CSIRT - Supertel

Centro de Respuesta a Incidentes Informáticos - EcuCERT

Presentado por **Marco Rivadeneira Fuentes**
Oficial de seguridad

Quito - Ecuador

Para empezar

La ciencia es un esfuerzo de colaboración. Los resultados combinados de varias personas que trabajan juntas es a menudo mucho más eficaz de lo que podría ser el de un científico que trabaja solo.

- Jhon Bardeen

AGENDA

1. Implementación del EcuCERT
2. Interacción del EcuCERT
3. Casos de Éxito

¿Cómo nace el EcuCERT?

Aparecen nuevas formas de **fraude**, **extorsión** y fomento de **delitos electrónicos**

CYBERCRIMEN

El Estado debe estar **preparado** **para responder de manera rápida, segura y eficiente**

¿Cómo nace el EcuCERT?

SOLUCIÓN: Crear un **grupo especializado**

SUPERTEL
SUPERINTENDENCIA DE TELECOMUNICACIONES

Nacional

Implementación

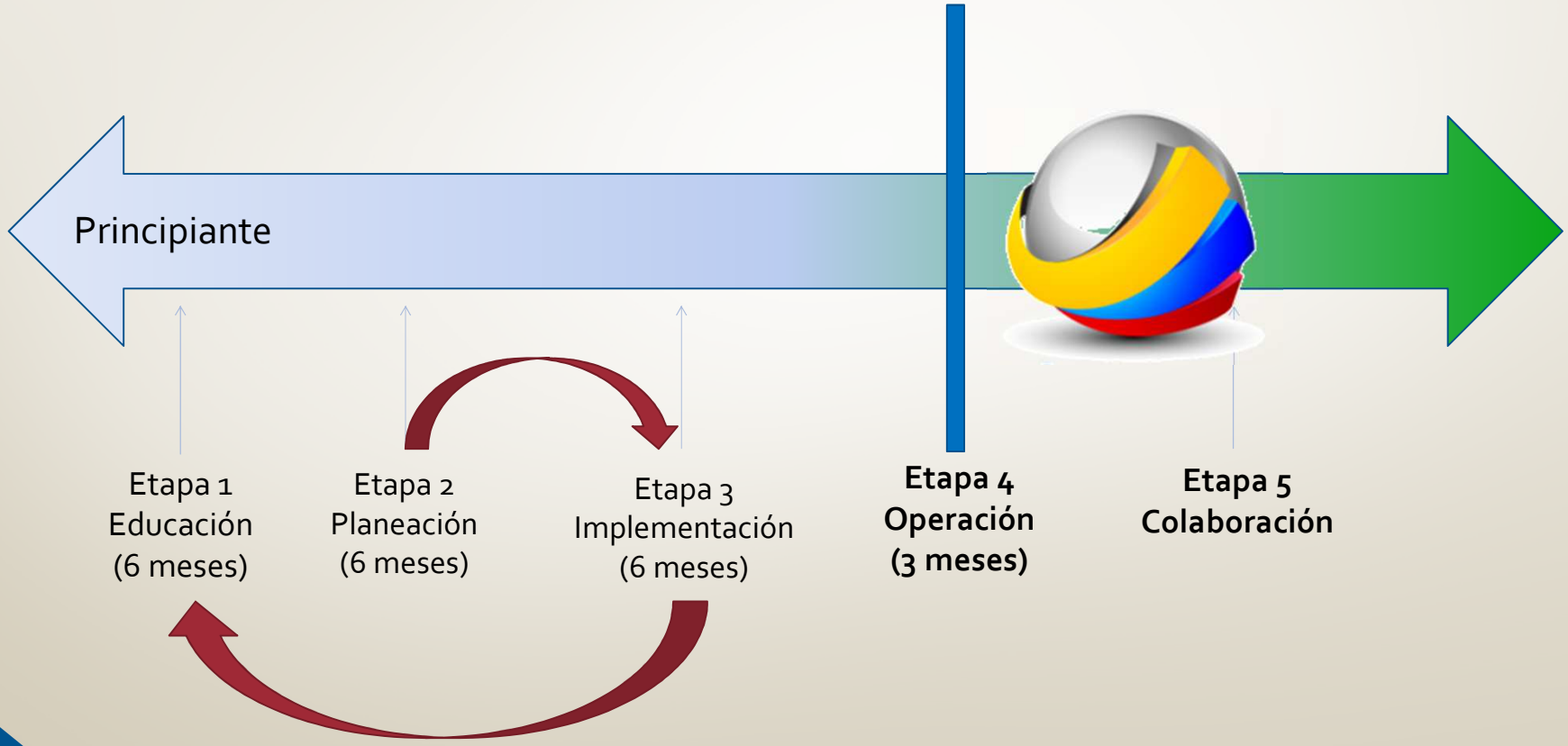
SUPERTEL
SUPERINTENDENCIA DE TELECOMUNICACIONES

La SUPERTEL tiene como objetivo, velar porque los usuarios reciban **servicios** de telecomunicaciones **legales, lícitos** y de calidad, además es el organismo encargado de **controlar** estos servicios.

Es prohibido usar los medios de telecomunicación contra la **seguridad** del **Estado**, el orden público, la moral y las buenas costumbres.

El Estado garantiza el derecho al **secreto** y a la **privacidad** de las telecomunicaciones.

Etapas de desarrollo



El EcuCERT

"Brindar a su Comunidad Objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico"

Comunidad Objetivo

1

SUPERTEL
SUPERINTENDENCIA DE TELECOMUNICACIONES

2

3

Ministerio
de Relaciones Exteriores,
Comercio e Integración

Ministerio
de Educación

Ministerio
de Turismo

Comunidad Objetivo

Estadísticas de Telecomunicaciones

2 millones líneas fijas
15’2 millones líneas
10´4 milliones de usuarios

6 operadores
3 operadores móviles
234 ISP

Dominios

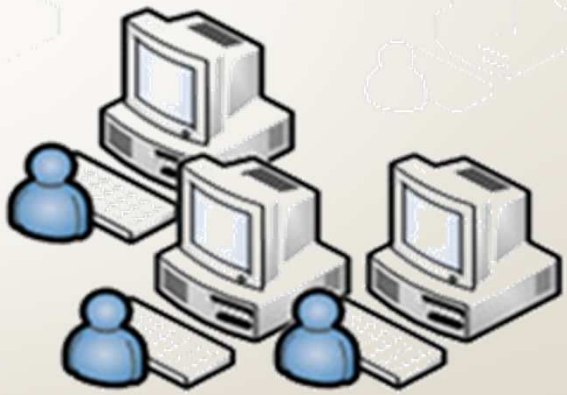
Uso general	.ec	clubsuizo.ec
Gobierno	.gob.ec	supertel.gob.ec
Comercial	.com.ec	greenetics.com.ec

Etapa de Operación

1. Infraestructura
2. Políticas y procedimientos
3. Personal (modelo organizacional)

Infraestructura

1. **Data Center** - Seguridades físicas y lógicas
2. Centro de **Monitoreo**
3. Laboratorio de **Pruebas**
4. Laboratorio **forense**
5. Herramientas de **hardware y software**
6. **Centro Alterno** de investigación y Capacitación



Infraestructura

Reporte

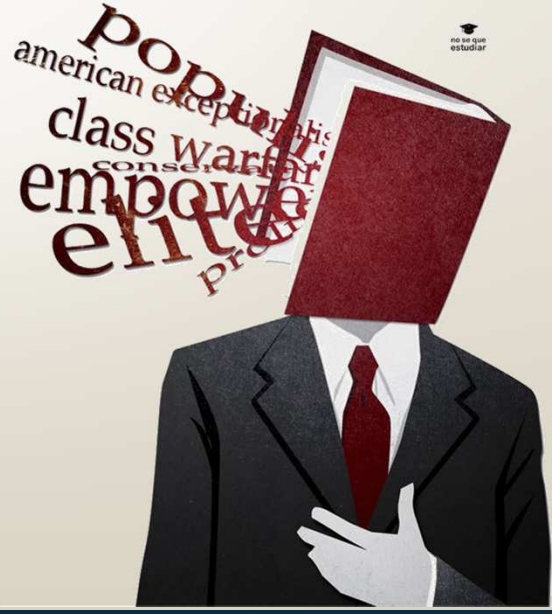
Alertas

Contácto

Comunicados

Políticas y procedimientos

- Clasificación
- Protección
- Conservación y Respaldo
- Destrucción
- Difusión
- Acceso



- Uso apropiado de los Sistemas
- Definición, Priorización y Asignación de Incidentes
- Gestión de Incidentes
- Cooperación con Otros Equipos de Respuesta

Modelo Organizacional

Coordinación

- Gestión de incidentes de seguridad
- Búsqueda de vulnerabilidades y laboratorio Forense
- Avisos proactivos y reactivo
- Desarrollo de aplicaciones e Investigación
- Capacitación, entrenamiento y sensibilización

AGENDA

1. Implementación del EcuCERT
2. Interacción del EcuCERT
3. Casos de Éxito

Interacción del EcuCERT

Computer Emergency Response Team

- CERT/CC **primer CERT creado en el mundo**, (CERT de la Universidad Carneggie Mellon), y que actualmente engloba a más de **67 equipos** de respuesta a incidentes de seguridad del ámbito gubernamental.

EcuCERT como CSIRT Nacional

Interacción del EcuCERT

Forum of Incident Response and Security Teams

- Organización internacional que engloba y acredita a más de **270 equipos** de respuesta a incidentes de seguridad del **ámbito gubernamental, empresarial y académico**

Interacción del EcuCERT

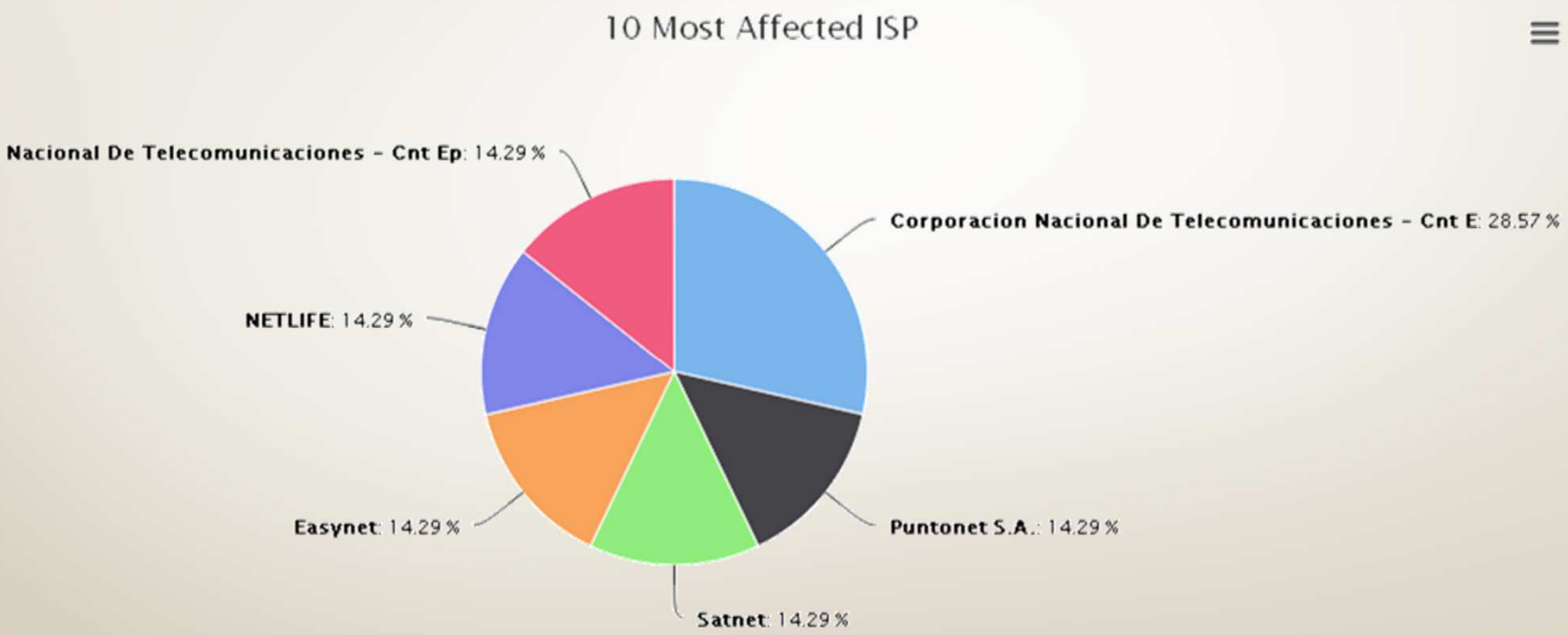
Interacción del EcuCERT

Unión Internacional de Telecomunicaciones

Es el organismo especializado de las **Naciones Unidas** para las **tecnologías de la información y la comunicación – TIC.**

Con quienes trabajamos?

Mayor número de afectaciones Ec



HORNET


IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS
Home
About Us
Services
Countries
Partners
Resource Centre
NEWS ALERT: FACEBOOK NUMBER ONE SOCIAL NETWORK FOR PHISHING ATTACKS
ITU
150 NATIONS
HAVE JOINED THE COALITION.
ITU-IMPACT IS TODAY, THE LARGEST GLOBAL CYBERSECURITY ALLIANCE

AGENDA

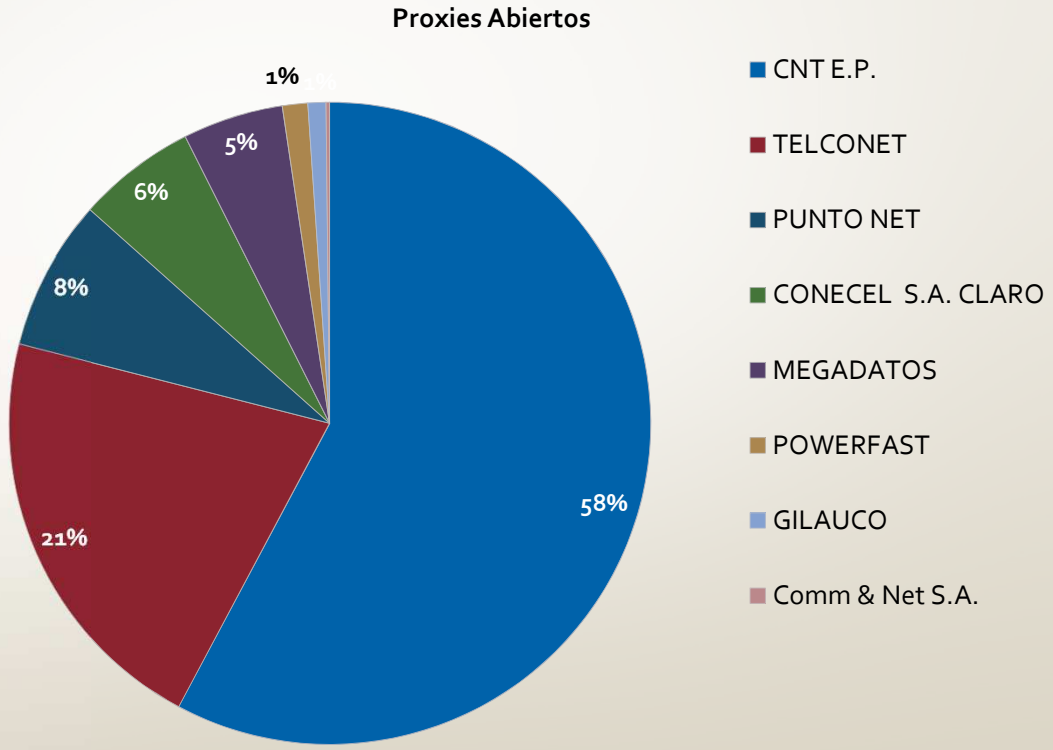
1. Implementación del EcuCERT
2. Interacción del EcuCERT
3. Casos de Éxito

PROXIES ABIERTOS

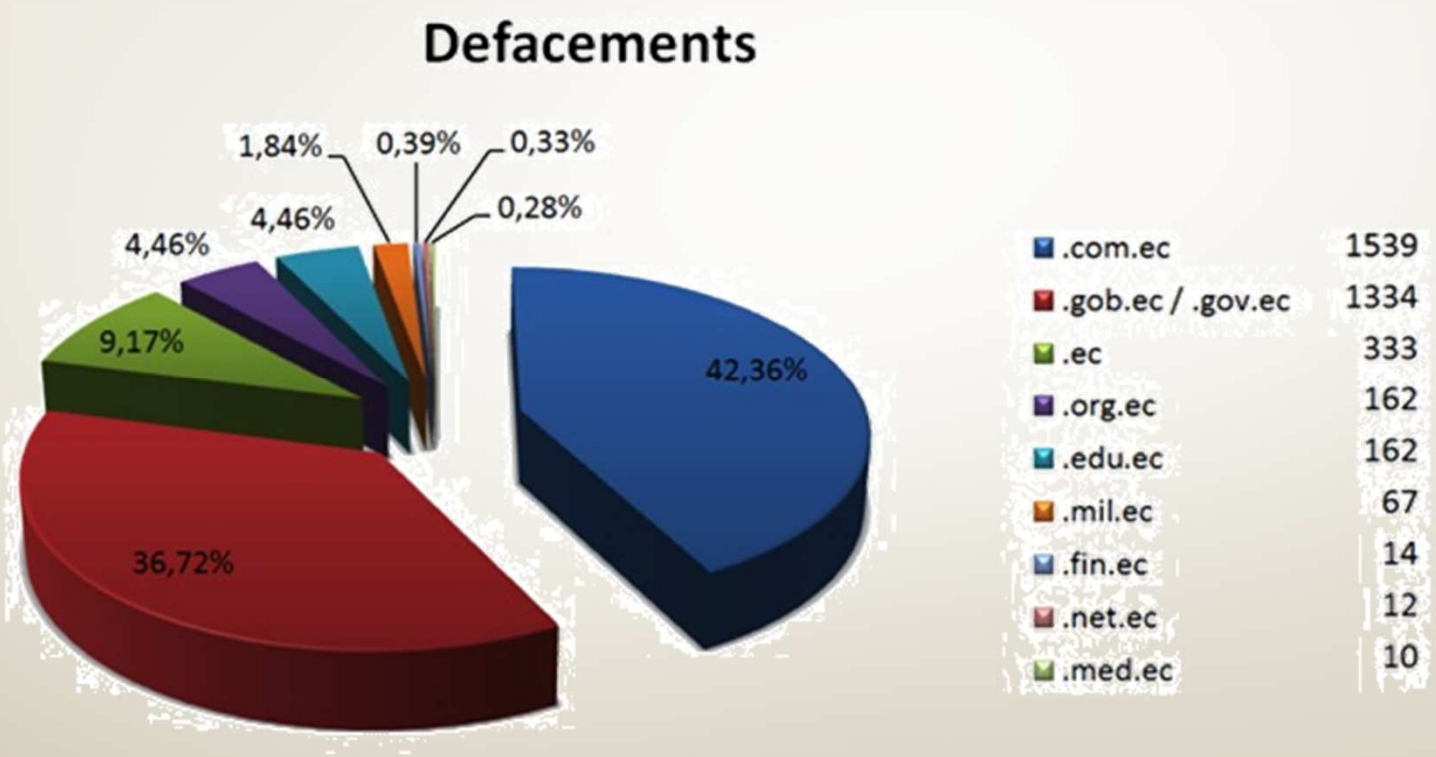
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

SISTEMAS DETECTADOS COMO PROXIES ABIERTOS RELACIONADOS A PORTADORES E ISP DENTRO DEL TERRITORIO ECUATORIANO.		
No.	Portador/ISP	Proxies Abiertos
1	COMM&NET S.A. / RED ACCESS	1
2	CNT E.P.	319
3	CONECEL S.A. CLARO	33
4	GILAUCO S.A. GILAUCO	5
5	MEGADATOS	28
6	CORPORACION POWERFAST POWERFAST	7
7	PUNTO NET S.A. / PUNTO NET	42
8	TELCONETS.A. / TELCONET	117

Total	552



Desfiguraciones WEB



Delitos Registrados

CSIRT Nacional

Ecucert - Supertel

Enero 2014 – septiembre 2014

DECODIFICADORES ILíCITOS

- En cooperación con la Corporación Nacional de Telecomunicaciones y proveedores de internet privados se bloqueo dominios de red para evitar su funcionamiento.
- Más de 5000 usuarios ilegales fuera de línea.

Delitos Registrados

CSIRT Nacional

Ecucert - Supertel

Enero 2014 – septiembre 2014

FRAUDE IPPBX

- 33 casos registrados
- Empresas (Empresas privadas, Servicios petroleros, IESS, Cancillería)
- Fraude económico (30.000$)
- Destinos atípicos (Guinea, Ghana, Austria, Gambia)
- El Ecucert junto con CNT investiga los casos de fraude IPPBX

Delitos Registrados

CSIRT Nacional

Ecucert - Supertel

Enero 2014 – septiembre 2014

Phishing

- 89 casos registrados
- Servidores infectados que sirven para robar datos.
- Suplantación de identidad de bancos, cooperativas e instituciones gubernamentales.
- El Ecucert en colaboración con los afectados trabaja para dar de baja los sitios fraudulentos.

Delitos Registrados

CSIRT Nacional

Ecucert - Supertel

Enero 2014 – septiembre 2014

Suplantación de identidad y cyberacoso

- 8 casos registrados
- Afectados usuarios de facebook (Policía metropolitana del Distrito Metropolitano de Quito, Sujetos Políticos, Mauro Andino, etc)

Suplantación de identidad

- 1 casos registrado
- Afectado asesor presidencial

Honeynet

Puertos destino	Número de intentos de ataque	Servicio
445	10267	Microsoft Active Directory, Compartición en Windows
38997	919	Sin un servicio especifico
23	788	Telnet
1433	641	Sistema de Administración de Microsoft SQL Server
22	502	Secure Shell (SSH)
5060	360	SIP (Session Initiation Protocol)
4899	285	Herramienta de Administración Remota RADMIN
3389	278	Microsoft Terminal Server
5900	263	Virtual Network Computing (VNC), Protocolo de Escritorio Remoto
80	243	HTTP

AGENDA

1. Implementación del EcuCERT
2. Interacción del EcuCERT
3. Casos de Éxito

GRACIAS

LA UNIÓN HACE LA FUERZA