Ministerio del Interior y Seguridad Pública

En el Mes de la Ciberseguridad **2021**

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERGUÍA PARA LAS PYMES

INTRODUCCIÓN

La vida cotidiana de personas y empresas está cruzada por servicios tecnológicos, que con sus vulnerabilidades los exponen a riesgos cibernéticos. En este contexto, la digitalización de las pymes se vuelve imperativa, pero el proceo no está exento de riesgos, los que deben tomarse en cuenta si no se quiere naufragar a mitad de camino.

Por ejemplo, según el estudio "Ciberseguridad en las empresas chilenas", realizado por IPSOS en 2019, 4 de cada 10 empresas reconocen haber tenido algún ataque cibernético y 40% de las micro, 45% de las pequeñas y el 56% de las medianas empresas se consideran vulnerables frente a ciberataques.

Al mismo tiempo, según la encuesta TIC (2018), solo 7% de las empresas de Chile tenían un área, cargo o rol dedicada la seguridad TIC (31% de las grandes empresas declaró tener un área para resolver incidentes TIC, mientras que en las pymes solo el 5%).

Esto toma especial relevancia por la masiva adopción de tecnologías digitales durante la pandemia. De acuerdo con la OCDE, las pymes chilenas son las que más lo hicieron dentro de los países estudiados (62%), mientras 90% de ellas cree que este cambio será permanente. Sin embargo, la urgencia no se tradujo en una adopción que considerara la ciberseguridad en el proceso, no solo referente a los sistemas, sino que también a la cultura organizacional en torno a ella.

CAMBIO DE PARADIGMA

Ante esta nueva realidad, debemos tener algo bien claro: si una pyme comienza a usar sistemas digitales como redes sociales, puntos de venta, CRM, ERP, entre otros, sin medidas adecuadas de ciberseguridad, están arriesgando la pérdida de todos sus activos y reputación en caso de sufrir un incidente.

En general las medidas tomadas por las pequeñas y medianas empresas son:

- Comprar software de protección
- Entregar información a colaboradores
- Contratar outsourcing de seguridad

Y por el otro, entre los principales ataques que sufren las empresas se cuentan:

- Pérdida temporal de acceso a archivos
- Eliminación de sitios web.
- Corrupción de programas o sistemas
- Pérdida permanente de archivos y del acceso a servicios.

Finalmente, los mayores temores de las pymes ante la perspectiva de sufrir un ataque informático son:

- Fuga de información
- Pérdida de la continuidad operacional
- Sufrir phishing, ransomware y amenazas avanzadas.

Es en vista de estos riesgos y percepciones que preparamos esta guía, con el objeto de ayudar a las pymes a realizar una transformación digital segura con las siguientes herramientas gratuitas.

AUTO EVALUACIÓN

Antes de comenzar a tomar acciones relativas a la mejora de la ciberseguridad de nuestra empresa, es clave saber cuál es su situación actual. Para eso se debe realizar una evaluación, un diagnóstico que nos dirá cuál es el nivel de madurez de la ciberseguridad de nuestra organización, y nos guiará en los aspectos más urgentes que necesitan mejoras.

Estos son algunos de los factores que debemos revisar internamente como compañía al momento de ingresar al ciberespacio o profundizar nuestra relación con él:

1.- Teletrabajo:

La tecnología permite a los emprendedores trabajar desde sus casas, pero al hacerlo, ¿tomamos las mismas precauciones que en la oficina? ¿Realmente conocemos todas las medidas de seguridad que necesitamos? ¿Aumentan los riesgos al utilizar computadores personales? ¿Crecen los riesgos al aumentar las interacciones y transacciones de productos o servicios que realizamos digitalmente?

2.- Comercio electrónico:

Su tasa de penetración llega al 82% en Chile. Empresas de todos los tamaños deben adaptarse a estas condiciones, reinventando sus procesos y adoptando una estrategia de negocios e-commerce. La pandemia impulsó la transformación digital de las empresas, pero no necesariamente acompañada de la adopción de una cultura y sistemas ciberseguros.

3.– Cloud:

La computación en nube (cloud computing) puede significar grandes cambios para las pymes, especialmente en relación con el almacenamiento de datos sensibles. ¿A qué riesgos se exponen en la nube y cómo puedo minimizarlos? ¿Qué historial tiene mi proveedor garantizando la confidencialidad de los datos de sus clientes? ¿Hay datos tan valiosos que me conviene solo manejarlos en servidores propios?

4.– Datos y su privacidad:

Toda la información que maneja un negocio tiene valor, de ahí la importancia de identificar el capital digital de una empresa y resguardarlo adecuadamente.

5.– Concienciación general para sus recursos humanos:

A la hora de hablar de seguridad de la información, siempre suele hablarse de tecnologías y procesos, pero en realidad los protagonistas de la seguridad en las empresas son los empleados que gestionan y utilizan los dispositivos tecnológicos de la organización para trabajar con la información.

Una aproximación gratuita a este tipo de evaluación y las consiguientes recomendaciones se puede encontrar en la Guía de Ciberseguridad para Pymes de la Cámara Nacional de Comercio: **https://pymecibersegura.cl/quest.**

I KIT DE SISTEMAS Y HERRAMIENTAS

Para remediar algunas de las deficiencias detectadas en una organización se pueden emplear distintas herramientas, que son de código abierto, software desarrollados y distribuídos con una licencia que permite que cualquier persona pueda ver el código y utilizarlo libremente, sin restricciones.

A.– Herramientas para analizar seguridad

Tienen como objetivo analizar los riesgos informáticos y evaluar las vulnerabilidades a las que están expuestas las empresas, de manera de prevenir un ciberataque que ponga en peligro los activos de la empresa o se exponga al robo de información, como los datos de sus clientes.

Herramientas de monitoreo de redes y seguridad

- **WAZUH:** https://wazuh.com/
- **NAGIOS:** https://www.nagios.org/
- **GRAFANA:** https://grafana.com/
- **SPLUNK** (Ofrece una capacidad básica free): https://www.splunk.com/
- **LogRhythm:** https://logrhythm.com/

Herramientas de análisis de información

- **Amap:** https://www.kali.org/tools/amap/
- **cisco-torch:** https://www.kali.org/tools/cisco-torch/
- **DMitry:** https://www.kali.org/tools/dmitry/
- **DotDotPwn:** https://www.kali.org/-tools/dotdotpwn/

Herramientas para gestión de incidentes a través de ticket

- **OTRS:** https://otrs.com/es/home/
- **JIRA:** https://www.atlassian.com/es/-software/jira
- **GLPI:** https://glpi-project.org/

B.– Analizadores online

Es una plataforma que permite analizar en línea archivos y URL sospechosas que puedan contener algún tipo de malware u otros fines ilícitos.

- **VIRUS TOTAL:** https://www.virustotal.com/es/
- **ANY.RUN:** https://any.run

C.– Análisis forense

Conjunto de técnicas y herramientas de investigación científica para extraer información de cualquier soporte sin alterar su estado. Cuando se es víctima de un ciberataque, el análisis forense recopila datos sobre el incidente en etapas: Identificar el ataque, preservar los discos, analizar la información rescatada y presentar la evidencia.

- **CAINE:** http://www.caine-live.net/
- **DEFT Linux:** http://www.deftlinux.net/
- **SIFT:** https://www.sans.org/tools/sift-workstation/

D.– Sandbox

Es una máquina virtual o entorno de prueba aislado donde ejecutar un software o código sospechoso, en base a archivos adjuntos o URL desconocidas, para observar su comportamiento, identificar el tipo de código y generar un reporte de acciones para no dañar los sistemas. También se usan para probar e implementar un software. Algunos son:

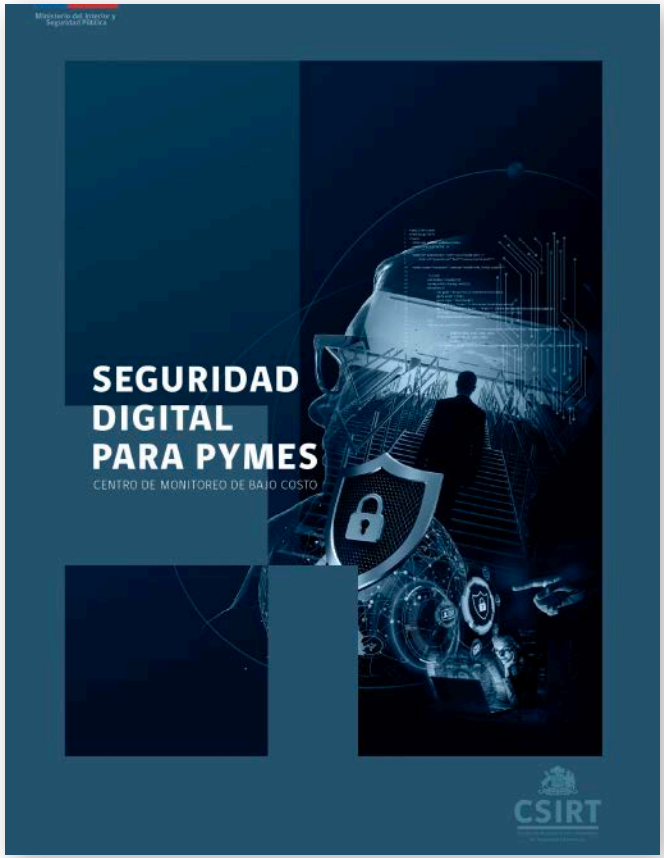
- **CUCKOO:** https://cuckoosandbox.org/
- **SANDBOXIE:** https://github.com/sandboxie/sandboxie
- **SNDBOX:** https://www.sndbox.com/

II KIT DE CONCIENTIZACIÓN

El CSIRT de Gobierno dispone de la siguiente guía escrita especialmente para ayudar a las empresas pequeñas y medianas del país:

En "Seguridad digital para pymes: Centros de monitoreo de bajo costo", Carlos Montoya, fundador y director de Whilolab, detalla el uso de siete herramientas de código abierto (Maltrail, Suricata, Elastic-Search, Logstach, Kibana, TheHive y MISP) con el fin de proteger la confidencialidad, integridad y disponibilidad de sus activos informáticos.

Encuéntrela aquí: https://www.csirt.gob.cl/-media/2020/10/AN2-2020-18.pdf.



Asimismo, desarrollamos estos ciberconsejos, fáciles de compartir entre los funcionarios de la compañía:

—CIBERCONSEJOS— DE SEGURIDAD para Pymes

1 VULNERABILIDADES: Identifica las principales debilidades de tu negocio. Por ejemplo, cuáles son los datos más importantes de tu empresa: clientes, información financiera.

1.1 COMPUTADORES Y DISPOSITIVOS:

- Actualizar softwares, manteniendo el sistema operativo más reciente
- Utilizar siempre un antivirus actualizado
- Configurar un firewall

2 VULNERABILIDADES:

- Realizar copias de seguridad de los datos regularmente.
- Cifrar los datos confidenciales de la empresa.
- Establecer en toda la compañía contraseñas seguras.
- Proteger redes inalámbricas y los datos de los clientes.

2.2 PROTECCIÓN DE LOS DATOS:

REDES WIFI:
Si la oficina tiene una red WiFi asegúrate de que esté encriptada y oculta.

3 CAPACITAR EN CIBERSEGURIDAD:
Definir políticas y protocolos de seguridad para los trabajadores básicas y concientiza sobre los riesgos cibernéticos.

3.1 DISPOSITIVOS MÓVILES:
Si los trabajadores utilizan dispositivos móviles con información confidencial de los clientes y empresa, es necesario aplicar medidas de seguridad como:

- Usar contraseñas seguras
- Cifrar datos y establecer procedimientos de notificación de equipos perdidos o robados.

4 CUENTAS DE USUARIO PARA CADA TRABAJADOR:
Una buena medida de seguridad es que cada persona tenga su propia cuenta con una política de contraseña segura y renovación constante.

SI NECESITAS ORIENTACIÓN
comunícate con **CSIRT 24/ 7**
(+562) 2486 3850

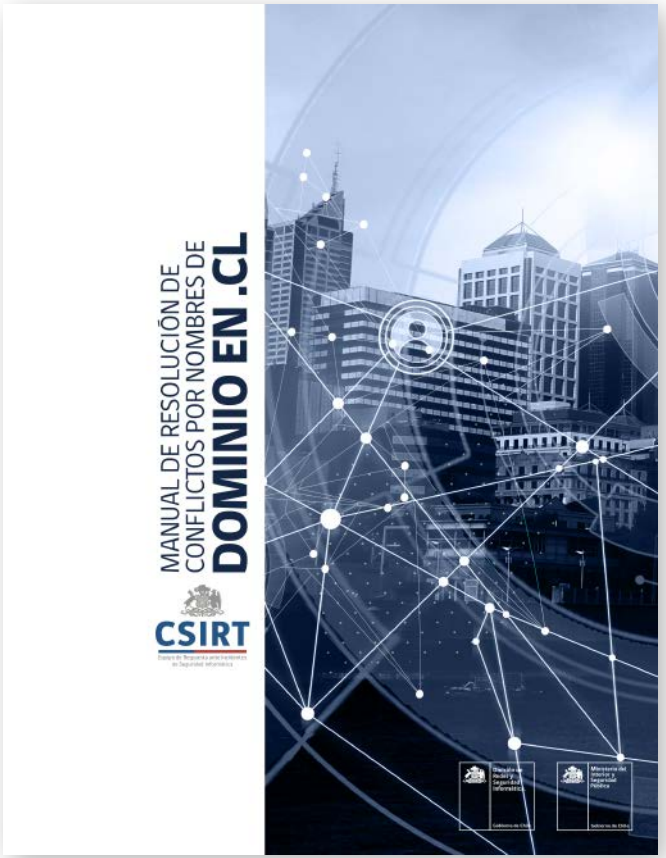
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

III KIT DE RECURSOS LEGALES

Una forma en que nuestra empresa puede verse amenazada es a través de la suplantación en internet de su imagen y nombre, con el objetivo de robar sus ventas, dañar su reputación o robar información de sus clientes.

A.– Procedimiento: Renovación de nombres de Dominios

Si nos vemos en esta situación, podemos hacer una solicitud de revocación de dominio ante NIC Chile, entidad que administra los dominios .cl. Los pasos para realizar estas solicitudes de revocación se detallan en la siguiente guía:
https://www.csirt.gob.cl/media/2020/04/Manual-Resolucion-nombres-de-dominio.pdf



B.– Políticas: De Seguridad de la Información:

Varias de las mejores prácticas en ciberseguridad pueden implementarse a través de políticas, procedimientos que describen cómo materializar estas prácticas en cuanto a procesos, responsables, herramientas e indicadores de su eficiencia y eficacia.

Pueden encontrar las políticas de seguridad de la información que hemos elaborado, aquí:
csirt.gob.cl/matrices-de-politicas.

- **Política General de Seguridad de la Información:** csirt.gob.cl/media/2021/05/PG-SGSI-001.docx
- **Política de Organización de la Seguridad de Información:** csirt.gob.cl/media/2021/05/PE-SGSI-001.docx
- **Política de uso de activos de información:** csirt.gob.cl/media/2021/05/PE-SGSI-002.docx
- **Política de seguridad ligada a los recursos humanos:** csirt.gob.cl/media/2021/05/PE-SGSI-003.docx
- **Política de Seguridad Física y del Ambiente:** csirt.gob.cl/media/2021/05/PE-SGSI-004.docx
- **Política de Gestión de Comunicaciones y Operaciones:** csirt.gob.cl/media/2021/05/PE-SGSI-005.docx
- **Política de Control de Acceso:** https://www.csirt.gob.cl/media/2021/05/PE-SGSI-006.docx
- **Política de Proceso de Desarrollo de Software:** csirt.gob.cl/media/2021/05/PE-SGSI-007.docx
- **Política de Gestión de Incidentes de Seguridad de la Información:** csirt.gob.cl/media/2021/05/PE-SGSI-008.docx
- **Política sobre el Uso del Correo Electrónico:** csirt.gob.cl/media/2021/05/PE-SGSI-009.docx
- **Política de planificación de la continuidad de la seguridad de la información:** csirt.gob.cl/media/2021/05/-PE-SGSI-010.docx
- **Política de trabajo a distancia y teletrabajo:** csirt.gob.cl/media/2021/05/PE-SGSI-011.docx

D.– Controles:

El CSIRT de Gobierno también ha elaborado Fichas de Control Normativo, para ilustrar sobre los diferentes controles normativos que son prioritarios para todo Sistema de Gestión de Seguridad de la Información. Estas directrices no reemplazan el análisis de riesgo institucional, pero permiten identificar instrumentos, herramientas y desarrollos que mejoran la postura de ciberseguridad institucional.

Al cierre de esta guía, contamos con los siguientes controles, a los que se seguirán sumando otros cada semana en: https://www.csirt.gob.cl/estadisticas.

No. 1 Política de Seguridad de la Información: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-1-politica-de-seguridad-de-la-informacion/
No. 2 Organización de la Seguridad de la Información: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-2-organizacion-de-la-seguridad-de-la-informacion/
No. 3 Concientización, Educación y Formación en Seguridad de la Información: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-3/
No. 4 Inventarios de Activos: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-4
No. 5 Política de Control de Acceso: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-5
No. 6 Políticas de Acceso a las Redes y a los Rervicios de la Red: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-6/
No. 7 Sistema de Gestión de Contraseñas: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-7/
No. 8 Perímetro de Seguridad Física: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-8/
No. 9 Protección contra Amenazas Externas y del Ambiente: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-9/
No. 10 Controles contra Códigos Maliciosos: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-10/
No. 11 Respaldo de la Información: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-11/
No. 12 Registro de Eventos: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-12/
No. 13 Registros del Administrador y el Operador: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-13/
No. 14 Sincronización de Relojes: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-14/
No. 15 Instalación de Software en Sistemas Operacionales: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-15/
No. 16 Gestión de las Vulnerabilidades Técnicas: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-16/

KIT DE APOYO TÉCNICO
ECONÓMICOS GUBERNAMENTAL

El Gobierno se encuentra permanentemente formulando y desarrollando diferentes instrumentos que van en apoyo de las pymes en diversos ámbitos. Algunos de estos instrumentos son:

SERNAC/CSIRT

A través del portal web del CSIRT de Gobierno se pueden verificar las URL de sitios web que se hayan registrado ante el SERNAC como puntos de comercio electrónico confiables.
URL: https://www.csirt.gob.cl

CORFO

Postulación AOI-Administración PFC "Programa de Formación para la Seguridad de la Información y la Ciberseguridad"
URL: https://www.corfo.cl/sites/cpp/convocatorias/aoi_admin_pfc_ciberseguridad

Becas Capital Humano, para formación en Tecnologías de la Información y Comercio Electrónico, entre otros temas relevantes para pymes.
URL: https://www.corfo.cl/sites/becascapitalhumano/home

Curso en coordinación con universidades:
URL: https://www.corfo.cl/sites/Satellite?c=C_NoticiaNacional&cid=1476723858849&d=Touch&pagename=CorfoPortalPublico%2FC_NoticiaNacional%2FcorfoDetalleNoticiaNacionalWeb

Cursos en línea para pymes a través de la plataforma Pymes en Línea:
URL: https://pymesenlinea.cl/

El CSIRT de Gobierno genera regularmente material de divulgación sobre ciberseguridad en diferentes formatos para dar cabida a estas complejas materias en un lenguaje más cotidiano y desde distintas ópticas organizacionales. Para mantenerse al tanto de nuestras más recientes publicaciones, les recomendamos seguir a nuestra institución en sus redes sociales:

- **Twitter:** https://twitter.com/CSIRTGOB
- **LinkedIn:** https://www.linkedin.com/company/35652602
- **Instagram:** https://www.instagram.com/csirtgobcl/.

Es así como el CSIRT de Gobierno dispone para la comunidad regularmente de nuevas:

- **Recomendaciones y Ciberconsejos:** (https://www.csirt.gob.cl/recomendaciones/).
- **Alertas:** (https://www.csirt.gob.cl/alertas/).
- **Vulnerabilidades:** (https://www.csirt.gob.cl/vulnerabilidades/).
- **Herramientas:** (https://www.csirt.gob.cl/sistemas-y-herramientas/).
- **Comandos y controles:** (https://www.csirt.gob.cl/estadisticas/).
- **Revistas CiberSucesos y Ciberguías**: https://www.csirt.gob.cl/recomendaciones/

Ministerio del Interior y Seguridad Pública

En el Mes de la Ciberseguridad **2021**

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBEGUIA PARA LAS PYMES

Director: Carlos Landeros Cartes

Jefa de contenidos y edición: Katherina Canales Madrid

Colaboradores equipo CSIRT: Carolina Covarrubias
Ramón Rivera
Hernán Espinoza

Diseño y diagramación: Jaime Millán

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

Teatinos 92 piso 6
Santiago, Chile