Vol. Nº 6
Enero/2021
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

TRANSFORMACIÓN DIGITAL

Desafíos de ciberseguridad

Ciberguía:
¿Cómo protegerse de los fraudes de verano?

Cooperación Internacional
Estonia

Tendencias
Técnicas y amenazas en auge para 2021

Comunidad Hackers
Fundación País Digital: Pymes más acompañadas en su transformación digital

Legal
La digitalización de la Administración Pública

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Carolina Covarrubias
Cristobal Hammersley
Ramón Rivera

Diseño y diagramación: Jaime Millán

EDITORIAL

Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Transformación digital. Un concepto cada vez más comentado, y con razón. Porque llevar los procesos de las organizaciones al plano cibernético resulta indispensable hoy por hoy, en Chile como en cualquier otro lugar del mundo, y más aún debido a la pandemia. Pero esto hay que hacerlo con ciberseguridad, porque si no, las oportunidades que nos entrega la transformación digital pueden facilitar asimismo que los ciberdelincuentes entren a nuestros sistemas y realicen estafas.

Por eso es que decidimos dedicar el presente número de CiberSucesos a este fenómeno. Como tema central de esta edición, entonces, tenemos un análisis de la importancia de llevar a cabo una transformación digital que tenga como requisito y norte la ciberseguridad. Para esto, es primordial desarrollar y mantener una arquitectura de red segura, que tenga en mente la proliferación del denominado internet de las cosas, los mecanismos para que exista una autentificación eficaz de los usuarios, y lograr una alta disponibilidad e interoperabilidad de los sistemas, entre otros factores.

La sección de Cooperación Internacional presenta este número a Estonia, país líder mundial en la digitalización de su relación entre el Estado y los ciudadanos. La experiencia de esta nación báltica, que recién este año cumple 30 años desde su independencia de la Unión Soviética, implementando una revolucionaria infraestructura de identidad digital, es descrita en detalle por dos expertas de la Autoridad de Sistemas de Información de Estonia.

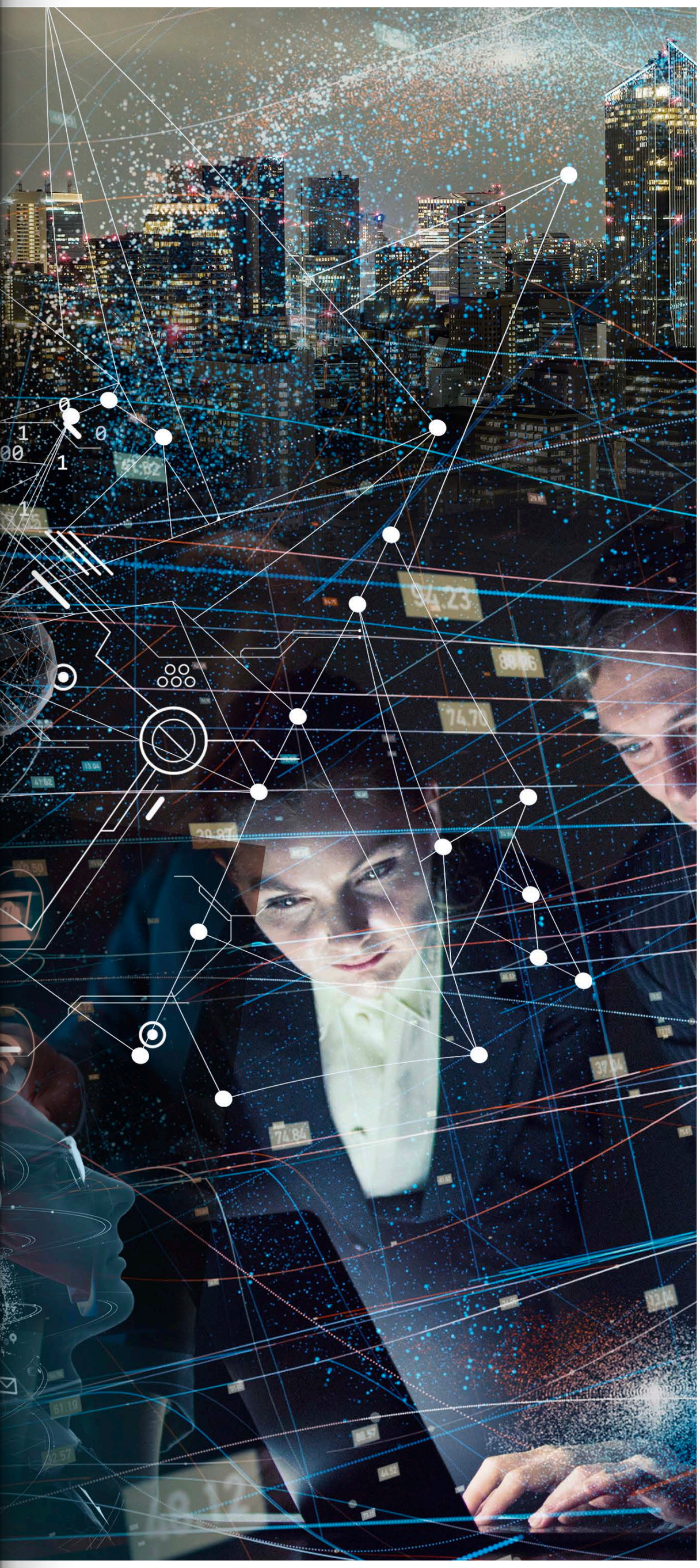
En Tendencias, presentamos (como no podía ser de otra forma para la primera edición del año), las principales técnicas que deberían "ponerse de moda" entre los ciberdelincuentes durante 2021, junto asimismo con nuevas tecnologías que podrían ayudar a mejorar nuestras defensas.

La sección Comunidad Hacker cuenta en esta ocasión con la Fundación País Digital, que nos aconseja y explica las formas en que apoyan a las pymes para generar un proceso de transformación digital exitoso, incluyendo seminarios y talleres para la entrega a las pequeñas empresas de los conocimientos necesarios para esta transformación, además de una herramienta de chequeo para que puedan diagnosticar su nivel de madurez digital.

Cierra el primer CiberSucesos, en el capítulo Legal, una mirada profunda a la actual legislación chilena promulgada con miras a fomentar la digitalización de la Administración Pública. Esto permitirá terminar con la necesidad de los chilenos de realizar miles de trámites de forma presencial, y de tener que presentar una misma información varias veces a distintos organismos del Estado.

DESAFÍOS DE CIBERSEGURIDAD EN LA TRANSFORMACIÓN DIGITAL

La transformación digital nos está aportando soluciones muy potentes, pero todo eso se puede volver en nuestra contra si no adaptamos los diferentes procesos a los actuales requerimientos de ciberseguridad, por ellos la implementación de la transformación digital debe estar cimentada en las bases de la ciberseguridad.



Lograr que las empresas traspasen al terreno virtual una mayor proporción de sus operaciones y negocio, es lo que se denomina transformación digital. Esto le permite a las organizaciones competir mejor y de forma más eficiente en el contexto actual, pero también hay que considerar que este cambio aumenta la exposición del negocio frente a las amenazas digitales. Por esto, al momento de comenzar el proceso de digitalización se debe tener como prioridad la ciberseguridad, con el fin de evitar dejar vulnerables infraestructuras esenciales.

Para llevar a cabo esta modernización se deben considerar al menos cuatro aspectos en materia de ciberseguridad. Es por ello que te entregamos recomendaciones para lograr de manera más exitosa esta transformación digital:

1.– DESARROLLAR Y MANTENER UNA ARQUITECTURA SEGURA

En materia de transformación digital es crítico contar con una arquitectura de red segura que considere el auge del Internet de las Cosas (IoT), los servicios en la nube y hoy también el trabajo remoto, donde se establecen un sinnúmero de conexiones, las cuales muchas veces pueden ser la vía de acceso de los ciberdelincuentes, especialmente cuando se trata de diseños de red construidos sin mayor orden o planificación a lo largo de varios años.

Para mantener una arquitectura segura, es importante tener criterios de ciberseguridad, manejando los altos estándares internacionales y mejores prácticas de aplicación general de la industria y , reduciendo los riegos de pérdidas a lo más mínimo, por ejemplo mantener los datos encriptados en los sistemas, permitir el seguimiento del tráfico para mantener la integridad de los datos, sistemas de monitoreo constante y mantener capas de seguridad de hardware como los Firewall, para así cubrir diferentes ambientes de seguridad en la arquitectura.

2.– POLÍTICAS DE DESARROLLO SEGURO

Al mismo tiempo, cuando se decida realizar la digitalización de algún proceso o servicio, es importante hacerlo bajo un modelo de desarrollo de software seguro, para detectar la mayor cantidad de vulnerabilidades posibles antes de que los productos sean puestos en funcionamiento de forma definitiva.

El desarrollo seguro comienza desde la planificación de un proyecto, considerando la seguridad de la información como un punto crítico dentro de la etapa de especificación de requerimientos. Es importante utilizar los múltiples mecanismos y procedimientos de seguridad que las tecnologías nos ofrecen para desarrollar códigos.
Una postura de seguridad consiste en desarrollar de la manera menos permisiva posible, y solo permitir acciones que sean estrictamente necesarias y solicitadas durante la etapa de requerimientos.

ALGUNAS **RECOMENDACIONES SON:**

1.– Durante el diseño e implementación se deben considerar las librerías y frameworks de terceros confiables que incorporan mecanismos de seguridad fundamentales para evitar errores de implementación.

2.– Durante la etapa de prueba, se deben verificar que no existan filtraciones de memoria que terminen por botar nuestro sistema ni filtraciones de datos que expongan información confidencial del mismo

3.– Las consultas hacia la base de datos deben estar parametrizadas y securitizadas para evitar inyecciones SQL.

4.– Codificar y escapar los datos ingresados para prevenir inyecciones de código que afecten nuestra aplicación, servidor o base de datos.

5.– Durante la implementación y pruebas se debe validar que los datos recibidos por un usuario sean acordes al formato esperado por la aplicación, para evitar inyecciones de archivos maliciosos que puedan ser ejecutados accidentalmente por nuestro sistema.

6.– Se deben implementar mecanismos de autenticación robustos, como el doble factor de autenticación, además las credenciales deben estar encriptadas durante el tráfico hacia la aplicación y deben ser almacenadas encriptadas también en caso de una filtración de datos de la base.

7.– Implementar mecanismos para el manejo seguro de sesiones de usuario (tokens, cookies, tráfico de datos) que puedan protegerlo de un man in the middle, o de secuestro de sesión.

8.– Se deben realizar pruebas de rendimiento y seguridad mediante el equipo QA para verificar que el proyecto cumple las expectativas de los requerimientos sin errores que pongan en peligro la integridad, disponibilidad y confidencialidad. Esto incluye realizar análisis de vulnerabilidades y código en búsqueda de filtraciones de información, controles de sesión defectuosos, entre otros.

9.– El monitoreo de rendimiento y análisis de logs resulta esencial para entender cómo funciona nuestro sistema una vez enviado a producción.

10.– Además, se debe contar con un equipo de mantención de código que resuelva las vulnerabilidades y despliegue actualizaciones de forma constante mientras sea necesario.

3.– AUTENTICIDAD DE LOS USUARIOS

Para mantener un sistema seguro hay que velar porque ingresen solamente los usuarios que correspondan. Por esto, ganan popularidad conceptos como la identificación estricta de usuarios y sus aparatos, incorporando la idea de zero trust y políticas de protección de datos y de detección de amenazas.

Para la autenticación de los usuarios existen diversos mecanismos. Lo básico es implementar un doble factor de autenticación, es decir, combinar algo que el usuario sepa (sus credenciales: usuario y contraseña) con algo que posea, como un token, una tarjeta o un celular que le permita recibir mensajes para autorizar su identificación. También hay sistemas que verifican otras características para asegurarse de que el usuario es quien dice ser, como permitirle conectarse solo desde determinadas IP o a ciertas horas del día.

En caso de no poder aplicar de forma íntegra las últimas tendencias en seguridad, aconsejamos, al emprender el camino de la transformación digital, considerar como requisito incorporar al menos algunos de sus principios y acciones. Por ejemplo, es necesario levantar un inventario de toda la información que maneja la empresa, definiendo su importancia, para identificar los datos que son cruciales proteger, las denominadas "joyas de la Corona", y así resguardarlos adecuadamente.

Por su parte, para resguardar la información sensible es necesario controlar los privilegios de acceso a ella. Esto se puede realizar definiendo perfiles en base a los roles que cumplen los distintos miembros de la organización (el denominado control de acceso basado en roles, o RBAC). En este sentido, se debe contemplar también el resguardo de lo que corresponda a infraestructura crítica, como redes de suministro eléctrico u hospitales. Esto cobra aún más relevancia hoy en día, en que muchas de estas compañías de extrema importancia han aumentado sus conexiones a internet, al entregar servicios de manera digital a causa del teletrabajo.

4.– ALTA DISPONIBILIDAD E INTEROPERABILIDAD

Otro factor para tener en cuenta al momento de llevar a cabo una transformación digital es construir servicios o sitios que cuenten con una alta disponibilidad, es decir, alojados de forma de ofrecer mayor disponibilidad, en cualquier momento y no importando la demanda que reciban.

Pero el principal desafío se centra en la interoperabilidad. Según la recientemente aprobada Ley N°21.180, el principio de interoperabilidad consiste en que los medios electrónicos deben ser capaces de interactuar y operar entre sí al interior de la Administración del Estado, a través de estándares abiertos que permitan una segura y expedita interconexión entre ellos.

Bajo este contexto resulta válido tener en consideración los riesgos que se ciernen sobre los procesos tecnológicos y humanos que permiten que la interoperabilidad ocurra de una manera segura.

Algunos de estos riesgos son los tradicionales que afectan a los aplicativos y sistemas operativos sobre los cuales se implementan estos servicios de intercambio automatizado de información por medios electrónicos. Estos son las vulnerabilidades propias de los aplicativos, malos controles de ingreso de datos que permiten inyecciones de SQL o uso de protocolo de comunicación no seguros que exponen los datos a terceras partes, la falta de actualización y parches de los sistemas operativos entre otros.

La agrupación OWASP ha identificado lo 10 problemas más recurrentes y críticos en el uso de API que afectan a los esquemas de interoperabilidad.

LAS TOP 10

API1: AUTORIZACIÓN DE NIVEL DE OBJETO
Las API tienden a exponer los puntos finales que manejan identificadores de objetos, creando un problema de control de acceso de nivel de amplia superficie de ataque. Las verificaciones de autorización a nivel de objeto deben considerarse en cada función que acceda a una fuente de datos utilizando una entrada del usuario.

API2: AUTENTICACIÓN DE USUARIO ROTA
Los mecanismos de autenticación a menudo se implementan de manera incorrecta, lo que permite a los atacantes comprometer los tokens de autenticación o aprovechar las fallas de implementación para asumir las identidades de otros usuarios de forma temporal o permanente.

API3: EXPOSICIÓN EXCESIVA DE DATOS
Esperando implementaciones genéricas, los desarrolladores tienden a exponer todas las propiedades de los objetos sin considerar su sensibilidad individual, confiando en que los clientes realicen el filtrado de datos antes de mostrárselos al usuario.

API4: FALTA DE RECURSOS Y LIMITACIÓN DE TARIFAS
Muy a menudo, las API no imponen ninguna restricción sobre el tamaño o la cantidad de recursos que puede solicitar el cliente / usuario. Esto no solo puede afectar el rendimiento del servidor API, lo que lleva a la denegación de servicio (DoS), sino que también deja la puerta abierta a fallas de autenticación como la fuerza bruta.

API5: AUTORIZACIÓN DE NIVEL DE FUNCIÓN ROTA
Las políticas de control de acceso complejas con diferentes jerarquías, grupos y roles, y una separación poco clara entre las funciones administrativas y regulares, tienden a generar fallas de autorización. Al explotar estos problemas, los atacantes obtienen acceso a los recursos y / o funciones administrativas de otros usuarios.

API6: ASIGNACIÓN MASIVA
La vinculación de los datos proporcionados por el cliente (por ejemplo, JSON) a los modelos de datos, sin un filtrado de propiedades adecuado basado en una lista de permitidos, generalmente conduce a una asignación masiva. Adivinar las propiedades de los objetos, explorar otros puntos finales de la API, leer la documentación o proporcionar propiedades de objetos adicionales en las cargas útiles de las solicitudes permite a los atacantes modificar las propiedades de los objetos.

API7: MALA CONFIGURACIÓN DE SEGURIDAD
La mala configuración de seguridad es comúnmente el resultado de configuraciones predeterminadas no seguras, configuraciones incompletas o ad-hoc, almacenamiento en la nube abierta, encabezados HTTP mal configurados, métodos HTTP innecesarios, uso compartido de recursos de origen cruzado permisivo (CORS) y mensajes de error detallados que contienen información confidencial.

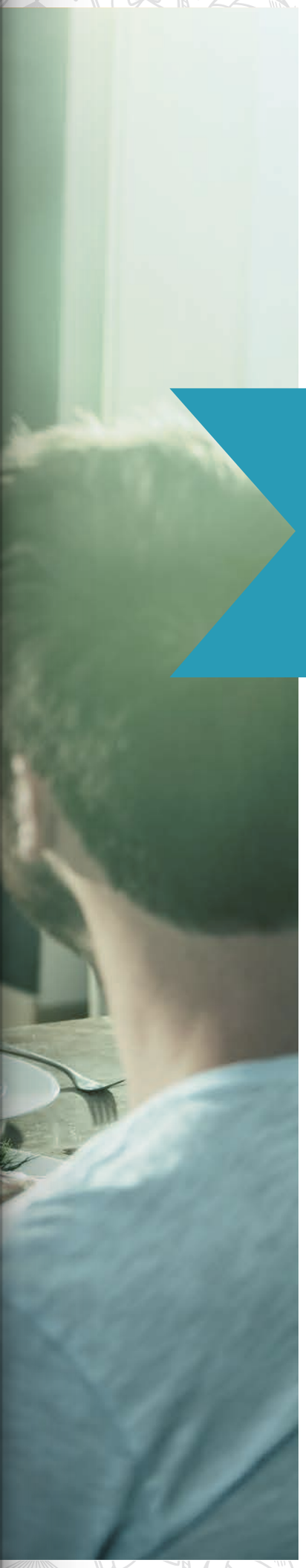
API8: INYECCIÓN
Los defectos de inyección, como SQL, NoSQL, Command Injection, etc., ocurren cuando se envían datos que no son de confianza a un intérprete como parte de un comando o consulta. Los datos maliciosos del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la debida autorización.

API9: GESTIÓN INADECUADA DE ACTIVOS
Las API tienden a exponer más puntos finales que las aplicaciones web tradicionales, lo que hace que la documentación adecuada y actualizada sea muy importante. Los hosts adecuados y el inventario de versiones de API implementadas también juegan un papel importante para mitigar problemas como las versiones de API obsoletas y los puntos finales de depuración expuestos.

API10: REGISTRO Y MONITOREO INSUFICIENTES
El registro y la supervisión insuficientes, junto con una integración faltante o ineficaz con la respuesta a incidentes, permite a los atacantes atacar aún más los sistemas, mantener la persistencia, cambiar a más sistemas para manipular, extraer o destruir datos. La mayoría de los estudios de infracciones demuestran que el tiempo para detectar una infracción es de más de 200 días, generalmente detectados por partes externas en lugar de procesos internos o monitoreo.

¿Qué es la **seguridad API?**

Un elemento fundamental de la innovación en el mundo actual impulsado por las aplicaciones es la API. Desde bancos, comercio minorista y transporte hasta IoT, vehículos autónomos y ciudades inteligentes, las API son una parte fundamental de las aplicaciones móviles, SaaS y web modernas y se pueden encontrar en aplicaciones internas y de cara al cliente. Por naturaleza, las API exponen la lógica de la aplicación y los datos confidenciales, como la información de identificación personal (PII) y, debido a esto, se han convertido cada vez más en un objetivo para los atacantes. Sin API seguras, la innovación rápida sería imposible.



CIBERGUÍA

CÓMO PROTEGERSE DE LOS FRAUDES *de Verano*

En verano se multiplica la demanda de arriendo de viviendas para vacaciones, ya que cada vez son más personas las que deciden arrendar alguna propiedad por Internet, debido a sus numerosas ventajas: más económico, rápido y tienen a un sólo clic diversas opciones.

Sin embargo, junto a esta tendencia aparecen también los fraudes con anuncios de arriendo vacacionales por Internet, una práctica delictiva muy popular en los últimos años.

¿CÓMO FUNCIONAN **LOS FRAUDES DE VERANO?**

1 La trampa comienza con la creación de un anuncio falso, utilizando fotografías robadas de otros anuncios con una descripción y un precio muy atractivo. Este señuelo tiene como objetivo atraer el interés de las potenciales víctimas y, al mismo tiempo, generar confianza.

2 Para esto, los estafadores usan páginas web especializadas, legales y fiables como Airbnb, Booking o Tripadvisor, y así publicar estas ofertas que resultan ser una trampa para los usuarios.

3 En ocasiones, el ciberdelincuente usa un intermediario que reside en nuestro país para recibir y luego reenviar el pago. Con esto, buscan dificultar las labores de identificación del verdadero estafador.

4 Otro tipo de fraude consiste en enviar correos con enlaces a supuestas webs fiables, pero que realmente son falsas. El objetivo es que compartamos nuestros datos bancarios, información personal u otros datos sensibles dentro de la web fraudulenta.

5 Como usuarios, nos dejamos llevar por la sensación de estar frente a una gran oportunidad y, como consecuencia, hacemos un pago por adelantado para no dejar escapar la oportunidad. Finalmente, sin saberlo, somos estafados.

6 Días, semanas o meses más tarde, cuando tratamos de contactarnos con el anunciante, los intentos serán en vano, ya que la publicación habrá desaparecido de la web, al igual que nuestro dinero. Probablemente, terminaremos en la dirección que aparecía en el aviso para darnos cuenta de que no existe tal propiedad, ni forma de contactar con el anunciante.

¿Qué podemos hacer para **evitar este tipo de fraudes?**

El CSIRT entrega algunas recomendaciones claves para tener en cuenta a la hora de irse de vacaciones, y así evitar caer en este tipo de fraudes:

1. Anuncios muy atractivos y precios muy económicos, no confiar. Muchos estafadores buscan atraer el interés de los usuarios por medio de fotos atractivas, zonas muy demandadas o descripciones muy ll-a mativas.
Te aconsejamos investigar los precios de mercado, compáralos con los de la oferta y continúa con el resto de las recomendaciones.

2. Descripción con prisas. Si el anuncio publicado está mal redactado, tiene faltas ortográficas o se nota que ha sido escrito apurado, es posible que nos encontremos ante una estafa. Es habitual que se utilicen traductores de texto automáticos, dejando el aviso con errores o mal redactado. Lo mismo puede aplicarse a las comunicaciones con el arrendador.

3. Problemas y más problemas. Arrendar una vivienda en verano no debería ser una carrera de obstáculos. Generalmente, los anuncios fraudulentos sólo muestran un correo electrónico y, una vez recibido el mail, los ciberdelincuentes contestan a los interesados desde otro correo, con el fin de dificultar el seguimiento en caso de denuncia. En ocasiones, también incluyen un teléfono de contacto, pero siempre se en cuentra apagado o no hay respuesta.

4. Autenticidad del anunciante y del inmueble. Es fundamental comprobar la identidad del anunciante, la titularidad y existencia del inmueble.
¡Cuidado! La documentación se puede falsificar, incluso hay casos donde los estafadores utilizan las propias fotocopias de CI de otras personas que han timado, usurpando su identidad.
Como consejos, es posible usar herramientas como Google Street View para ver si la propiedad que que remos arrendar existe o comprobar desde Google imágenes si las fotos del anuncio se han empleado en otras webs o plataformas diferentes.

5. Métodos de pago poco fiables. Es posible que el anunciante solicite un adelanto para reservar el alojamiento. Aunque no es una señal de alarma, debemos tener cuidado con el método de pago. Si nos propone una forma alternativa a la plataforma, es mejor desconfiar. Este tipo de webs disponen de plataformas de pago que aseguran nuestras transacciones.

Los ciberdelincuentes recurren a métodos cada vez más sofisticados para conseguir su objetivo, por eso recomendamos seguir el sentido común para evitar este y otros tipos de fraudes. Si algo es gratis o demasiado atractivo, es muy probable que el producto seamos nosotros.

¿QUÉ HACER EN CASO DE ESTAFA?

1. **DENUNCIA** la falsa oferta a los responsables de la plataforma.
2. **RECOPILA** todas las pruebas que puedas de la estafa e información sobre el anunciante.
3. **ACUDE** también a las autoridades pertinentes, como la Policía de Investigaciones (PDI), llamando al

+562 2708 0658

PRESENTE Y FUTURO DEL MODELO DE IDENTIDAD **DIGITAL EN ESTONIA**

La nación báltica es una de las más digitalizadas del mundo, gracias a las casi dos décadas que llevan construyendo e-Estonia, su ecosistema de interacción digital con los servicios del Estado.

Helen Raamat, eID Product Owner, Electronic Identity Management Department, RIA

Piret Urb ,Head of International Relations Information System Authority, RIA

El sistema de identidad digital es uno de los elementos de infraestructura centrales de e-Estonia, y éste consiste en un número de identificación único y persistente en el tiempo, que se entrega a cada uno de los residentes y que es parte fundamental de sus credenciales de identidad electrónica ("e Identity", o eID). Estonia cuenta con seis soluciones de eID en donde se encuentra incorporado este número de identificación. Tres de ellos -Digi-ID, e-Residence Digi-ID y Mobi-il-ID- son solo para usos electrónicos, mientras que el resto también puede ser usado como documento de identidad físico. Asimismo, existe un eID emitido por el sector privado y ampliamente usado, conocido como Smart-ID.

Para el funcionamiento de la identidad electrónica, el Estado debe asegurar el funcionamiento de una infraestructura de clave pública (PKI). Este modelo entrega dos claves, una secreta, la que debe ser protegida y solo puede ser usada por la persona a la cual le fue emitida; y otra pública que está disponible para cualquiera.

Gracias a que existe un lazo específico entre estas dos claves, este modelo permite un acceso seguro a los servicios electrónicos, posibilitando la autenticación y firma digitales. También permite transferir datos de forma segura y confidencial. Además, todas las operaciones realizadas con eID (autenticación, firma y descifrado) están protegidas con PIN.

Sin duda que el modelo de Estonia es muy atractivo e interesante, por eso para conocer más sobre esto, conversamos con Helen Raamat, eID Product Owner, Electronic Identity Management Department, RIA; y Piret Urb, Head of International Relations Information System Authority (RIA), quienes en esta entrevista nos hablaron sobre el proceso de cambios digitales que ha vivido su país, estrategia y los riegos de ser una nación tan digitalizado, entre otros temas.

¿Qué nuevas funciones y características pueden esperar los residentes de e-Estonia en el futuro próximo?

En Estonia, tal como en todo el mundo, esperamos impacientes que la crisis de salud termine. Por eso, el gobierno estonio, junto a la OMS, lanzó la iniciativa de contar con un pase inteligente de vacunación globalmente reconocido que permita a las personas volver a viajar. El proyecto aún está en fase piloto y ya varios países han sido contactados para unirse.
Además, el Estado está trabajando en incrementar los procesos automáticos en los servicios estatales y la comunicación con el gobierno, a través del portal eesti.ee. Por ejemplo, al nacer un hijo y registrarlo con su respectivo nombre, se envía automáticamente un e-mail a sus padres para que empiecen a recibir sus respectivos beneficios, sin tener que tratar por separado con los distintos organismos estatales responsables de ellos.
Otra funcionalidades en las que hemos estado trabajando es en implementar inteligencia artificial y machine learning para ser más eficiente y entregar mejores servicios. Ya contamos con más de 50 soluciones de IA operativas y otras 40 en proceso. Uno de estos proyectos es la construcción de un asistente virtual basado llamado #KrattAI. No será simplemente una interfaz basada en IA para usar los servicios públicos, sino que permitirá a las personas realizar sus trámites públicos desde cualquiera de los principales dispositivos y asistentes personales disponibles en el futuro.

¿Qué los llevó a implementar un sistema de identidad digital en Estonia y cuán difícil fue convencer al público de apoyarlo?

Comenzamos con la búsqueda de implementar un carnet de identidad, ya que el pasaporte era muy grande y pesado para llevar consigo todos los días. Si bien, la negociación en el Parlamento no fue fácil, la Ley de Documentos de Identidad fue aprobada en 2002, lo que hizo del carnet de identidad un documento obligatorio para todos.
Además de las iniciativas, creo que lo fundamental es que tenemos un gobierno innovador y abierto de mente, que logró impulsar esta iniciativa a través del Parlamento y así el país adoptó un sistema electrónico de administración de identidad. Gracias a esto, el Estado creó una base al establecer esta herramienta y con ello el ecosistema digital comenzó a prosperar. Sin embargo, tomó algunos años antes de que las personas entendieran los beneficios y la eficiencia del uso de la identidad electrónica.

¿Cuáles fueron las principales inquietudes de seguridad y privacidad que tuvo el público antes de la implementación de la identidad digital de Estonia y cómo las enfrentaron?

En un inicio, las preocupaciones se daban principalmente por la falta de conocimiento y experiencia sobre este tema. Probablemente, lo que nos benefició fue que Estonia comenzó este proceso de digitalización tiempo después de su independencia, por lo que había una fuerte disposición a adoptar las últimas innovaciones disponibles en el mercado mundial y hacer lo mejor para que funcionaran.
Los problemas de privacidad fueron resueltos en la medida en que aparecieron, hasta que un sistema sólido y seguro estuvo en funcionamiento. Si bien ya existía un registro de población, las siguientes bases de datos fueron creadas siguiendo el principio de privacidad por diseño. Estas son fuertemente reguladas por la Ley de Protección de Datos Personales y el GDPR de la Unión Europea. Toda persona es dueña de sus propios datos y tiene acceso a ellos.

¿Cuáles son las principales amenazas o riesgos que enfrentan sistemas de identidad digital como el de Estonia?

En términos generales, una mala evaluación de riesgos siempre es un peligro y la administración de riesgos en el ecosistema de identidad digital es aún un campo muy reciente, por lo que no existen investigaciones extensas o casos de estudios con un análisis sobre este tema. Estonia tiene 20 años de experiencia y son realmente valiosos para todos los países del mundo.
Por otra parte, sí consideramos que puede ser una amenaza la nueva tecnología cuántica, pero no sabemos mucho de ello todavía. Creemos que puede ser capaz de descifrar algunas partes de la criptografía hoy en uso, pero es solo una hipótesis, y ciertamente también habrá soluciones para ello. La dependencia de proveedores específicos también puede convertirse en un riesgo, pero eso es algo que se debería reducir en los próximos años.

¿Creen que su estrategia de identidad digital es replicable en otros países? ¿Qué necesitan naciones como Chile para tener un sistema como el de Estonia?

Cada país es diferente, con sus propias tradiciones, cultura y necesidades. Para comenzar, siempre tenemos que pensar cuál es el problema que se busca resolver y luego considerar la forma más apropiada de hacerlo. El modelo de Estonia, con algunas modificaciones, por supuesto, puede funcionar en muchos países donde la confianza de los ciudadanos hacia su gobierno sea alta. A esto es necesario sumar que la sociedad tenga un deseo de cambio y desarrollo digital. Con esto me refiero a un real interés por reducir la burocracia y la corrupción, impulsar la economía y crear transparencia. Al menos, este era un deseo fuerte en Estonia el año 2000, aunque nadie sabía realmente hasta dónde nos llevaría.

¿Cuán necesario es implementar sistemas basados en el blockchain para tener una infraestructura de identidad digital segura y confiable?

Según nuestra experiencia, no es necesario, pero de todas maneras nos mantenemos al tanto de la evolución de las tecnologías basadas en blockchain. Por el momento, aún carece de respaldo legal y no tiene el soporte técnico suficiente que exigen las soluciones de identidad de nivel nacional de alta confiabilidad, basadas en la regulación eIDAS.

DATOS DE ESTONIA

Las primeras tarjetas de identidad fueron emitidas en enero de 2002, y la primera firma digital fue ejecutada en octubre de ese año.
Uno de los primeros y más usados servicios electrónicos ha sido la declaración de impuestos online.
Desde 2005 está disponible i-voting, un sistema que permite a las personas sufragar desde cualquier computador en el mundo conectado a internet. Facilita la vida de muchos estonios viviendo en países sin una embajada, o para quienes en Estonia no pueden o no quieren salir el día de la elección.

TÉCNICAS Y AMENAZAS **EN AUGE PARA 2021**

El crimen digital nunca deja de buscar nuevas formas de burlar a la ciberseguridad, en una carrera armamentista que solo se aceleró durante 2020 producto de la pandemia del coronavirus. En ese contexto, estas son algunas de las técnicas y tecnologías que diversos expertos estiman serán las que probablemente tengan más relevancia en el mundo de la ciberseguridad y las amenazas digitales este año.

Los ciberdelincuentes mejoran sus modos de ataque

DEEPFAKES: APROVECHANDO LA CONFIANZA DE LAS VIDEOLLAMADAS

Hace poco era monopolio de estudios de cine con altos recursos, pero hoy se pueden hacer con aplicaciones en el celular: son los deepfakes, videos a los que se le reemplaza o crea un rostro distinto y altamente realista a través de machine learning (específicamente, al principio eran realizados usando deep learning, de ahí su nombre).

Esta técnica se puede usar para diseminar noticias falsas, haciendo parecer que una persona dijo algo que no, o para crear contenido pornográfico sin autorización de la persona dueña de la cara que se superpone al video original, lo que puede ser usado para humillarla y chantajearla. Ya ha habido denuncias de chantajes a mujeres en India, por ejemplo, a través del uso de desnudos falsos con sus rostros.

Más aún, gracias a la expansión de las videollamadas durante la pandemia, se han visto casos de ingeniería social avanzada donde se realizan video llamadas empleando técnicas de deepfake, en donde un atacante finge ser un familiar o amigo de la víctima. En Chile se ha denunciado en las redes sociales el uso de videollamadas breves con una forma primitiva de deepfake (usando como rostro el sacado de fotos de Facebook) como apoyo a estafas que usan ingeniería social y descubrimiento pasivo para engañar a la víctima y hacerle creer que el delincuente es un familiar y así conseguir que se le haga una transferencia de fondos.

Una variante igualmente preocupante es el desarrollo de "clones de voz", como el que engañó al ejecutivo de una empresa alemana para hacerle depositar US$ 243 mil, tras hacerse pasar por su gerente general, replicando su voz con inteligencia artificial (una variante del ataque tipo BEC, business email compromise).

PELIGROS EN LA NUBE: MALAS CONFIGURACIONES

Los servicios de infraestructura en la nube se han convertido en una gran opción para mantener las operaciones durante la pandemia. Por eso, para 2021, Gartner estima un crecimiento del 29% en las ventas de este servicio. Por tanto, las filtraciones de información desde la nube también crecerán, en especial debido a malas configuraciones y protecciones asignadas, lo cual es también resultado del déficit de profesionales de la seguridad informática.
Las configuraciones inseguras ya son hoy un problema. Por ejemplo, según un informe de Sophos publicado a mediados del año, dos tercios las empresas que dijeron haber sufrido una filtración desde una nube pública declaraban que eso fue posible por una mala configuración, mientras el resto acusó el robo de credenciales de autenticación.

USO DE MALWARE EN TRABAJADORES REMOTOS

Los usuarios que trabajan remoto desde sus hogares ya son objetivo de los ciberdelincuentes, quienes ingresan a través de ellos a las redes corporativas. Los atacantes, al analizar a un trabajador remoto, comprenden sus características para coordinar a través de ellos un ataque a las redes corporativas y no levantar sospechas, la mayoría de las veces utilizando ingeniería social.
Kaspersky es una de las firmas que poner entre sus tendencias un incremento en los ataques a aplicaciones de trabajo, explotando vulnerabilidades de, por ejemplo, los accesos VPN. De hecho, las vulnerabilidades de los RDP (protocolos de escritorio remoto), ampliamente usados para las conexiones VPN, fueron la principal vía de acceso del ransomware en la primera mitad de 2020, de acuerdo con Coveware, Emsisoft y Recorded Future. Una tendencia que viene en crecimiento incluso antes de la pandemia, aclaran, cuando bandas decidieron especializarse en escanear redes vulnerables y luego realizar ataques de fuerza bruta sobre ellas.

RANSOMWARE: AUGE EN LA INFRAESTRUCTURA CRÍTICA, Y USO DE LA LIBERACIÓN DE INFORMACIÓN CONFIDENCIAL COMO AMENAZA

A medida que los sistemas de TI convergen cada vez más con los sistemas de tecnología operativa (OT), especialmente la infraestructura crítica serán el objetivo de los ciberdelincuentes a través de la extorsión, difamación y desconfiguración, colocando incluso en riesgo vidas humanas.
Kaspersky espera que crezca aún más la cantidad de ataques de extorsión a través del ransomware y ataques DDoS, además de exploits de día cero. Al mismo tiempo, desde Eset esperan un auge del ransomware que no solo impide el acceso a los datos de la víctima, sino que va publicando de a poco la información privada de la empresa, sus socios y clientes, para aumentar la presión a fin de obtener el pago.
En Chile estos ataques han sido muy sonados en los últimos años, afectando famosamente en 2020 al Banco Estado (causa de Sodinokibi) y a Cencosud (por Egregor), por ejemplo.

Tendencia Digital

ATAQUES DE INGENIERÍA SOCIAL APOYADOS POR EL INTERNET DE LAS COSAS

Los dispositivos que interactúan con los usuarios como los dispositivos inteligentes u otros sistemas en el hogar (IoT), serán utilizados para realizar ataques más sofisticados. La información que se logre extraer puede incluir las rutinas diarias, hábitos, información financiera, entre otras, la cual será de ayuda para realizar ataques más precisos basados en ingeniería social.
Los ataques "inteligentes" pueden además ser más certeros para apagar sistemas de seguridad, deshabilitar cámaras o secuestrar dispositivos, además de posible extorsión por información sensible o confidencial, robo de credenciales o rescate de sistemas.

AMENAZAS FINANCIERAS: ROBO DE BITCOIN Y SKIMMING DIGITAL A SERVIDORES

De acuerdo con la firma rusa de ciberseguridad Kaspersky, entre las tendencias en ciberdelitos financieros para 2021, mencionan el MageCarting, o el robo de los datos de tarjetas de crédito directamente desde los servidores. El también llamado webskimming afectó, por ejemplo, de parte solo del grupo criminal Keeper, a más de 570 sitios de e-commerce en el mundo, con un total de 250 mil clientes, incluyendo negocios en Chile.
En el mismo ámbito, Kaspersky advierte de un posible mayor riesgo del robo de Bitcoin, a medida que personas en economías frágiles y alta inflación podrían ser más proclives a realizar fraudes en criptodivisas que en la moneda local, especialmente Bitcoin.

AUGE DEL MALWARE "FILELESS"

Los ataques con códigos maliciosos que no necesitan grabarse en la memoria del equipo objetivo para atacar, conocidos como fileless, deberán aumentar este 2021. El concepto no es nuevo, y durante 2020 se vio un aumento en su popularidad, según entidades como la ONU y el NCSC del Reino Unido. Al no requerir de la descarga de un archivo, y funcionar en base a programas ya existentes en los sistemas, estos ataques son más difíciles de detectar. Para contrarrestarlos, se recomienda la implementación de sistemas como los EDR.

HOSPITALES Y CLÍNICAS: INTEGRANDO CIBERSEGURIDAD

El área de la salud suele trabajar con dispositivos de alta tecnología para sus procedimientos médicos, dejando potenciales brechas que faciliten la intrusión a sus sistemas, su secuestro, espionaje o inutilización. Hospitales y clínicas se han vuelto un objetivo clave en el mundo para los atacantes, quienes roban datos sensibles y destruyen fichas clínicas, lo que afecta a miles de pacientes. En 2021 las inversiones en ciberseguridad para el área de la salud pública y privada se verán aumentadas en todo el mundo.

Proteger el área de la salud es clave, lógicamente, para que no se multipliquen casos como el ransomware ocurrido en septiembre en varios hospitales de Alemania, que bloqueó sus sistemas e impidió la atención de varios pacientes, incluyendo uno que finalmente falleció. Muchos medios señalaron que esta persona había muerto debido al ransomware, pero la justicia determinó que el ciberataque no terminó con su vida, ya que aún si hubiera podido ser atendida, no tenía esperanzas de sobrevivir.

... AUNQUE TAMBIÉN AUMENTA **LA ADOPCIÓN DE MEJORES TÉCNICAS DE PROTECCIÓN**

ZERO TRUST: el modelo de arquitectura "confianza cero"

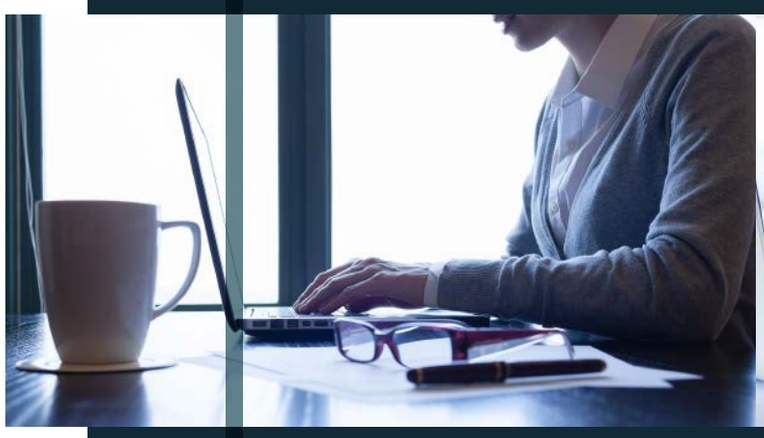
Este modelo se ha abierto paso en la industria por su sólida y estricta seguridad, dificulta el movimiento lateral de un atacante y es una excelente forma de proteger la confidencialidad e integridad de los activos más importantes. Y si ya venía como tendencia en alza, la coyuntura solo hará crecer la implementación de modelos zero trust, o inspirados en él. Esto porque la pandemia obligó a múltiples profesionales acceder a las redes corporativas desde sus equipos en el hogar, exponiéndose a un mundo nuevo de amenazas, y este nuevo modelo es perfecto para reducir los riesgos de escalamiento y movimiento lateral.

INTEGRACIÓN IA: RESPUESTA A INCIDENTES AUTOMATIZADA E INTELIGENTE

El tiempo de respuesta a un ataque malicioso es un determinante en el impacto de incidente, ya que mientras más tiempo pase, más tiempo habrá tenido el atacante para investigar a la víctima y desplegar sus ataques. La inteligencia artificial junto con la automatización y machine learning pretenden disminuir estos tiempos a tan solo milisegundos, encontrando vulnerabilidades de día cero y mitigando patrones maliciosos, permitiendo a los equipos de respuesta trabajar con mayor eficiencia.

PYMES MÁS ACOMPAÑADAS EN **SU TRANSFORMACIÓN DIGITAL**

Más de 30 mil pequeñas y medianas empresas han contado con el apoyo de esta fundación, que busca orientar y entregar las herramientas necesarias a los emprendedores para que logren avanzar en el proceso de digitalización de su negocio. Si tienes una pyme y quieres sumergirte en este importante cambio, te contamos las iniciativas que lleva a cabo País Digital.



Las pymes representan un importante sector para la economía, al generar fuentes de trabajo e impulsar la economía de nuestro país. Hasta octubre de 2019, en Chile existían más de 900 mil empresas, de ellas 220 mil eran pymes y 680 mil, microempresas. Por esto, su crecimiento y desarrollo es fundamental, y la modernización en los procesos digitales constituye un importante avance y permite darles una continuidad operacional, especialmente desde el 2020 con la llegada del Coronavirus.

Sin embargo, no todas las organizaciones están preparadas o no saben cómo convertir su negocio. Esta necesidad e inquietud de crear una cultura digital tuvo un grupo de empresarios y emprendedores chilenos el año 2001, en una misión público-privada, quienes con la finalidad de impulsar y masificar a través de distintas acciones y proyectos la transformación digital en Chile formaron la Fundación País Digital (FPD).

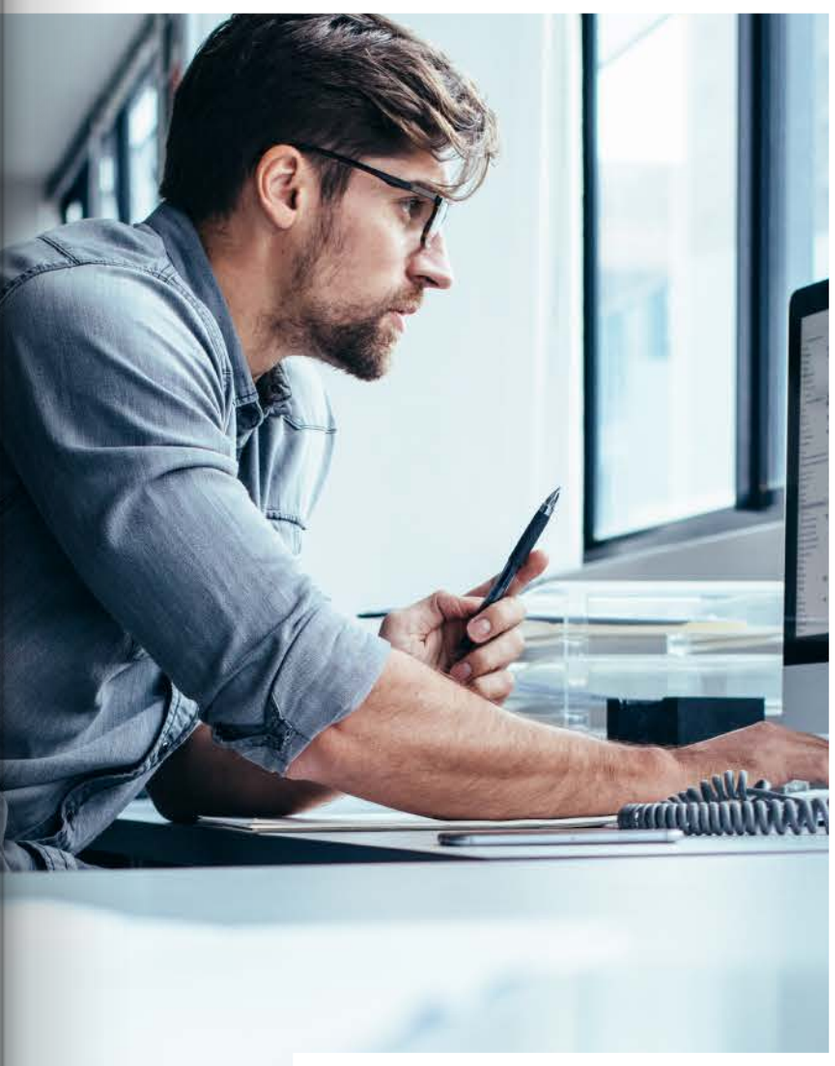
Esta fundación cuenta con 26 socios vigentes y está presidida por Pelayo Covarrubias, quien asegura: "Nuestro principal objetivo es preparar a las empresas ante el avance de las nuevas tecnologías y se puedan mantener vigentes frente a las necesidades de los consumidores. Buscamos entregarles todas las herramientas y conocimientos para que puedan modernizarse y avanzar en el proceso de transformación digital. Hemos organizado talleres y seminarios, que han permitido llegar en forma presencial a más de 5 mil pymes y en forma remota, debido a la pandemia, hemos logrado capacitar a 25 mil más. Sumado a lo anterior, confeccionamos un libro gratuito sobre soluciones digitales para pymes".

PROYECTOS Y AVANCES DIGITALES PARA LAS PYMES

La crisis sanitaria obligó a muchas empresas a volcar sus negocios al e-commerce contribuyendo, de cierta manera, a acelerar el proceso digital. Pero este trabajo ya lo estaba realizando País Digital hace algunos años para "preparar el futuro de Chile y el mundo, construyendo una sociedad mejor de la mano de la ciencia, educación, innovación y tecnología".

Es así como algunas de las iniciativas que han venido realizando desde el año 2001 son: "Chequeo Digital", una herramienta en línea y gratuita para realizar un autodiagnóstico del nivel de madurez digital de cualquier empresa; Pyme Activa Antofagasta, un proyecto junto con BHP que consiste en construir "toolkits" que describan planes de asesoría e instalación y software; Acelera tu Negocio B2B, un programa de formación, mentoría y activación en ventas para las micro y pequeñas empresas del segmento B2B.

Junto con esto, la fundación ha organizado talleres y seminarios, entregando herramientas y conocimientos para profesionalizar sus negocios, permitiendo llegar en forma presencial a más de 5 mil pymes en Santiago y regiones y en forma remota, debido a la pandemia, se logró capacitar a 25 mil más.



RECOMEN**DACIONES**

En ocasiones, comenzar con el proceso de digitalización para algunos puede ser engorroso o causar cierto temor. Por esto, la Fundación País Digital entrega los siguientes consejos para iniciar el proceso de transformación digital:

- Digitalizar el negocio no siempre requiere de una gran inversión, por eso es importante informarse de las tecnologías que existen y salir de la zona de confort.
- Averiguar sobre las herramientas gratuitas o de bajo costo que permiten a las empresas sumarse al carro de la digitalización, lo que trae un gran número de beneficios.
- Arriesgarse y atreverse a digitalizar el negocio para que no queden fuera de la revolución industrial.

Como reflexión, Pelayo Covarrubias enfatiza: "Estamos viviendo la cuarta revolución industrial, la que se ha visto acelerada por lo que nosotros llamamos el 'Laboratorio COVID', que nos ha enseñado a relacionarnos, trabajar, estudiar y comprar, entre muchas otras acciones cotidianas, de una forma muy distinta a la que estábamos acostumbrados y donde la gestión de datos y la inteligencia artificial serán procesos cada vez más comunes, por ello es vital que las pequeñas y medianas empresas se sumen al carro de la digitalización".

Para conocer más sobre Fundación País Digital y sus iniciativas, puedes ingresar a su sitio web:
https://paisdigital.org/

Junto con esto, queremos destacar que este proceso también se debe realizar considerando todas las medidas de ciberseguridad para evitar y prevenir que la empresa sea víctima de un ciberataque. Para tener una pyme segura, puedes encontrar algunas recomendaciones elaboradas por el CSIRT en el siguiente enlace:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-de-seguridad-para-pymes/

LA DIGITALIZACIÓN **DE LA ADMINISTRACIÓN PÚBLICA**

Sabemos que la transformación digital consiste en la integración de las nuevas tecnologías en todas las áreas de una institución para cambiar su forma de funcionar y que ofrece muchas oportunidades de crecimiento en todos los ámbitos, sectores, regiones y cualquier tipo de empresa o institución, ya que conlleva la mejora de los procesos que aumentan la eficacia y reduce los costos. Mucho se ha hablado de ella y de su implementación en el ámbito privado, pero ¿qué sucede en el mundo de la Administración Pública?

UN GIGANTESCO CAMBIO EN LA FORMA QUE OPERA LA **ADMINISTRACIÓN PÚBLICA SE APROXIMA**

Realizar trámites presenciales, reunir documentos y carpetas con certificados en papel emitidos por distintos servicios pú blicos son acciones que tienen sus días contados. Ello, debido a que con la Ley N°21.180 sobre la Transformación Digital del Estado comienza un paso sin retorno hacia una relación del Estado con los ciudadanos cero papel y 100% digital, que debe concluir a fines de 2024 como plazo máximo.

Hasta ahora, la transformación digital en la Administración Pública ha sido un asunto de altos y bajos, cuyos avances esta ban sujetos generalmente a la planificación de cada institu ción o departamento. Con la ley, esto se acaba y ya no depen derá de la buena voluntad de las instituciones ni será una ex cepción en algunas de ellas. Esta ley es un cambio de paradig ma en cómo se ejerce la función pública.

Pero este cambio no es repentino, sino que se viene trabajan do en él desde antes de que se aprobara la ley. Esto, porque en enero de 2019 el Presidente Sebastián Piñera dictó el Instruc tivo de Transformación Digital, para que gradualmente todos los organismos operen en la modalidad cero papel, digitalicen trámites, eliminen las filas y usen la Clave Única como medio para autenticar la identidad de las personas.

Así y con fecha 11 de noviembre de 2019 se publicó en el Diario Oficial la Ley Nº 21.180 que establece la "Transforma ción digital del Estado", por medio de la cual se modifican diversos cuerpos legales con el objetivo de establecer la obli gatoriedad del soporte electrónico, de manera que todos los nuevos trámites y servicios que el Estado ofrece a los ciuda danos sean preferentemente digitales.

La nueva ley dispone que los organismos públicos deberán ha bilitar plataformas electrónicas que funcionarán 24/7 aten diendo las solicitudes de las personas. Este trámite concluirá con una respuesta electrónica, la que tendrá la misma validez que los certificados en papel y que será notificada en los nuevos domicilios digitales gestionados por el Registro Civil.

De esta manera, la ley busca mejorar la eficiencia y la comuni cación entre los servicios estatales, para lo cual modifica (principalmente) la Ley 19.880, que establece las bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado.

¿EN QUÉ CONSISTEN LOS CAMBIOS Y CÓMO BENEFICIAN A LOS CIUDADANOS?

La ley tiene tres pilares fundamentales: Cero Filas, Cero Papel e Identidad Digital, lo que se refleja en los cambios que establece.

INTERCAMBIO DE DOCUMENTOS EN PODER DE LA ADMINISTRACIÓN DEL ESTADO

Una de las modificaciones más importantes de la nueva ley y que mayor impacto tendrá respecto de los ciudadanos, dice relación con que un servicio público no pida La ley establece que respecto a dichos documentos los órganos de la administración tendrán la facultad de requerirlos a otros órganos mediante una plataforma electrónica destinada al efecto.

NOTIFICACIONES ELECTRÓNICAS

En materia de notificaciones, la Ley N°21.880 cambia el antiguo sistema de notificación por carta certificada, estableciendo la obligatoriedad de que éstas sean efectuadas por un medio electrónico (salvo excepciones), a un sistema de domicilios digitales únicos, el cual se compondrá por las direcciones de correo electrónico que dispongan los interesados en un procedimiento y cuyo registro llevará el Servicio de Registro Civil e Identificación.

OBLIGATORIEDAD DE SOPORTE Y COMUNICACIÓN ELECTRÓNICA

Se establece que los procedimientos administrativos deberán expresarse por medios electrónicos, constar en un expediente electrónico, además de que los documentos en soporte papel deberán ser digitalizados. Junto a ello, se establece que toda comunicación en dicho procedimiento deberá realizarse por medios electrónicos.

PLATAFORMAS ELECTRÓNICAS.

La ley establece la obligatoriedad en el uso de plataformas electrónicas para el ingreso de solicitudes, formularios y presentación de documentos respecto de interesados, permitiendo el acceso en línea a los expedientes electrónicos, así como la obtención de copias certificadas generadas por dicha plataforma. de esta manera, los ciudadanos podrán hacer un seguimiento a sus solicitudes de manera fácil, rápida y transparente.

DOCUMENTOS SUSCRITOS CON FIRMA ELECTRÓNICA

El poder para obrar en un procedimiento administrativo podrá constar en un documento suscrito mediante firma electrónica. Estos cambios tendrán un impacto significativo en la relación de los ciudadanos con la administración pública, la que será más rápida, más transparente y menos costosa.

¿EN QUÉ ETAPA SE ENCUENTRA SU IMPLEMENTACIÓN?

La entrada en vigencia de la ley es deferida por evento, encon trándose en las últimas etapas de desarrollo los reglamentos a los que hace referencia la ley. Sin perjuicio de ello, el día 12 de noviembre de 2020 el Presidente Sebastián Piñera firmó el Decreto con Fuerza de Ley (DFL) de Gradualidad que estable ce los detalles de la Ley de Transformación Digital.

EL DFL establece la gradualidad en la implementación de esta ley con plazos diferenciados para las instituciones en función de sus capacidades, presupuesto y madurez tecnológica, con un plazo máximo de cuatro años para implementar las dife rentes iniciativas. De esta manera, los primeros organismos en avanzar en el proceso de transformación digital serán las ins tituciones de la Administración Central del Estado, la Contra loría General de la República y las Fuerzas Armadas y de Orden y Seguridad, seguidas por los Gobiernos Regionales y los Mu nicipios.

La implementación de esta ley así como el cumplimiento de los plazos establecidos es fundamental considerando que hoy, a raíz de la crisis sanitaria, los chilenos realizan el 85% de los trámites con el Estado por internet. Tarea que debe ejecutarse con un fuerte fundamento en ciberseguridad para asegurar la continuidad de los servicios, así como la privacidad de los datos de los ciudadanos e instituciones del Estado.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS

+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl