
Especialista en ciberseguridad

¿Cuáles son las etapas de un análisis forense digital?

Tal como la serie de ficción CSI, en la vida real existe la disciplina Cyber Forensics la cual lleva la ciencia criminalística aplicada a la investigación de entornos digitales. En nuestro país puede ser conocida con diferentes nombres entre los cuales están Digital Forensics, Forense Digital, Pericia Informática, Peritaje o Análisis Forense, y su alcance va desde dispositivos de almacenamiento digital de información, hasta elementos electrónicos que generen algún tratamiento de datos. Muchos procesos son importantes, pero uno de los principales es que exista una metodología la cual permita a diferentes investigadores llegar a las mismas conclusiones del investigador original.

Sin embargo, rigurosas etapas deben ser respetadas de principio a fin para no exponer a riesgos la integridad de la evidencia original. Esto dado que el enfoque principal busca dar respuesta a la comisión de un delito o crimen y sus resultados deberán ser expuestos a un ente persecutor, abogados o un tribunal, siendo

Estas técnicas de investigación involucran el correcto tratamiento de evidencia ya sea electrónica o digital, preocupándose principalmente de las etapas de identificación, recolección, preservación, análisis y documentación. Cada una de las fases mencionadas involucra un estudio y planificación, nada queda al azar ya que incluso el mismo transporte o condiciones medioambientales podrían arruinar los dispositivos.

Actualmente existe una delgada línea entre responder a un incidente informático o tomar la decisión de realizar un análisis forense. Pero cómo resolver esa interrogante, según mi punto de vista el informe pericial debe realizarse cuando quien lo requiere necesita plasmar los hechos investigados en un documento formal el que incluso pueda ser presentado frente a una autoridad tanto de una organización, como de un organismo externo. En ocasiones, quien realiza un informe de este tipo puede ser nombrado “perito judicial” aunque también puede presentarse en un proceso penal como “testigo experto” jurando o prometiendo frente a un tribunal, respecto a las actividades realizadas sobre la evidencia y sus correspondientes conclusiones.

Sin lugar a dudas cada rama de la ciberseguridad es interesante y el análisis forense no deja de serlo. Frecuentemente te enfrentas a nuevos desafíos, ello implica estudiar sistemas muy poco conocidos, es necesario documentarse y crear ambientes de prueba para revisar ciertas evidencias, sumado a lo anterior debes buscar mecanismos para evitar alterar estos soportes digitales que pasan a ser la única fuente original de información que podría aclarar tanto un incidente como un delito o crimen.

En lo práctico, forense se traduce en realizar una serie de procedimientos, entre los que destacan el “triage” cuando las circunstancias lo ameritan, es decir, rescatar aquellas evidencias más importantes en un momento dado. Esto podría necesitar dispositivos físicos que previenen la escritura dando pie a otros procesos ya sea de adquisición o clonación. Sin embargo, también se requieren habilidades técnicas, conocimientos de sistemas operativos, pensamiento crítico y analítico, sin dejar de lado habilidades blandas o comunicacionales para exponer frente a una autoridad o juez, por lo que adicionalmente debes poseer ciertos conocimientos legales.

3.- Hardening

Es el conjunto de actividades que son llevadas a cabo para reforzar al máximo posible la seguridad de un sistema operativo, con el propósito de eliminar tantos riesgos de seguridad sea posible y reducir la superficie de vulnerabilidad de un sistema a amenazas cibernéticas, ello mediante la detección de vulnerabilidades en el mismo. Al minimizar la superficie de ataque, los agentes maliciosos tienen menos medios de entrada o puntos de apoyo potenciales para iniciar un ciberataque.

Mediante el servicio de Hardening es posible realizar un levantamiento de las configuraciones de seguridad que puedan tener los distintos componentes de una infraestructura, ya que una de las claves del Hardening es la configuración de los ajustes. Mientras más funciones realice un sistema, más vulnerable se vuelve, por tanto es recomendable considerar el endurecimiento del sistema a lo largo de todo el ciclo de vida de las TI.

El Hardening tiene como objetivo tener conocimiento de configuraciones débiles, por defecto o configuraciones realizadas de manera incorrecta que puedan significar un riesgo a nivel de ciberseguridad y procura lograr un entorno en el que sea posible desarrollar las operaciones regulares de las organizaciones reduciendo la superficie de vulnerabilidad, el Hardening implica auditorías regulares y metódicas, identificación, corrección de vulnerabilidades y ajustes de configuración para hacer más seguros los sistemas.

Experto:

Roberto Diaz
Especialista en ciberseguridad

¿Cuáles son las mejores prácticas de hardening del sistema operativo?

Con base en la experiencia de estar en ambos lados del escenario, tanto ofensivo como defensivo, creo que hay algunos puntos a considerar que son vitales y que en la práctica generan un impacto mayor en la seguridad del componente a proteger.

Algunas de ellas son:

- Asegurar la aplicación de actualizaciones de seguridad en todos los componentes de software/hardware de la organización, si no es posible implementar mecanismos para su aplicación automatizada, se deben generar políticas que permitan asegurar que las versiones de cada elemento están controladas y actualizadas. Una estrategia de actualización correcta permitirá a la organización responder de forma rápida a eventuales vulnerabilidades.

- Eliminar a todo nivel el uso de protocolos vulnerables. Ya sea porque no permite características básicas de seguridad, como por ejemplo protocolos que no implementa cifrado. Porque corresponden a versiones obsoletas con vulnerabilidades conocidas. O por ser vulnerables por diseño, como es el caso de varios protocolos legados de Windows y que hasta el día de hoy hemos detectado, que se mantienen en uso en algunas organizaciones.

- Gestión del control de usuarios. En este punto caen todas los controles que tienen que ver con:
  - Contraseñas: Se debe exigir una complejidad mínima, un tiempo de vigencia máximo y evitar el uso de contraseñas por defecto.
  - Eliminar cuentas de usuarios que no están activos en la organización.
  - Controlar la no proliferación de usuarios sobre privilegiados.

- A nivel físico, el control de medios extraíbles y el cifrado de los dispositivos de almacenamiento.

- Por último, se debe asegurar el despliegue de soluciones de seguridad en el endpoint así como un correcto monitoreo de eventos generados en él.

4.- Incident Response

Hoy en día, las empresas y organizaciones están invirtiendo en tecnologías, En ciberseguridad no es tan importante considerar si se producirá un ciberataque, sino cuándo. Es por eso que la respuesta a incidentes no solo es una actividad importante para los CSIRT, sino también una operación de seguridad crucial para organizaciones de todos los tamaños, industrias y tecnologías.

La respuesta a incidentes es la reacción a un ataque cibernético donde se identifica a los actores de la amenaza, intenta contener el incidente de seguridad, erradicarlo de la red y luego concentrarse en recuperar el sistema o la red después del ataque. Esto incluye sacar conclusiones y acumular conocimientos que luego se pueden usar para fortalecer las defensas de seguridad de las organizaciones.

El servicio de Incident Response implica una serie de acciones operativas que se materializa en proveer apoyo directo, in site o remoto, a las organizaciones en la contención, mitigación, recopilación de evidencia y análisis de esta en un incidente informático, y realizar las labores de contención y erradicación de los sistemas afectados.

El Incident Response tiene por objetivo reducir el tiempo de respuesta de un incidente, ya que mientras más rápida y efectiva sea, se puede minimizar el daño financiero, a los equipamientos y software causado por un incidente, dejando en manos de expertos el análisis en tiempo real de las amenazas, reduciendo su impacto incluyendo protocolos de registro, pruebas y evidencias que permitan beneficiarse de las lecciones aprendidas.

Experto:

Andres Godoy
Especialista en ciberseguridad

¿Cómo debiera abordar la respuesta en materia de incidentes de ciberseguridad una organización?

La respuesta a incidentes conlleva una serie de etapas, no obstante, dentro de las principales se encuentran la de detección, análisis, contención y erradicación.En lo práctico esto implica una búsqueda frenética del vector de entrada, intentar remover los accesos del atacante y expulsarlo de la organización, o detener la propagación del malware dentro plazos muy acotados. En paralelo, el área comunicacional debería trabajar en conjunto con los abogados y preparar al directorio para estar al tanto de lo que está ocurriendo, qué acciones se están llevando a cabo y cuáles son los siguientes pasos. Sumado a esto, riesgo operacional se encargará de sus tareas propias pero, tal vez lo más importante, será establecer el impacto que generó el atacante, si hubo exfiltración y desde cuándo y saber si aún sigue dentro de la red.

Todo parece complicarse aún más cuando entra en juego el concepto de “Análisis Forense Digital”. Estos procedimientos provienen del mundo policial y judicial donde la evidencia cobra un valor sagrado y su integridad debe ser preservada a lo largo de la investigación. Por una parte Respuesta a Incidentes busca la celeridad y si ello implica ocupar las mismas máquinas para resolver el problema, esto se hará, mientras que lo Forense persigue todo lo contrario, es decir, evitar que las evidencias sean manipuladas y alteradas para no afectar un futuro procedimiento penal o civil. Además, el proceso forense en estricto rigor realiza un análisis completo a un volumen de datos y puede tardar un tiempo demasiado prolongado para una respuesta a incidentes.

5.- Monitoreo de fuga de datos

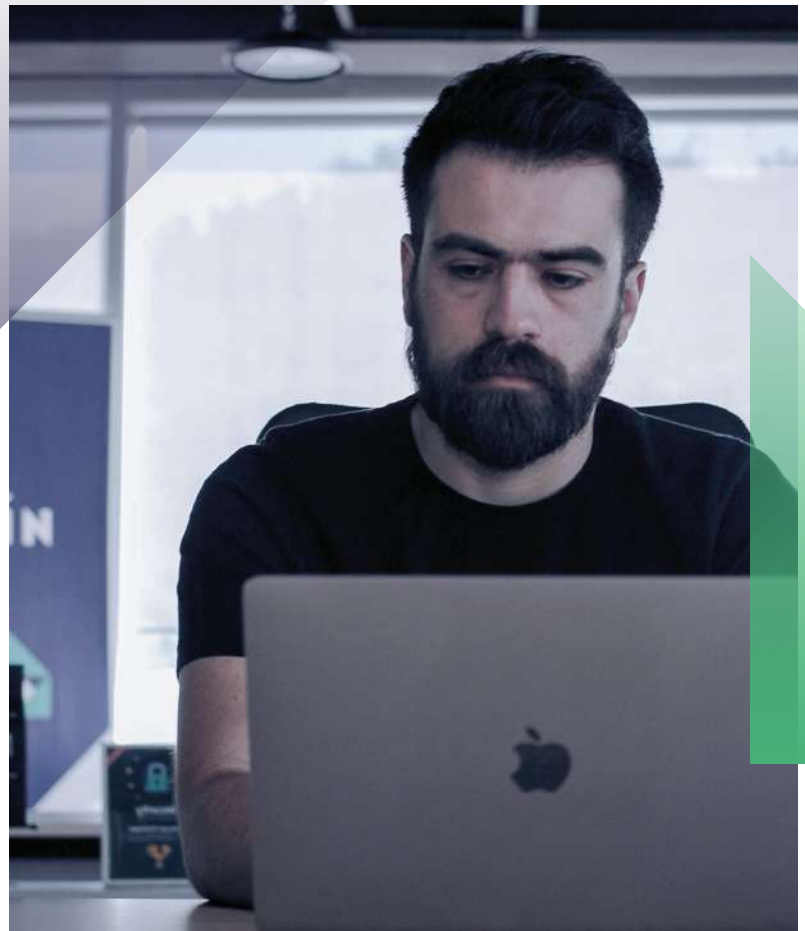
Las organizaciones están generando y recibiendo continuamente grandes cantidades de datos los cuales necesitan ser almacenados y protegidos contra el robo, la pérdida y el uso indebido. Sin importar que los datos sean almacenados internamente o en repositorios en la nube, esta información está sujeta a las amenazas de la exfiltración o fuga lo que afecta a las organizaciones de múltiples maneras.

La exposición de información sensible es una seria amenaza a la confidencialidad de la información personal y de las organizaciones y puede ocurrir tanto de manera accidental como maliciosa. El costo de una simple brecha de seguridad en una organización en términos financieros, de reputación de imagen y en la confianza de los consumidores, puede significar el colapso de la propia organización, por lo que este tipo de amenazas se ha convertido en una de las principales prioridades para los equipos de seguridad.

El servicio de Monitoreo de fuga de datos permite al cliente visualizar a tiempo alguna fuga de información que pueda afectar la reputación de la institución y la continuidad operacional. El servicio consiste en realizar búsquedas bajo demanda sobre posibles fugas de información que puedan existir tras alguna alerta que se genere mediante redes sociales o de manera interna.

El objetivo del servicio es detectar posibles fugas de información crítica corporativa, o de datos sensibles de usuarios como: Datos PII (Información personal identificable), número PAN o tarjetas de crédito, credenciales, documentos internos, entre otros, los cuales al fugarse impactan directamente en el negocio y la imagen de nuestros clientes. Es por esto que siempre buscamos apoyarlos para que puedan responder de forma proactiva a este tipo de incidentes, disminuyendo los impactos económicos para la empresa y los daños reputacionales asociados a la exfiltración de datos.

Detectar una filtración de datos puede ser extremadamente desafiante durante un ataque sofisticado para los equipos internos de una organización.



Experto:

Felipe Olea
Especialista en ciberseguridad

¿Cómo logran los atacantes exfiltrar datos de una organización?

He visto como la exfiltración de datos en las organizaciones se puede realizar de distintas maneras. Las técnicas más comunes que utilizan los cibercriminales para robar datos, una vez dentro de la organización, es transferir los archivos a su centro de comando y control utilizando técnicas como "DNS Tunneling", en donde el atacante abre un túnel desde el equipo comprometido al servidor del hacker permitiendo hacer un bypass a defensas tales como firewalls. También suelen instalar herramientas legítimas, como "Rclone", en los sistemas comprometidos para sincronizar o subir los archivos a Mega o cualquier otra plataforma en la nube, para así luego descargar los datos en sus servidores.
Lamentablemente hoy en día veo cómo los cibercriminales ni siquiera necesitan acceso a la empresa para exfiltrar la información. Usualmente se piensa que el atacante tiene que entrar a la red interna para robar o copiar los datos, pero para la mayoría de las organizaciones el riesgo está en cómo ellas mismas exponen la información.

Es común encontrarnos con servicios expuestos mal configurados o desactualizados, presentando alguna vulnerabilidad (incluso algunos que no deberían estar exponiéndose), como apis, proxies, balanceadores de carga, etc. Los atacantes suelen aprovecharse de esto e intentan manipular y utilizar estas aplicaciones para hacer que el servidor les entregue información que no debería. Esto lo veo a menudo y es debido a un mal manejo de errores, poca sanitización en el input del usuario, control de acceso débil o incluso, dejan información privilegiada en el código de la página web, encontrándose disponible a solo un par de clicks para cualquier persona.

Lo anterior, sumado a que casi nunca controlan la cantidad de peticiones que puede hacer un usuario en una determinada cantidad de tiempo, permite a una persona mal intencionada automatizar peticiones y sacar información dependiendo de las respuestas. Por ejemplo, en el caso de las apis, permitiría a un atacante fácilmente analizar la api, ver cómo se consume esta, ver cómo se consumen los datos de la api y así... para luego intentar inyecciones a la base de datos, en el Backend, o incluso, en el Frontend, obteniendo credenciales (por ejemplo) que le den acceso privilegiado a más información.
Hoy es importante contar con servicios que estén regularmente detectando dónde se presentan estos fallos de seguridad, sobre todo cuando antes los ojos de la ley son las empresas las responsables de cuidar los datos de sus clientes.

CÉLULAS ÁGILES

Especialistas de ciberseguridad

Uno de los retos a los que se enfrentan las organizaciones es la demanda de nuevos perfiles tecnológicos que posean experiencia comprobada y sean capaces de integrarse rápidamente a una organización.

El servicio de Células Ágiles, se caracteriza por la búsqueda, capacitación e integración de un especialista en ciberseguridad con el fin de formar o integrar células de trabajo para un proyecto en particular o diversas iniciativas del negocio, permitiéndole a nuestros clientes enfocarse en las funciones estratégicas del negocio

El objetivo de este servicio es que el cliente pueda contar con un especialista en ciberseguridad para resolver las necesidades de un proyecto en particular o transversal al negocio. Dejando en manos de especialistas con un alto componente técnico, la selección, capacitación e integración y evitando lidiar con el panorama competitivo de alta rotación de los especialistas de ciberseguridad. Accediendo así a los mejores talentos, reduciendo tiempos de selección y aumentando la eficiencia.

Nos caracteriza

- **Un enfoque centrado en nuestros clientes y una alta calidad en el servicio**
- **Grupo humano compuesto por profesionales de gran experiencia**
- **Proactividad para entender las necesidades de nuestros clientes**
- **Procesos consensuados, medibles y auditables**
- **Una prestación de servicios coordinada y supervisada técnicamente**

Perfiles

- **Célula ágil de Ethical Hacking**
- **Célula ágil de Arquitecto de seguridad**
- **Especialista de Cumplimiento de ciberseguridad**
- **Especialista DevSecOps**
- **Especialista Técnico Ciberseguridad OT**
- **Security Advisor**

Experto:

Bastian Peso
Especialista en ciberseguridad

A través de la asesoría con células ágiles hemos comprendido diversas problemáticas que tienen las organizaciones en temas de procesos y operaciones, logrando resolverlas con soluciones que integran visiones multidisciplinarias, enfocándose siempre en los objetivos que busca el cliente. En efecto, esta es una de las cualidades con las que contamos, dado que poseemos una alta capacidad de adaptación al dinamismo de los nuevos proyectos de ciberseguridad, entendiendo los procesos críticos del negocio.

Las células ágiles de ciberseguridad pueden abarcar diversas áreas, desde el desarrollo seguro, ethical hacking, concientización, cumplimiento y normativas, entre otros. En mi caso, como Pentester perteneciente a una célula, verifico que las funcionalidades provistas por el cliente cuenten con estándares de calidad que le permita brindar un servicio seguro y confiable de cara al cliente final. A nivel técnico, las revisiones de código, análisis automatizados y pruebas de penetración dinámicas son tareas del día a día, siempre comunicando los hallazgos para que sean resueltos a tiempo por los equipos encargados, sin afectar la continuidad operacional.

En otras áreas, como en la concientización, las células ágiles permiten abordar temas complejos que requieren visiones expertas de diversas áreas para lograr un resultado exitoso y por supuesto medible.

Esta modalidad de trabajo es indispensable hoy en día para abordar de manera inteligente los nuevos proyectos, y su importancia recae en la capacidad de adaptarse rápidamente a las dificultades que van apareciendo a lo largo de los ciclos de desarrollo, y luego resolverlas para que no se conviertan en problema en el caso que surjan nuevamente. Otro factor importante a considerar, es que la célula ágil tiene la capacidad de mutar, agregar o quitar recursos para que la célula incremente su velocidad y eficiencia a lo largo del tiempo, ofreciendo un mejor servicio.

¿Qué factores determinan que una célula ágil sea más eficiente que una estructura tradicional de trabajo?

Trabajar en modalidad de células facilita ciertos procesos que son más lentos en las estructuras tradicionales, es por esto que está siendo adoptada en la mayoría de las empresas modernas. Algunas de los pro que puedo identificar son:

- **Equipo altamente especializado que se integra de manera óptima a la organización.**
- **Diversos perfiles técnicos que facilitan la resolución de problemas.**
- **Mayor efectividad gracias a la comunicación directa y efectiva.**
- **Entrega de valor contínua.**
- **Apoyo constante y anticipación de problemas**

CUMPLIMIENTO NORMATIVO

1.- DevSecOps/ Ciberseguridad en el SDLC

El desarrollo seguro de software es un modelo de trabajo que se basa en la realización de chequeos de seguridad continuos del proyecto en construcción, incluso desde sus fases iniciales y antes de que se escriba una sola línea de código. Estas pruebas se centran en descubrir y corregir cualquier error en una etapa temprana, y comprenden tests de autenticación, autorización, confidencialidad, no repudio, integridad, estabilidad, disponibilidad o resiliencia.
Un proceso SDLC seguro garantiza que las actividades de seguridad, como las pruebas de penetración, la revisión de código y el análisis de arquitectura, sean parte integral del esfuerzo de desarrollo.

El servicio DevSecOps consiste en una consultoría y apoyo constante a las organizaciones para implementar la ciberseguridad en todo el proceso de vida del desarrollo de software, y tiene por objeto contar con un software más seguro, que exista conciencia de las consideraciones de seguridad por parte de los equipos involucrados, la detección temprana de fallos de seguridad y por consiguiente también la reducción de los costos y tiempos como resultado de la detección temprana, y la reducción de riesgos cibernéticos.

Nuestro servicio de DevSecOps está basado en 4 etapas fundamentales:

Evaluación inicial

Levantamiento de información actual y nivel de madurez. Permite conocer las brechas existentes entre lo que se tiene actualmente versus lo que se debería tener respecto a documentos, herramientas, roles, etc.

Planificación

Una vez conocida las brechas existentes, se preparará una planificación que permitirá visualizar los próximos pasos a seguir en cuanto a documentación e implementación de nuevas herramientas.

Implementación

Durante este proceso, se implementará el roadmap definido en la etapa de planificación. Se documentará o revisará documentación existente, se revisarán procedimientos, herramientas de apoyo y difusión de todo el material creado.

Integración

Integración del proceso DevSecOps a cada célula definida en el plan. Esto permitirá que las células puedan comenzar a trabajar implementando seguridad en el ciclo de vida de sus proyectos.

Experto:

Neftali Saavedra
Especialista en Ciberseguridad

¿Cuáles son los principales retos de seguridad DevOps?

En base a mi experiencia estos son algunos de los retos más relevantes a los que nos enfrentamos a la hora de implementar seguridad en los ciclos de desarrollos basados en metodologías ágiles. Los cuales podríamos dividir en dos grupos, por una parte lo relacionado a planificación y definiciones de línea base, y otros relacionados a la gestión y tratamiento de los riesgos.

En el primer grupo de planificación y definiciones de línea base, podemos encontrar los siguientes:

1. **Tiempos más acotados en los pasos a producción:** El negocio muchas veces exige que sus requerimientos sean atendidos de manera rápida por las células de desarrollo, muchas veces existe poca o nula interacción con el área de seguridad o ciberseguridad durante las fases tempranas de desarrollo o planificación de los proyectos. Lo que se traduce en que las revisiones de seguridad puedan demorar el producto final en su entrega producto de los tipos de revisiones o gran cantidad de vulnerabilidades no atendidas en tiempo y forma. Por este motivo es importante que en las células de desarrollo se cuente con un integrante de seguridad el cual sea capaz de entregar los lineamientos y consideraciones a la hora de planificar o llevar a cabo dicho proyecto con esto se estimaron los tiempos de revisiones de seguridad, remediación y/o acciones correctivas en el propio código o componentes de los mismos.

2. **Existencia de definiciones o lineamientos de seguridad:** Muchas veces a la hora de implementar la seguridad en el código, me he dado cuenta de que en algunas organizaciones existe poca o nula existencia de lineamientos sobre desarrollo seguro o consideraciones que deben tener los desarrolladores para crear aplicaciones. Además, en algunos casos tampoco están dados los requerimientos mínimos de seguridad o específicos para un tratamiento seguro de la información sensible.

Respecto a la gestión y tratamiento de los riesgos, tenemos:

3. **Infraestructura como código**: Dado que el principal objetivo de DevOps es generar despliegues continuos sobre la infraestructura que soportara los desarrollo, se hace mucho uso de infraestructura como código, por ejemplo contenedores o Docker que facilitan la automatización para el desarrollo, implementación y ejecución de microservicios. Sin embargo, a pesar de la agilidad, escalabilidad y portabilidad de esta tecnología, se plantean algunos problemas de seguridad importantes.

4. **Desconfiguraciones o errores en las implementaciones**: Es habitual que se generen implementaciones con desconfiguraciones en los distintos ambientes de desarrollo, QA, pre-productivos o productivos afectando tanto las pruebas de seguridad como generando vulnerabilidades que podrían ser aprovechadas por un atacante o insider dependiendo del caso. En este sentido todo componente que se utilice en el código o los pasos a producción, deben ser revisados en búsqueda de fallas no solo de programación sino que también de vulnerabilidades.

5. **Gestión de privilegios y manejo de los secretos:** Por otra parte, y aun cuando muchos desarrolladores ya lo ha adoptado como práctica, es importante reforzar el uso de mecanismos que permitan aplicar de manera correcta un sistema CRUD (Create, Read, Update, Delete), es decir que cada usuario posea un perfil específico para ciertas acciones que pueda ejecutar en la aplicación y no sea posible escalar privilegios por algún fallo en el sistema.

6. **Gestión de vulnerabilidades:** Finalmente, y de acuerdo a mi experiencia, entendemos que la principal razón de los equipos de DevOps de incorporar al área de seguridad, es que esta certifique sus aplicativos con la finalidad de pasar a producción lo antes posible. Por este motivo es importante que la detección de fallos de seguridad no esté sólo centrada en el aplicativo o desarrollo como tal, sino que se certifique el conjunto completo de piezas que forman parte del puzzle considerando componentes, dependencias, infraestructura, código y fallos técnicos.

2.- Consultoría CIS Controls

La evolución de las tecnologías de la información y comunicación nos ha permitido automatizar y optimizar muchas de las actividades que se llevan a cabo en nuestra organización. Estas tecnologías han ido ocupando un lugar cada vez más importante, hasta el punto de que hoy en día, sin ellas, muchos de nuestros procesos de negocio no serían posibles. En ese contexto, la ciberseguridad ha tomado mayor relevancia en las organizaciones, tanto que han diseñado y ejecutado programas para proteger su información, su activo más importante, y para actuar de la mejor manera frente a un ataque cibernético porque, como sucede con los riesgos financieros o de reputación, el riesgo cibernético genera impacto negativo en los objetivos de negocio.

El servicio de Consultoría CIS Controls consiste por una parte en realizar el levantamiento en base al cumplimiento de controles de seguridad criticos y determinar el de grado de madurez de Ciberseguridad de las organizaciones basado en framework CIS TOP Security Controls, y por otra, una vez que se cuenta con los resultados, se diseña un plan de trabajo a corto y mediano plazo, donde se priorizan las acciones que ayudaran a elevar el grado de cumplimiento, junto con la metodología y recomendaciones para una implementación efectiva de los controles.

Trabajar bajo este marco ayudará a las organizaciones a adoptar una metodología la cual les permitirá tener una visión completa en aspectos de seguridad de los activos tecnológicos. Los 18 CSC son un conjunto de acciones para la defensa del ciberespacio que brindan formas específicas y escalables que ayudan a prevenir los incidentes informáticos, considerando el perfil de riesgo de una organización y los recursos disponibles para su implementación.

Estos controles priorizan y enfocan un número menor de acciones con resultados muy beneficiosos que permiten el cumplimiento de diferentes framework como NIST, serie ISO 27000, NERC CIP entre otros.

Los controles CIS nos ayudan a responder preguntas como

- **¿Cuáles son las áreas más críticas para establecer un programa de gestión de riesgos?**
- **¿Qué medidas defensivas proporcionan el mayor valor?**
- **¿Cómo podemos hacer un seguimiento de la madurez de nuestro programa de gestión de riesgos?**
- **¿Cómo podemos compartir nuestra información sobre los ataques y atacantes e identificar las causas fundamentales?**
- **¿Qué herramientas se utilizan mejor para resolver qué problemas?**
- **¿Qué controles CIS se asignan a los marcos regulatorios y de cumplimiento de mi organización?**

Experto:

Rodrigo Jimenez
Especialista en Ciberseguridad

¿Cuales son los atributos positivos que entrega el framework CIS Controls?

Los controles CIS (Center for internet Security) son un marco metodológico para implementar controles de Ciberseguridad. Los CIS Controls pueden implementarse en instituciones públicas hasta empresas privadas. Su misión es identificar, desarrollar, verificar, difundir y mantener las mejores prácticas de ciberseguridad. CIS ofrece soluciones de ciberseguridad mundial para prevenir y responder rápidamente a incidentes de ciberseguridad y permita a las empresas a construir un ambiente ciberseguro.

IS Controls son clasificados en 3 grupos de implementación, el Grupo de implementación 1 (IG 1), enfoca un piso mínimo de Ciberseguridad para comenzar, luego se encuentra el grupo de implementación 2 (IG 2) dónde una empresa o institución se encuentra en una fase intermedia para la ciberseguridad y por último el grupo de implementación 3 (IG 3) el cual se sitúa a la empresa en una fase avanzada

Los atributos positivos de CIS Controles permiten lo siguiente:

- **Crear un programa de Ciberseguridad**
- **Practicar higiene Cibernética con recursos y experiencia**
- **Priorizar los esfuerzos de Ciberseguridad**
- **Aplicar foco en un conjunto reducido de controles y las medidas que permitan abordarlos (IG1, IG2 y IG3)**
- **Mapear los marcos mundialmente aceptados como la NIST, ISO 27000, PCI DSS, HIPAA, FISMA, NERC CIP, entre otras.**

En NIVEL4 hemos realizado distintas consultorías en Ciberseguridad utilizando basados en CIS Controls (V7, V8), lo cual ha permitido, implementar un programa de Ciberseguridad basado en los CIS Controls y por ende proteger y resguardar la información de todos los usuarios con un foco de mejora continua en el tiempo.

Nuestra experiencia, respecto a la evaluación de riesgo críticos en las empresas es Mantener un inventario de activos detallado, mantener un inventario del software autorizado, realizar respaldos de sistema completos, proteger respaldos y asegurar respaldos automatizados de forma regular

3.- Consultoría ISO 27001

La ciberseguridad es una disciplina cuyo objetivo es ayudar a gestionar el riesgo de las organizaciones a través de la adopción de un sistema de gestión de seguridad de la información que detecte, mitigue, monitoree y responda ante riesgos de seguridad de la información, buscando preservar no solo la disponibilidad y continuidad de un proceso productivo, sino que también la integridad y confidencialidad de todos los activos de información relevantes para los procesos de soporte y servicios productivos que son el núcleo y esencia del negocio.

Para ello, cada organización involucrada en el desarrollo y mantenimiento de un sistema de seguridad de la información debe redactar y aprobar una batería de herramientas normativas, como políticas y procedimientos que tengan por objeto, preservar la confidencialidad, integridad y disponibilidad de la información, gestionar el riesgo, implementar controles que busquen disminuir los riesgos y amenazas, mejorar el funcionamiento de los procesos, entre otros.

El servicio de Consultoría ISO 27001 tiene por objeto apoyar a las organizaciones en la creación, redacción, revisión y actualización de documentos como políticas, procedimientos o procesos según estándar internacional de seguridad de la información ISO 27001, con el objeto de ayudar a las organizaciones a mejorar la gestión de sus riesgos, con un enfoque sistémico para la gestión de la información que garantice la mejora continua de la seguridad de la información.

El objetivo es asesorar a las organizaciones a integrar la adopción de criterios que le permitan cumplir con los requisitos de la norma adaptándonos a sus necesidades particulares, entregando las directrices de adopción y cumplimiento, con el objetivo de contar con una línea base de ciberseguridad y seguridad de la información ya que sin un marco normativo sólido, las organizaciones se exponen a múltiples tipos de amenazas informáticas.

Experto:

Rodrigo Jimenez
Especialista en Ciberseguridad

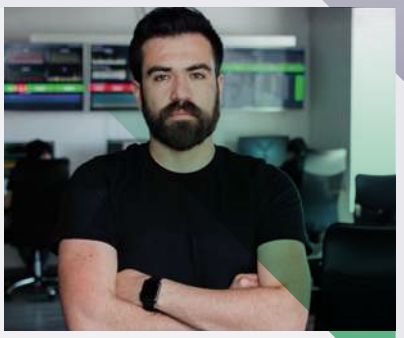
¿Cuáles son los principales errores de las organizaciones al implementar y seguir un Sistema de Gestión de Seguridad de la Información (SGSI)?

SGSI (Sistema de gestión de seguridad de la información) permite a una institución o empresa, evaluar los riesgos y definir las aplicaciones de control necesarias para poder eliminar o minimizar sus consecuencias negativas. SGSI ofrece un conjunto de políticas que permiten resguardar la integridad, la confidencialidad y disponibilidad de los activos de información, basadas en la norma ISO 27001 (114 controles).

Algunos principales errores en un SGSI:

- Comité de Seguridad de la información no agendada
- Comité de incidentes no agendada
- No registrar incidentes tecnológicos en bitácora
- Comité de riesgos no agendada
- No registrar riesgos (Legacy)
- No apoyar al CISO con presupuesto
- No apoyar al CISO con el CEO con incidentes de Ciberseguridad
- Saltar temas NDA (Non Disclosure Agreement) y nuevos proveedores
- No inventariar activos (Hardware y Software)
- Sólo preparar una auditoría para poder responder (EJ: Política lista)
- No contar con un sistema online para firma de documentos (Firma electrónica)
- No contar con un SIEM ni guardar logs para visualizar eventos posteriormente
- No realizar DRP a la infraestructura para poder recuperarse en tiempo
- No realizar pruebas de respaldo y restauración de datos
- No contemplar política (BYOD) para poder utilizar los equipos
- No realizar inducción para equipos de desarrollo seguro

CIBERSEGURIDAD EN CIFRAS



Hernán Möller Zavalla
COO y socio fundador de NIVEL4.

¿Cuál es la situación de Chile este 2022?

La premisa de que existen empresas que ya han sido afectadas por un incidente, sólo que no lo han detectado, se hace cada vez más evidente. Al momento de indagar por cifras de algunos de estos eventos se torna complicado en base a la fuente de información que se está consultando. Los avances en monitoreo y análisis de información a nivel global permiten que muchas veces los proveedores de inteligencia ofrezcan servicios a sus potenciales clientes incluso sobre eventos que ellos mismos desconocen. Este dato entrega valor a dicha fuente de información pero, a su vez, genera incertidumbre acerca de qué tan confiable o seguro es el recurso consumido. Hoy en día observamos que muchas de estas fuentes de datos manejan diversas cifras, algunas de ellas incluso abultan sus números en base a información duplicada o incompleta.

En relación a incidentes del tipo phishing, vale decir sobre aquellas organizaciones en que su activo web fue utilizado para el alojamiento de páginas falsas, que las cifras indican que en lo que va del año al menos 750 dominios .CL fueron utilizados para estos fines. Mientras que, por otra parte, sobre 130 sitios nacionales fueron detectados con malware según revela Abuse.ch.

Otra cifra preocupante corresponde a la fuga o leak de credenciales, lo que genera una alarmante sensación de inseguridad dentro de las organizaciones. Por una parte, los proveedores de inteligencia se esfuerzan por reportar datos vinculados al dominio de su cliente, no obstante, muchas veces estos datos son extemporáneos y no se produjeron necesariamente vulnerando la seguridad de la organización, sino más bien algún servicio tercerizado que fue explotado y provocó que ciertos colaboradores se viesen afectados. Fuentes no confirmadas señalan que al menos 130.000 credenciales (en base a orígenes de IP's nacionales) se encuentran circulando por botnets del tipo Stealer, mientras que por nuestra parte logramos verificar que al menos 2.824 casillas y sus correspondientes contraseñas pertenecen al espectro CL.

La disparidad en las cifras se da nuevamente por el grado de fiabilidad de la fuente y la mayoría de las veces se desconoce la forma en cómo se obtuvieron los datos. Sumado a lo anterior, existe el factor de oportunidad de la información dado que existen centenares de dataleaks circulando tanto por internet como por la darkweb, con datos antiguos u obsoletos. Pero esta información no deja de ser crucial para el atacante ya que amplía la superficie de ataque de la organización y permite conocer, de cierta forma, a su víctima.

Desde sus inicios, NIVEL4 ha sido una empresa innovadora, buscando siempre estar a la vanguardia. Por esto mismo, desde el día uno, hemos desarrollado herramientas de uso interno que permitan facilitar la operación y mejorar la calidad de servicio hacia nuestros clientes. Durante varios años, hemos estado desarrollando plataformas para el registro y gestión de vulnerabilidades, ejercicios de awareness, concientización y simulación de pruebas de phishing, entre otros. A lo largo de estos años, recopilamos mucha información valiosa que permite a las instituciones conocer el estado actual de la ciberseguridad en Chile, y de esta forma lograr una proyección hacia el futuro. Nuestras plataformas contienen información de más de 250 clientes de todos los rubros tales como banca, retail, retail financiero, gobierno, fintech, salud y minería entre otros.

Este informe busca ser un fiel reflejo del trabajo de todos estos años, permitiendo dar visibilidad sobre la situación actual de ciberseguridad en nuestro país, dando una visión hacia donde avanzaremos los próximos años y ayudando a las organizaciones en la tomar decisiones respecto a los presupuestos de ciberseguridad que las empresas deben considerar.

Vulnerabilidades

En la actualidad, todas las organizaciones utilizan computadores, smartphones y redes inalámbricas. Y esto las expone a una multitud de ciberamenazas por el uso de aplicaciones, páginas web, correo electrónico, redes sociales, etc. siendo las más comunes las vulnerabilidades, las cuales son explotadas principalmente para robar información personal o de la organización, la cual utilizan para cometer delitos como fraude, extorsión y exfiltración entre otros. Podemos definir una vulnerabilidad de forma genérica como un fallo en un sistema que puede ser explotada por un atacante generando un riesgo para la organización o para el mismo sistema, de ahí la importancia de su reconocimiento, análisis y mitigación.

Categoría 1 Vulnerabilidades

1.1 Porcentaje de vulnerabilidades encontradas, clasificadas por severidad según CVSS score 3.

La siguiente categoría nos indica el porcentaje de vulnerabilidades encontradas durante el año 2022 por el equipo de operaciones de NIVEL4, clasificadas por su severidad en base a CVSS score. Adicionalmente para fines de análisis se agruparon por industria.

Severidad	Porcentaje
Crítica	2,60%
Alta	12,23%
Media	47,60%
Baja	27,92%
Informativa	9,66%

1.2 Porcentaje de vulnerabilidades encontradas, clasificadas por severidad según CVSS score 3. clasificadas por industria

Cuando analizamos los datos desagregados ordenados por industria, nos encontramos que tratándose de las las vulnerabilidades según su severidad clasificadas como críticas su mayor presencia se encuentran en el sector gobierno y el menos porcentaje de ella en los sectores salud y financiero; a su vez, tratándose de las las vulnerabilidades según su severidad clasificadas como altas su mayor presencia se da en los sectores seguros y salud y el menos porcentaje de ella en los sectores manufactura y energía, finalmente tratándose de las las vulnerabilidades según su severidad clasificadas como media su mayor presencia se da en los sectores tecnología y manufactura y el menos porcentaje de ella en los sectores gobierno y energía.

Industria	Crítica	Alta	Media	Baja	Informativa
Energía	2,33%	9,88%	40,40%	35,76%	35,76%
Financiera	1,31%	11,39%	42,41%	31,41%	13,48%
Gobierno	6,18%	13,48%	37,65%	38,76%	3,93%
Manufactura	2,84%	6,82%	48,30%	33,52%	8,52%
Salud	0,64%	17,20%	45,22%	26,11%	10,83%
Seguros	2,15%	19,35%	44,09%	25,81%	8,60%
Tecnología	2,99%	10,45%	52,83%	25,07%	8,66%
Otros	2,33%	9,30%	69,76%	6,98%	11,63%
Suma total	**2,60%**	**12,23%**	**47,60%**	**27,92%**	**9,66%**

1.2 TOP 10 de tipos de vulnerabilidades por CWE

CWE permite identificar los problemas más comunes al momento de desarrollar aplicaciones o plataformas y permiten categorizar los hallazgos durante un análisis de vulnerabilidades o ethical hacking. A continuación, presentamos los errores más comunes encontrados por nuestro equipo de especialistas durante el año.

Rango	Identificación	Nombre
1	CWE-693	Falla del mecanismo de protección
2	CWE-200	Exposición de información confidencial a un actor no autorizado
3	CWE-497	Exposición de información confidencial del sistema a una esfera de control no autorizada
4	CWE-327	Uso de un algoritmo criptográfico roto o riesgoso
5	CWE-1104	Uso de componentes de terceros sin mantenimiento
6	CWE-799	Control inadecuado de la frecuencia de interacción
7	CWE-307	Restricción incorrecta de intentos de autenticación excesivos
8	CWE-284	Control de acceso inadecuado
9	CWE-471	Modificación de datos supuestamente inmutables
10	CWE- 204	Discrepancia de respuesta observable

Sector Energía

Rango	Identificación	Nombre
1	CWE-693	Falla del mecanismo de protección
2	CWE-200	Exposición de información confidencial a un actor no autorizado
3	CWE-497	Exposición de información confidencial del sistema a una esfera de control no autorizada
4	CWE-327	Uso de un algoritmo criptográfico roto o riesgoso
5	CWE-1104	Uso de componentes de terceros sin manteni-miento
6	CWE-799	Control inadecuado de la frecuencia de interacción
7	CWE-307	Restricción incorrecta de intentos de autenticación excesivos
8	CWE-284	Control de acceso inadecuado
9	CWE-285	Autorización incorrecta
10	CWE- 204	Discrepancia de respuesta observable

Sector Financiero

Rango	Identificación	Nombre
1	CWE-693	Falla del mecanismo de protección
2	CWE-497	Exposición de información confidencial del sistema a una esfera de control no autorizada
3	CWE-200	Exposición de información confidencial a un actor no autorizado
4	CWE-1104	Uso de componentes de terceros sin manteni-miento
5	CWE-327	Uso de un algoritmo criptográfico roto o riesgoso
6	CWE-471	Modificación de datos supuestamente inmutables
7	CWE-799	Control inadecuado de la frecuencia de interacción
8	CWE-285	Autorización incorrecta
9	CWE- 204	Discrepancia de respuesta observable
10	CWE-307	Restricción incorrecta de intentos de autenticación excesivos

Sector Salud

Rango	Identificación	Nombre
1	CWE-693	Falla del mecanismo de protección
2	CWE-497	Exposición de información confidencial del sistema a una esfera de control no autorizada
3	CWE-1104	Uso de componentes de terceros sin mantenimiento
4	CWE-327	Uso de un algoritmo criptográfico roto o riesgoso
5	CWE-201	Inserción de información confidencial en los datos enviados
6	CWE-395	Uso de NullPointerException Catch para detectar la falta de referencia de puntero NULL
7	CWE-209	Generación de mensaje de error que contiene información confidencial
8	CWE-287	Autorización incorrecta
9	CWE-521	Requisitos de contraseña débil
10	CWE-89	Neutralización incorrecta de elementos especiales utilizados en un comando SQL

Sector Gobierno

Rango	Identificación	Nombre
1	CWE-693	Falla del mecanismo de protección
2	CWE-200	Exposición de información confidencial a un actor no autorizado
3	CWE-497	Exposición de información confidencial del sistema a una esfera de control no autorizada
4	CWE-1104	Uso de componentes de terceros sin mantenimiento
5	CWE-327	Uso de un algoritmo criptográfico roto o riesgoso
6	CWE-799	Control inadecuado de la frecuencia de interacción
7	CWE-1104	Uso de componentes de terceros sin mantenimiento
8	CWE- 204	Discrepancia de respuesta observable
9	CWE-307	Restricción incorrecta de intentos de autenticación excesivos
10	CWE-319	Transmisión de textos sin cifrar de información confidencial

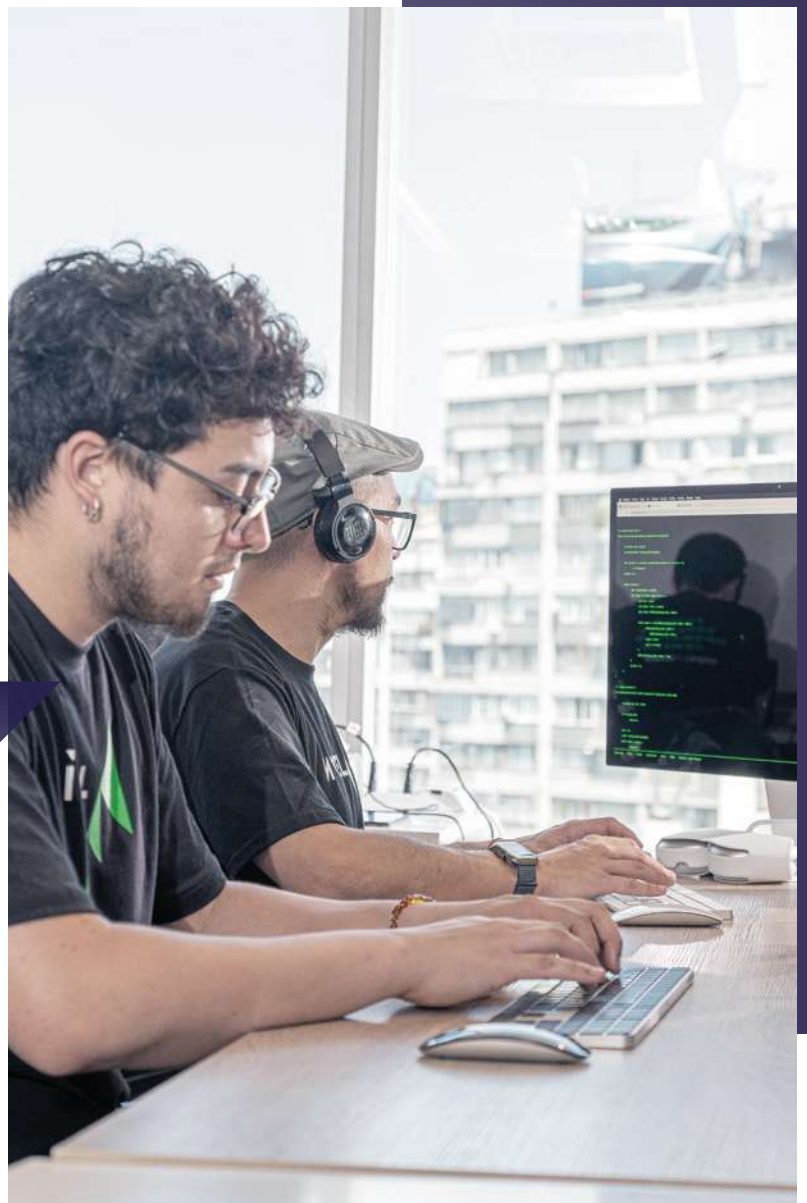
Sector tecnología

Rango	Identificación	Nombre
1	CWE-200	Exposición de información confidencial a un actor no autorizado
2	CWE-693	Falla del mecanismo de protección
3	CWE-497	Exposición de información confidencial del sistema a una esfera de control no autorizada
4	CWE-1104	Uso de componentes de terceros sin mantenimiento
5	CWE-327	Uso de un algoritmo criptográfico roto o riesgoso
6	CWE-799	Control inadecuado de la frecuencia de interacción
7	CWE-307	Restricción incorrecta de intentos de autenticación excesivos
8	CWE-284	Control de acceso inadecuado
9	CWE-434	Carga sin restricciones de archivo con tipo peligroso
10	CWE-285	Autorización incorrecta

1.3 Tiempo promedio de resolución o mitigación de las vulnerabilidades clasificadas por severidad según CVSS score 3.

En promedio, las organizaciones, atendiendo la severidad de las vulnerabilidades se demoran en la mitigación de estas:

Baja	8,9 días
Media	15,4 días
Alta	23,6 días
Crítica	24,2 días



Phishing

La importancia de la concientización en ciberseguridad se define en la habilidad que tienen las personas para reconocer que están frente a una amenaza. A pesar de que las organizaciones son las responsables finales de gestionar el riesgo cibernético y mitigar un incidente, son las personas las que están directamente expuesta a los ciberataques, eso porque el phishing sigue siendo la principal amenaza a la ciberseguridad.

Categoría 2 Campañas de Phishing Test

2.1 Cantidad promedio de campañas de Phishing que las organizaciones ejecutan durante el año, incluyendo cantidad de usuarios que participan en estas campañas.

Porcentaje de campañas de Phishing Test realizadas el 2022 por las organizaciones en Chile

1,5

Usuarios promedio que participan por campaña

3970

Porcentaje de campañas realizadas por industria

Financiera | Tecnología | Gobierno

Cantidad promedio de usuarios que participan por industria

Financiera | Tecnología | Gobierno

2.2 Cantidad promedio de usuarios que visitan, hacen clic, ingresan datos o descargan un archivo malicioso, en una campaña de Phishing.

Cantidad de usuario visitan	Cantidad de usuario hace clic	Cantidad de usuario que ingresa datos o descarga archivo
1895	309	149

Resultados por industria

Industria	Cantidad de usuario que no abren o ignoran los correos	Cantidad de usuario visitan	Cantidad de usuario hace clic	Cantidad de usuario que ingresa datos o descarga archivo
Financiera	79,05%	11,8%	5,4%	3,75%
Tecnología	38,5%	49,9%	7,8%	3,8%
Gobierno	60%	26%	11,2%	2,8%

Awareness y Concientización

La educación de los usuarios en materia de ciberseguridad y fraudes digitales, ayuda a evitar la mayor parte de los incidentes que ocurren comúnmente en las organizaciones. El 90% de las brechas de seguridad comienzan por un error humano. Si las personas que utilizan la información lo hacen aplicando medidas simples pero eficientes, o si tienen los suficientes conocimientos como para advertir sobre situaciones sospechosas, los equipos de seguridad TI pueden actuar a tiempo para contener y mitigar incidentes.

Crear concientización entre los grupos de usuarios es esencial en las empresas y organizaciones, porque son las personas quienes usan la información para poner en marcha el negocio.

Categoría 3 Adopción de estrategias de awareness y concientización

Cuando partimos de la base que un clic desprevenido realizado por un colaborador puede exponer a una organización a incidentes graves de ciberseguridad, entendemos la necesidad de trabajar una estrategia de concientización, que permita por un lado capacitar y educar, pero por otro exponer la importancia del rol de los colaboradores dentro de una organización, ya que como se señala reiteradamente, la ciberseguridad es tarea de todos.

Entonces, nace la pregunta, si es tan importante la adopción de estrategías de awareness y concientización en materia de ciberseguridad **¿Están desarrollando las organizaciones planes de concientización?**

- **El 57,7% de las organizaciones desarrollan una estrategia permanente de concientización**
- **El 19, 3% de las organizaciones realizan acciones esporádicas y sin persistencia en el tiempo, lo que dificulta poder medir el impacto de modo que cumplan su rol en la gestión del cambio del capital humano y la vinculación de los contenidos.**
- **Lamentablemente el 23,1%, si bien entiende la importancia de este tema aún no cuenta con los recursos internos o externos que le permita desarrollar una cultura organizacional enfocada en la ciberseguridad**

De las organizaciones que desarrollan una estrategia permanente de concientización hemos observado que:

- **El 66,6% externaliza y deja en manos de especialistas la estrategia y desarrollo de un programa de concientización, el cual les permite tener métricas, mejorar la experiencia del aprendizaje, darle continuidad y evolución a los contenidos y servir**

Presupuesto en ciberseguridad

Categoría 4 Presupuesto de las organizaciones

En el transcurso de estos años, considerados desde el nacimiento de NIVEL4, hemos asesorado a más de 500 organizaciones de todas los rubros tanto en Chile como en la región, consolidando en una primera etapa servicios de ataque como el Ethical Hacking, Red Team y Pruebas de Phishing. Pero las necesidades de las organizaciones y la experiencia que nos dejaban las asesorías nos hicieron ver que el enfoque debía incluir una protección 360°, lo que nos llevó a crear nuevas líneas de negocios y de esta forma poder prestar una asesoría integral, Así es como centramos nuestros servicios en 4 pilares: ataque, defensa, cumplimiento normativo y educación.

Es por ello que, hemos sido protagonistas en el crecimiento constante de las empresas para mantener protegido sus sistemas, con todo lo que esto conlleva, como por ejemplo el aumento de presupuesto para las áreas de ciberseguridad. Este aumento de presupuesto se traduce en varias cosas, como por ejemplo en la creación o crecimiento del equipo interno de la empresa, desarrollo de estrategias de concientización, así como la contratación de nuevos servicios especializados.

4.1 ¿Cuánto están invirtiendo las organizaciones chilenas en ciberseguridad?

Con mucho entusiasmo, hemos visto cómo la inversión de las organizaciones ha ido en aumento año tras año en materia de ciberseguridad, ello motivado en parte por la conciencia de la importancia de ella, los ataques de conocimiento públicos de organizaciones e instituciones de gobierno que creíamos robustas en la materia, y el cumplimiento normativo que nos impone nuevas obligaciones a fin de garantizar la seguridad de la información.

Si retrocedemos al año 2020 y lo comparamos con el último Q del 2022, podemos ver un crecimiento de más del 100% en el ítem presupuestario “ciberseguridad” de las organizaciones.

Datos interesantes

- **Las organizaciones pasaron de realizar 1 Ethical Hacking al año, a ejecutarlos 4 veces al año.**
- **Las organizaciones pasaron de realizar Ethical Hacking solo a sus plataformas críticas, a ejecutarlos progresivamente sobre todos sus activos.**
- **Las organizaciones cambiaron su preocupación de protección centrada solamente en lo que se encontraba expuesto a internet, a integrar la preocupación permanente de protección de su red interna, debido a que el concepto "perímetro" ya no es el de antes.**
- **Las organizaciones pasaron de adoptar medidas de seguridad y protección solo con fines de cumplimiento, a adoptarlas por una necesidad a fin de asegurar la continuidad operacional, gestionar el riesgo, proteger los derechos de los usuarios de los sistemas y prevenir la afectación reputacional.**
- **Las organizaciones pasaron de desconocer que habían sido vulneradas por ciberatacantes a adoptar un fuerte enfoque preventivo centrado en revisiones periódicas, realizando ejercicios de simulaciones de ataques, la concientización y entrenamiento constante de equipos técnicos y colaboradores.**
- **Las organizaciones pasaron de realizar 1 simulación de Phishing al año, a realizar 3 y acompañarlas de estrategias de concientización y educación con el fin de generar un cambio cultural.**

Finalmente, estando en el año 2022, las organizaciones entienden que deben protegerse y las entidades regulatorias tienen hoy el desafío de normar, fiscalizar y sancionar, así como proponer las integraciones del ecosistema de ciberseguridad que permitan en la mayor medida de lo posible resguardar los derechos de las personas en el ciberespacio, entendiendo que la ciberseguridad es un desafío permanente de las organizaciones en beneficio de las personas y la estabilidad nacional.

"PARA DONDE VAMOS"

Hacerse cargo de la dirección estratégica de una empresa, siempre representa un gran desafío, marcado principalmente por la resistencia al cambio organizacional, poder contar con el tiempo necesario para generar sinergias entre los equipos y alinear las expectativas de la dirección, pero esta tarea se vuelve más difícil cuando se trata de una empresa como NIVEL4, que en el transcurso del tiempo han aprendido cómo hacer bien las cosas, tienen claridad de quiénes son, han sabido proyectar técnicamente su expertis y habilidades y se han consolidado en un mercado nacional bastante incipiente, reconociendo las necesidades de las organizaciones y alineando su línea comercial a ellas.

NIVEL4, lleva 8 trabajando para adaptarse a las necesidades de las organizaciones, con la marcada visión de convertirse en un socio estratégico de sus clientes, ayudándolos a proteger y resguardar los activos de información así como plataformas digitales frente a los diversos tipos de amenazas. Esta premisa, se construye desde la asesoría especializada cercana, que muchas veces no es lo que el cliente quería en principio pero si lo que necesitaba en la práctica, desarrollada por un equipo técnico consolidado que también ha crecido y se ha especializado con el crecimiento sostenido de NIVEL4.

Katherina Canales
CSO de NIVEL4.

Hoy las cifras nos acompañan, tenemos las capacidades para expandirnos y rediseñar la oferta de servicios para que se adapte día a día a las necesidades de las organizaciones, que involucren a los directores y alta gerencia y les garanticen el cumplimiento de estándares nacionales, internacionales, mejores prácticas reconocidas y la regulación que a pasos agigantados se vuelve más cercana, ya que proyectos de ley como Datos personales y ley Marco de Ciberseguridad, impondrán a las organizaciones nuevos y mejorados estándares de protección, la adopción de mecanismos técnicos de seguridad en resguardo de las personas, las organizaciones y su patrimonio.

Cómo lo haremos:

- Aprovechando las capacidades de expansión que tenemos, el prestigio que los profesionales chilenos han construido en la región y los servicios prestados en los últimos años a países como Argentina, Perú, Colombia, Paraguay y Ecuador, buscaremos consolidar operaciones internacionales, abrir nuevos mercados y posicionarnos siempre en base a los atributos que nos caracterizan como: cercanía, velocidad en la entrega de servicios, adaptabilidad a las necesidades y que nos diferencian de la competencia.

- Queremos crecer en número de clientes, penetrar mercados donde la ciberseguridad aún no es tema, rediseñar algunas líneas de servicios especializados que se adapten con mayor facilidad a las obligaciones normativas, dirigidos a los sectores regulados, y a la necesidad de las organizaciones para mitigar los riesgos tecnológicos, reconociendo la importancia de la protección de entornos industriales, infraestructuras críticas y tecnologías emergentes. Lo que consecuencialmente nos llevará a crecer en infraestructura, capacidades, formación y entrenamiento de talentos y capital humano. Dicho de otra forma, apuntamos a un crecimiento orgánico, responsable y sostenido de la compañía.
  Este 2023 también trabajaremos para fortalecer e incrementar las alianzas estratégicas con partner, organizaciones y grupos de interés que nos permitan, un mayor crecimiento, poder llegar a mercados cautivos, vincularnos con diferentes ecosistemas, crecer en experiencias y poder aportar a la comunidad de la ciberseguridad.

- De igual manera,como parte de una estrategia de visibilidad, seguiremos vinculando contenido, publicando columnas, compartiendo noticias e investigaciones desarrolladas por nuestros expertos y marcando presencia en los principales y más importantes eventos de ciberseguridad del mundo.

- El desafío es grande, pero si queremos grandes resultados, tenemos que apuntar alto, pero sobre todo asegurar las condiciones y realizar las acciones que permitan que las cosas pasen.

"AMENAZAS Y TENDENCIAS 2023 "

Evolución de los ciberataques ¿Cuál será el escenario este 2023?

Distante se ven ataques como Wannacry, la filtración de datos RockYou2021, e inclusive el secuestro de datos de Pipeline (ocurrido el 2021). Y es que las ciberamenazas avanzan de manera vertiginosa. Globalmente ocurren más de 30 mil ciberataques diarios, mientras que el 64% de todas las compañías a nivel mundial declaran haber sufrido uno. Esto nos habla de una evolución acelerada sin señales de decaer.

Uno de los puntos que contribuyó a que esto ocurriera, es que dichas acciones maliciosas ya no pertenecen únicamente a ciberdelincuentes profesionales. Por el contrario, hoy vemos muchos ataques ejecutados por amateurs, los cuales logran ser -en algunos casos- efectivos por malos hábitos de usuarios desprevenidos.

Sumado a lo anterior, múltiples técnicas se han adicionado a los ataques a modo de ampliar su efectividad, incluyendo la ingeniería social, la extorsión, el secuestro, filtración de datos, y ataques de denegación de servicio distribuida, generando daños reputacionales e inclusive deteniendo las operaciones tanto internamente como de cara al cliente.

Es por esto que afirmamos que los ataques no se detendrán y que, por el contrario, seguirán avanzando y tornándose más complejos. En base a nuestros análisis, recopilación de datos y antecedentes globales, determinamos seis tendencias en ciberataques para el 2023.

1 Inteligencia artificial, Machine Learning y Deep Fake

El avance en la tecnología dio pie a nuevas herramientas para diseñar y ejecutar ataques, volviéndose cada vez más sofisticados. En primer lugar, la IA tuvo un doble efecto: por un lado positivo, porque nacieron nuevas plataformas de inteligencia y detección en base a algoritmos de aprendizaje automático y comportamientos; y por otro lado lo negativo, ya que los ciberdelincuentes adoptaron estas tecnologías rápidamente para ejecutar ataques de distintos tipos, como el reconocimiento de sistemas de seguridad débiles, correos de phishing personalizados por usuario, e incluso ayudó a desarrollar suplantaciones de identidad avanzada -conocida como Deep Fake-, donde se ha podido clonar la voz -y en muchos casos- la cara, lo que ha llevado a realizar fraudes involucrando la suplantación de altos ejecutivos o políticos.

El uso de estas herramientas será mucho más amplio en los próximos meses y en distintas regiones del mundo.

2 Ransomware dirigido y nuevos modelos de extorsión

El primer ransomware hizo su debut hace más de 30 años en un disquete, y no ha cambiado mucho desde entonces, solo que actualmente el contexto es distinto y se han sumado nuevas herramientas.

De un momento a otro, los ataques de este tipo se dispararon, pasando de los modelos básicos de secuestro y encriptación de datos, a nuevas estrategias de extorsión y sitios de filtración creados por los mismos atacantes. El 2023 esta tendencia seguirá al alza, dado que es muy efectiva por la presión que ejerce sobre la víctima, y porque los ciberdelincuentes obtienen altas sumas de dinero gracias a esto. En cifras, el costo total de los ataques de ransomware el 2021 ascendió a 3.4 billones de dólares.

Sumado a esto, una tendencia fuerte que observaremos es la triple extorsión, donde no solo prima la obtención de dinero, sino que también dañar la reputación al máximo y obtener múltiples beneficios. Si en el modelo de doble extorsión veíamos la filtración de datos como un método de presión, en la triple extorsión añadimos ataques DDoS para que la víctima colapse y no tenga escapatoria. Esto tiene un trasfondo, ya que no solo busca dañar al objetivo principal, sino alcanzar a los socios estratégicos, partners, colaboradores y clientes.

En esta tendencia veremos también ataques dirigidos a compañías y organizaciones por industria, con un estudio previo y mezcla de técnicas de ingeniería social. No es algo del todo nuevo, pero que sí ha mutado hacia estrategias más complejas.

3 Crecimiento del mercado de ciberamenazas as-a-service

Las ciberamenazas ''a servicio'' (o as-a-service como se les conoce en inglés) han sufrido un crecimiento exponencial en los últimos tres años. Y es que generó un mercado -y una demanda- de malware, kits de phishing y ransomware. Cuando hablamos de que hoy personas amateurs pueden ejecutar una campaña maliciosa, nos referimos a esto, a la posibilidad de comprar cualquier activo malicioso en la Dark Web y foros clandestinos.

Hoy existen diversos kits de phishing avanzados con diseños muy convincentes que suplantan a las principales marcas del mundo, inclusive Google y Microsoft con sus login de acceso. Lo que convierte a este negocio en algo muy llamativo tanto para personas que se quieren iniciar en los delitos digitales, como para los grupos avanzados.

Este modelo de negocio ha sido tan rentable para los grandes grupos de ciberdelincuentes, que hoy vemos cómo reclutan nuevas personas ofreciendo grandes sumas de dinero. Por ende, es algo que seguirá en crecimiento y lo veremos cada vez más en los próximos meses.

4 Ataques a dispositivos IoT en industrias

Los dispositivos IoT aumentan cada vez más en popularidad, sumándose al trabajo en distintas industrias, como la minería, salud, agricultura, automotriz, entre otras. El problema recae en que los estándares de seguridad de estos dispositivos debe aumentar acorde avanzan las ciberamenazas. Si bien hay bastante documentación sobre vulnerabilidades IoT, aún falta desarrollo de software eficaz frente a estas problemáticas. Todos los informes actuales indican que este tipo de dispositivos son un blanco fácil ya que permiten ingresar a redes con poca seguridad.

Otro punto clave, es el desarrollo de malware para IoT masivo, el cual puede alterar el funcionamiento de los dispositivos o filtrar información.

Una de las puertas de entrada a muchos sistemas serán este tipo de dispositivos.

5 Dispositivos Mobile, un nuevo objetivo

Los entornos móviles son cada vez más utilizados por los usuarios. En un solo dispositivo es posible almacenar datos sensibles como cuentas bancarias, contraseñas, ubicación, fotografías, correos, entre otros, ampliando la superficie de ataque.

No pasó mucho tiempo hasta que explotó el número de malware dirigido a entornos móviles, tanto para Android como iOS. Hoy vemos muchas aplicaciones fraudulentas que logran colarse en Play Store y alcanzar el millón de descargas, como troyanos bancarios, herramientas maliciosas de recolección de datos, entre otros.

Si en los años previos el aumento de estas amenazas fue de un 50%, se espera que este 2023 los ciberataques a entornos mobile sigan en alza, enfocándose específicamente en la recolección de datos sensibles e información bancaria.

6 Usuarios y colaboradores, siempre serán el blanco principal

Si bien todas estas ciberamenazas están en alza y representan una alerta de primera categoría, los usuarios y colaboradores siempre serán el objetivo principal de los ciberdelincuentes. Saben el gap que existe en el conocimiento sobre ciberseguridad, y que en algunas industrias el nivel de madurez en estas temáticas es bajo, por lo que casi siempre van a ser la primera puerta de entrada para ataques avanzados. La tecnología en muchos casos no falla, pero nosotros, las personas, sí. Es fundamental educar y sensibilizar sobre estas nuevas tendencias en ciberseguridad y mantenernos atentos sobre los rápidos avances tecnológicos.

Muchas organizaciones están sufriendo el proceso de cambio de la transformación digital, lo que supone un cambio en la cultura organizacional y añade nuevas responsabilidades a cada colaborador. Generar un entorno enfocado en las buenas prácticas, con desarrollo de políticas y normativas, pruebas de seguridad avanzada, donde los usuarios se sientan parte del ecosistema y la importancia que tienen dentro de este, es clave.

En NIVEL4 queremos ayudarte a proteger los activos más importantes de tu compañía: la información, las operaciones y el capital humano. La ciberseguridad es hoy. Integra una estrategia de ciberseguridad completa y disminuye el nivel de susceptibilidad frente a un ciberataque.


CCNA Security
Official Exam Certification Guide
NIVEL

NÍVEL

“La ciberseguridad es hoy. Asegura tu compañía, protege a las personas”.

Página web: www.nivel4.com
Blog N4 Labs: www.blog.nivel4.com
Correo de contacto: contacto@nivel4.com

Annual Report 2022

Avenida Providencia 1208,
oficina 1204
Santiago, Chile
https://nivel4.com

NIVEL4® CyberSecurity