

Tabla de Contenido

Introducción	1
1. La Internet	1
1.1. Capa de Red y Protocolo de Internet (IP)	2
1.2. Capa de Transporte y protocolos TCP y UDP	5
1.3. Capa de Aplicación	8
2. Estrategias para el uso de datos de escaneo de la red chilena	13
2.1. Estructura del trabajo	13
2.2. Hipótesis	15
2.3. Objetivo General	15
2.4. Objetivos Específicos	15
2.5. Contribuciones	15
1. Antecedentes	17
1.1. Medición de Internet para Monitoreo de Seguridad computacional	17
1.1.1. Mediciones Activas y Pasivas	18
1.1.2. Técnicas Generales de Medición en Seguridad	19
1.1.3. Técnicas Específicas de Medición en Seguridad	21
1.1.4. Uso de Mediciones en conjunto con otros datos de Seguridad	24
1.1.5. Dificultades Generales de Mediciones y Escaneos de Internet	24
1.1.6. Ámbito de la Investigación Realizada	25
1.2. Organizaciones y Software Orientados a Monitoreo de Internet	25
1.2.1. Organizaciones	25
1.2.2. Software	26
1.2.3. Ámbito de Diseño e Implementación de Software realizado	28
1.3. La “Red Chilena” en cada contexto	28
1.3.1. Según Sistemas Autónomos	28
1.3.2. Según relevancia para usuarios chilenos	30
1.3.3. Según servicios asociados a dominios .CL	30
1.3.4. Según información de proveedores externos	31
1.3.5. Definiciones a usar	32
2. Revisión Preliminar de Datos de Escaneo manejados	33
2.1. El CLCERT	33
2.1.1. Datos Manejados	33
2.2. Análisis Preliminar de Datos Manejados	35
2.2.1. Datos del CLCERT	35

2.2.2.	Datos de Censys	43
2.2.3.	Escaneo de Protocolos, Software y Versiones	46
2.2.4.	Datos de Malware Fuentes Reservadas	48
2.3.	Dificultades	56
2.3.1.	Existencia de lagunas de datos en algunos intervalos de tiempo	56
2.3.2.	Existencia de datos con alta varianza en cortos intervalos de tiempo	57
2.3.3.	Diferencias de resultados entre datos de distintas fuentes	57
2.4.	Conclusiones	61
3.	Análisis de Concentración de Servicios Dependientes del ccTLD chileno	62
3.1.	Antecedentes del estudio	62
3.1.1.	NIC Chile	63
3.1.2.	Servicios a estudiar	64
3.1.3.	Datos a utilizar y recopilar	64
3.2.	Herramientas usadas y desarrolladas	66
3.2.1.	Escaneo usando ZMap y Mercury	66
3.2.2.	Importación a OSR	66
3.2.3.	Procesamiento de datos	67
3.3.	Análisis de datos recopilados	67
3.3.1.	Análisis sobre todos los dominios chilenos	68
3.3.2.	Análisis de FQDNs Gubernamentales	77
3.4.	Consideraciones	78
3.4.1.	Recomendaciones	78
3.4.2.	Limitaciones	79
3.4.3.	Trabajo Futuro	80
3.4.4.	Conclusiones	81
4.	Estrategias de análisis de datos de Escaneo usando múltiples fuentes	83
4.1.	Antecedentes	83
4.1.1.	Motivación	83
4.1.2.	Red Chilena en este contexto	84
4.1.3.	Estrategias Propuestas	84
4.2.	Comparación histórica de datos de escaneo de protocolos	86
4.2.1.	Datos históricos del CLCERT	86
4.2.2.	Datos Históricos de Censys	92
4.2.3.	Conclusiones de Estrategia	92
4.3.	Comparación de datos de escaneo de protocolos de múltiples proveedores	93
4.3.1.	Comparación entre ambas fuentes	93
4.3.2.	Uso de Tercera Fuente	94
4.3.3.	Conclusiones de Estrategia	97
4.4.	Uso de datos de abandono en estimación de máquinas vulnerables	98
4.4.1.	Definición de Abandono	98
4.4.2.	Abandono por Certificados	99
4.4.3.	Abandono por Software Obsoleto	102
4.4.4.	Conclusiones de Estrategia	112
4.5.	Conclusiones	112
4.5.1.	Limitaciones del trabajo	112

4.5.2.	Trabajo Futuro	116
4.5.3.	Conclusiones	117
5.	OSR: Un Observatorio de Seguridad para la Red Chilena	119
5.1.	El Sistema Actual	119
5.1.1.	Infraestructura y Procesos	120
5.1.2.	Problemas	121
5.2.	Diseño del nuevo sistema	122
5.2.1.	Requisitos	123
5.2.2.	Decisiones de Diseño	124
5.2.3.	Limitaciones	126
5.3.	Implementación del Nuevo Sistema	127
5.4.	Funcionamiento del nuevo sistema	127
5.4.1.	Máquina Principal	127
5.4.2.	Archivos de Configuración	127
5.4.3.	Rendimiento	129
5.5.	Trabajo Futuro	131
5.5.1.	Nuevos procesos	131
5.5.2.	Nuevas entradas y salidas	131
5.5.3.	Scheduler interno de tareas	132
5.5.4.	Sitio Web con Datos Agregados	132
5.6.	Conclusiones	132
	Conclusión	133
	Bibliografía	141
	Anexos	141
	Anexo A. Análisis de ccTLD sobre dominios de gobierno	141
A.1.	Distribución de dominios gubernamentales	141
A.2.	Concentración de dominios gubernamentales	142
A.3.	Uso en dominios gubernamentales de Proveedores Conocidos	147
A.4.	Infraestructura compartidas en dominios gubernamentales	147
A.5.	Consideraciones sobre dominios gubernamentales	148
	Anexo B. Detalles de Implementación del Sistema OSR	149
B.1.	Herramientas a utilizar	149
B.2.	Módulos implementados	149
B.2.1.	Comandos	150
B.2.2.	Conexiones Remotas	151
B.2.3.	Consultas SQL	151
B.2.4.	Notificaciones	152
B.2.5.	Modelo de datos	152
B.2.6.	Tareas	154
B.2.7.	Procesos	155
B.2.8.	Entradas	157
B.2.9.	Salidas	158

Anexo C. Validación histórica de datos de escaneo de protocolos de Censys	159
C.1. Datos históricos de Censys	159
C.1.1. Análisis global de IPs encontradas	159
C.1.2. Continuidad de las IPs por protocolo	160