



ArCERT

Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Argentina

***Oficina Nacional de Tecnologías de Información
Subsecretaría de Tecnología de Gestión***

***Ing. Lorena B. Ferreyro
Ing. Marcela I. Pallero***

Montevideo - República Oriental del Uruguay

- Noviembre de 2008 -

Temario

- ❑ CSIRTs
- ❑ ArCERT
 - Constitución
 - Objetivos y actividades
 - Productos y servicios
 - Respuesta a incidentes
 - Otras acciones
- ❑ Gestión de incidentes de seguridad

Qué es un CSIRT

Un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) es una entidad de servicios responsable de recibir, revisar y responder a actividades o reportes vinculados a incidentes informáticos.

CERT/CC

CSIRT = CERT = CIRC = IRT = SERT = IRC

Qué es un incidente de seguridad informática

Cualquier evento adverso, real o potencial, vinculado a la seguridad de los sistemas informáticos o a las redes de computadoras.

El acto de violar una política de seguridad explícita o implícita.

CERT/CC

Por qué son necesarios los CERTs

- Todas las organizaciones sufren incidentes de seguridad
- La velocidad de la respuesta limita el daño y baja los costos de la recuperación
- Se necesitan recursos especializados
- Colaboran con tareas preventivas (alertas) y correctivas (restablecimiento del servicio)
- Se vinculan con equipos de similar naturaleza

Coordinación de **E**mergencias en **R**edes
Teleinformáticas de la Administración
Pública **Ar**gentina

Argentina - **C**omputer **E**mergency
Response **T**eam

ArCERT - Principales características

CREADO

Julio de 1999

MARCO LEGAL

Resolución N° 81/1999

Aprueba creación y establece funciones

Disposición N° 01/1999

Aprueba Reglamento de Operación

Decreto N° 1028/2003

Acciones de la ONTI en materia de seguridad informática

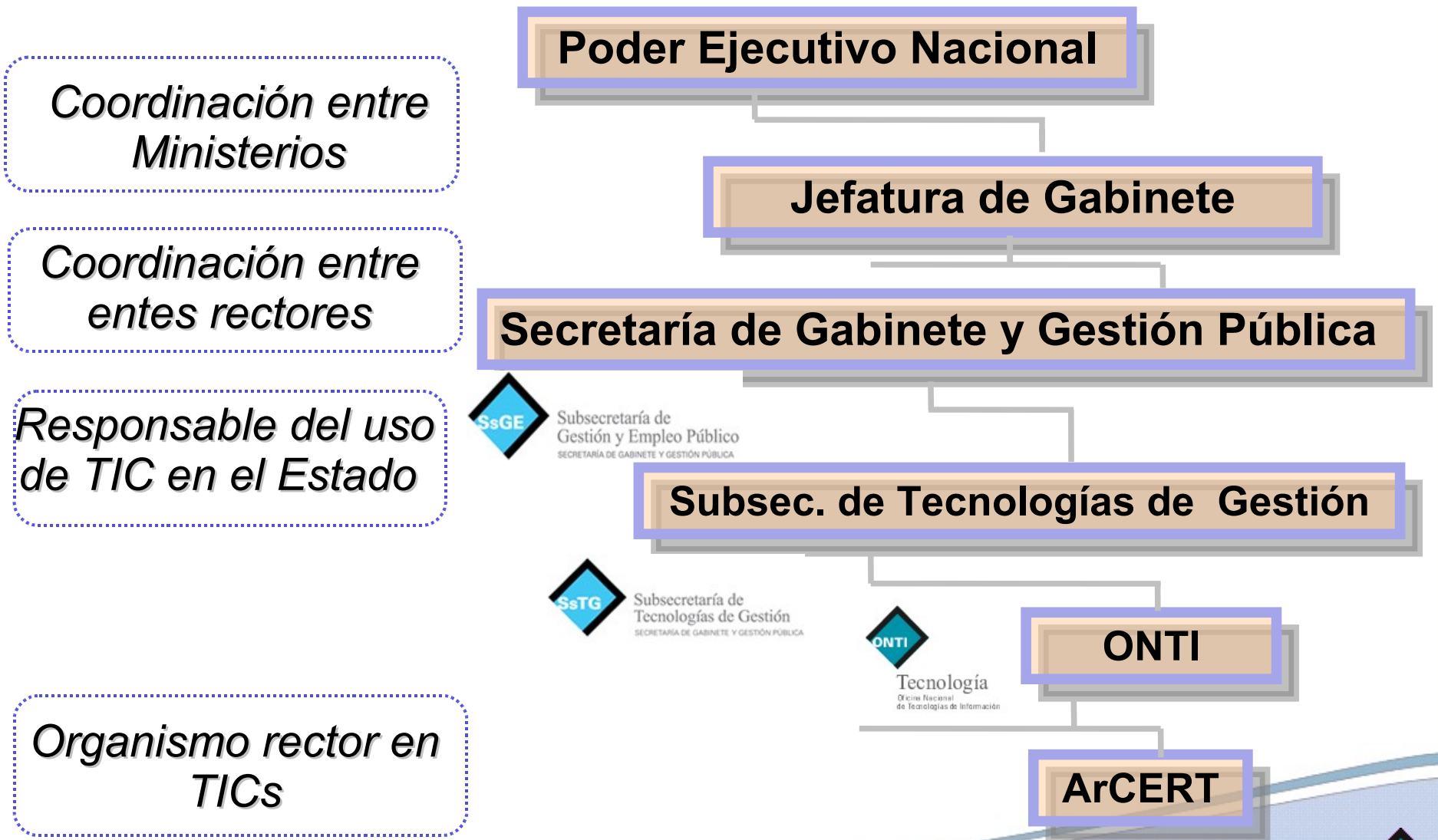
Decreto N° 21/2007

Acciones de la SSTG en materia de seguridad informática

AMBITO

Organismos Públicos

ArCERT– Dependendencia orgánica



Coordinación entre Ministerios

Coordinación entre entes rectores

Responsable del uso de TIC en el Estado

Organismo rector en TICs

ArCERT - Principales Objetivos

OBJETIVO PRINCIPAL

Incrementar los niveles de Seguridad Informática del Sector Público

OBJETIVOS ESPECIFICOS

Atención de Incidentes de Seguridad

Actividades Preventivas

- Concientización
- Capacitación
- Difusión de Alertas e Información
- Políticas de Seguridad de la Información

Servicios

Acciones de Cooperación Interna

ENTIDADES PÚBLICAS

- Organismos Nacionales y Provinciales
- Poder Judicial
- Poder Legislativo

ENTIDADES PRIVADAS

- Cámaras
- Bancos e ISPs
- Público en General
- Empresas del sector TIC

SECTOR ACADÉMICO

- Universidades Nacionales

Acciones de Cooperación Internacional

- Membresía en el FIRST desde 2004
Sede del primer Coloquio Técnico en Latinoamérica (2005)
- Participación en la Iniciativa de la OEA para la construcción de una red hemisférica de CSIRTs
- Participación en reuniones de CSIRTs con responsabilidad nacional
- Interacción con CSIRTs de la región
 - COLARIS [2005, 2006, 2007,2008]
 - Curso para la formación de CSIRTs en áreas de gobierno de Latinoamérica (BA-2005, Rio-2006)
- Designación de Expertos en iniciativa de la ITU



Marco Normativo Nacional

- Política de Seguridad de la Información para el Sector Público
 - Decisión Administrativa 669/2004
 - Modelo de Política de Seguridad de la Información

The screenshot displays the ArCERT website interface. At the top, the ArCERT logo is on the left, and the SSTG logo and 'Tecnología y Gestión' text are on the right. Below the header is a navigation menu with categories like 'Inicio', 'Política de Seguridad', 'Modelo de la Política', 'Preguntas más Frecuentes', and 'Más Información'. The main content area features a large banner with the text 'Descargue el Modelo de Política de Seguridad de la Información' and an 'APROBADO POR DISPOSICIÓN ONTI 006/2005' stamp. Below the banner, there is a 'Bienvenido' section with introductory text and a list of actions. To the right of the text is a triangular diagram representing the 'Seguridad de la Información' model, with vertices labeled 'Confidencialidad', 'Integridad', and 'Disponibilidad', and sides labeled 'Legalidad', 'Autenticidad', and 'No Repudio'. The diagram also includes 'Protección a la Duplicación' and 'Confidencialidad' on the left side.

ArCERT Coordinación de Emergencias en Redes Teleinformáticas

SSTG Tecnología y Gestión
Subsecretaría de Tecnología y Gestión
Secretaría de la Gestión Pública

REPÚBLICA ARGENTINA

Inicio

Política de Seguridad

- Inicio
- Actividad de la ONTI
- Decisión Administrativa
- Necesidad de definir una Política
- Beneficios de implementar una Política de Seguridad
- Por qué un estándar internacional
- Prejuicios y falsas afirmaciones

Acceso exclusivo para la Administración Pública

Modelo de la Política

- Estructura del Modelo
- Acceso al Modelo
- Sugerencias

Preguntas más Frecuentes

Más Información

- Principales amenazas
- Enlaces de interés
- Historial de novedades

Descargue el Modelo de Política de Seguridad de la Información

APROBADO POR DISPOSICIÓN ONTI 006/2005

Bienvenido

En este sitio encontrará las principales acciones que se están llevando a cabo, para la implementación de Políticas de Seguridad de la Información, en el ámbito de la Administración Pública Nacional de la República Argentina.

En este espacio podrá:

- Conocer la **reglamentación** que normaliza la definición de una Política de Seguridad de la Información en la Administración Pública Nacional.
- Acceder a la **Política de Seguridad de la Información Modelo** elaborada para el Sector Público y conocer el proceso por el cual se generó y sus principales características.
- Encontrar lineamientos generales sobre cómo abordar la redacción de la **Política de Seguridad de la Información** de su Organismo o adaptarla al nuevo Modelo.
- Conocer qué están haciendo el resto de los Organismos al respecto.

Seguridad de la Información

Legalidad, Autenticidad, Integridad, No Repudio, Disponibilidad, Confidencialidad, Protección a la Duplicación

Marco Normativo Nacional

➤ Ley de Delitos informáticos

- Ley 26.388 → modificación al Código Penal
- Sancionada el 24 de junio de 2008

➤ Convención de Budapest sobre Ciberdelito

- Suscrita el 8 de noviembre de 2001 por los miembros del Consejo de Europa, junto con Estados Unidos, Canadá, Japón, Costa Rica, México y Sudáfrica.
- Acciones en Argentina

Servicios y proyectos

- **Firewall** (basado en software de libre disp.)
- **SiMoS** - Sistema de Monitoreo de Seguridad
- **DNSar** – Análisis de Servidores y Dominios DNS
- **CAL** - Sistema de Sensores (desarrollo + piloto)
- **RAM** – Recolección y Análisis de Malware (desarrollo + piloto)
- **Lista de Seguridad** – Envío de alertas

¿QUE ES?

Sistema de monitoreo remoto de seguridad

OBJETIVO

Detectar vulnerabilidades en servidores que brinden servicios en Internet

BASADO EN

Herramientas de libre disponibilidad
Interface Web de usuario
Planificador de actividades

ACUERDOS

Autorización previa por Convenio
Compromiso de confidencialidad

Interface Web de usuario



- » Inicio
- » Equipos
- » Reportes
- » Administración
- » Salir

Ingreso de Datos de Nuevo Equipo

Completando este formulario, ud. puede solicitar el servicio para un nuevo equipo. Esta solicitud será procesada y analizada por personal de ArCERT, quienes decidirán la aceptación o no de su pedido

:: Datos del Equipo

Dirección IP o HostName (FQDN)	<input type="text"/>	Otros
Alias - Breve Nombre Descriptivo	<input type="text"/>	<input type="text"/>
Sistema Operativo	<input type="text" value="Aix"/>	<input type="text"/>

:: Datos del Análisis del Equipo

Periodicidad	<input type="radio"/> Una única vez	Opciones del Análisis	
	<input type="radio"/> Semanal - Seleccione día -		<input type="checkbox"/> Ataques de Denegación de Servicio
	<input type="radio"/> Mensual - Seleccione día -		<input type="checkbox"/> Detrás de Firewall
Horario Preferido	- Seleccione Horario -		

Ingresar Nuevo Equipo

¿QUE ES?

Sistema de análisis de servidores y dominios DNS

OBJETIVO

Detectar y alertar sobre falencias en los servidores DNS de los Organismos

Mantener una base de datos histórica con dicha información

Generar información estadística



DNSar
Sistema de Control de Configuración para Servicios DNS

Reporte del dominio: .gov.ar

Reporte generado con los datos obtenidos el día: 16 - 09 - 2006.

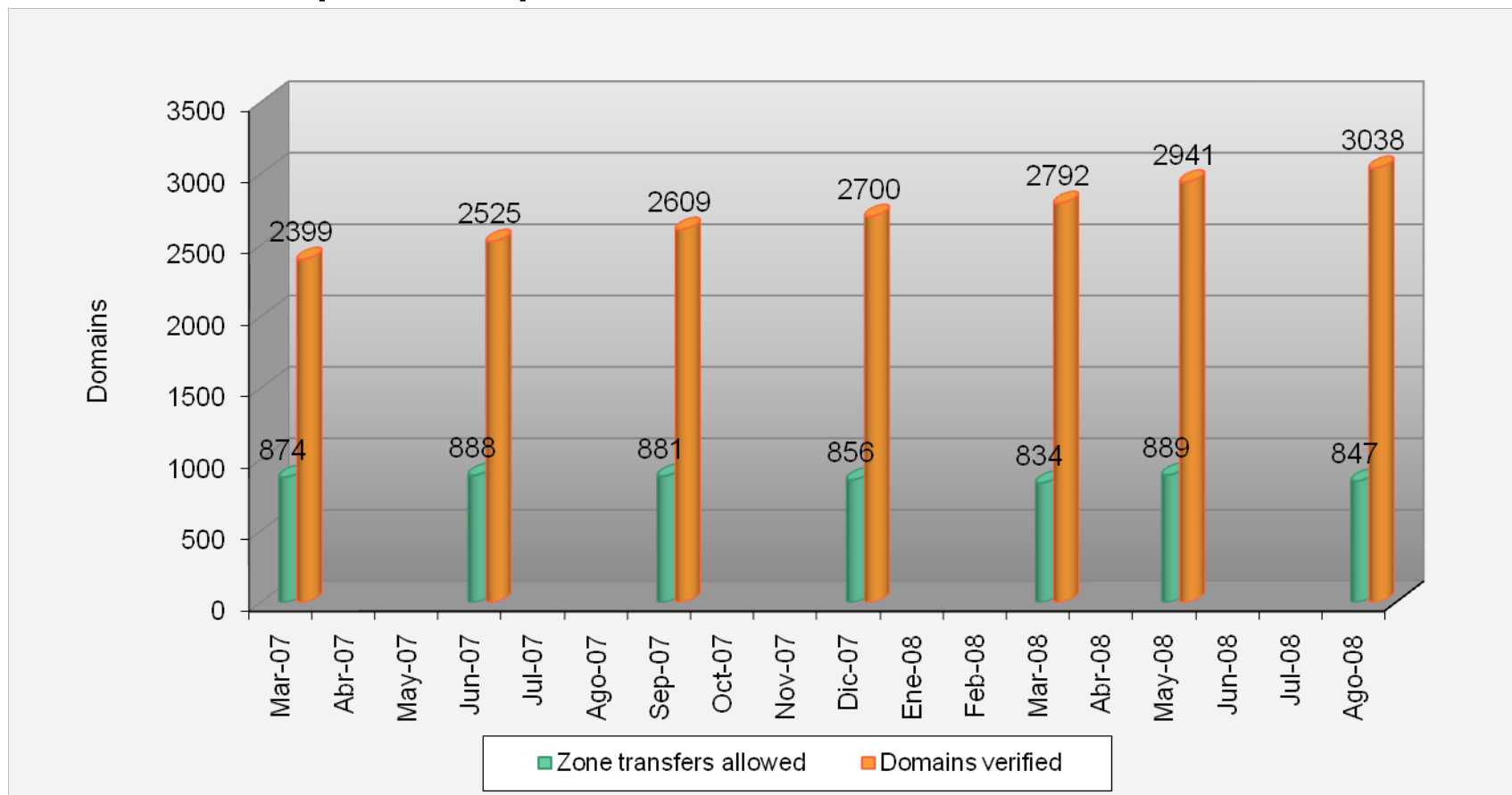
::Información general del dominio

Entidad Registrante	SECRETARÍA DE SEGURIDAD NACIONAL - MINISTERIO DE INTERIORES
Email Responsable	nsar@secreta.gov.ar
Contacto Técnico	nsar@secreta.gov.ar
Email Contacto Técnico	nsar@secreta.gov.ar

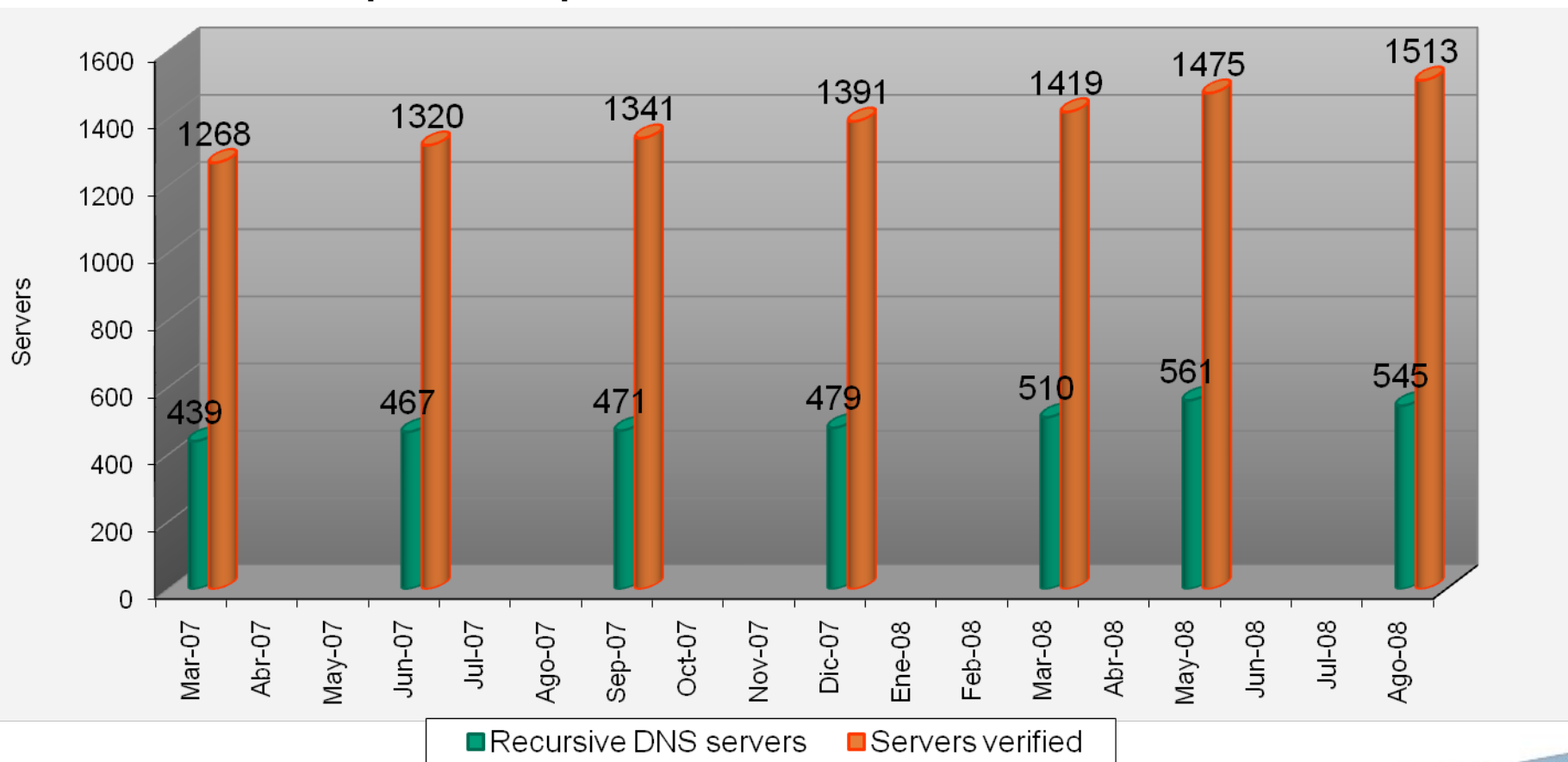
::Información de los servidores de nombres definidos en la zona padre

FQDN	IP	Estado	¿Acepta consultas recursivas?
ns3.secreta.gov.ar	200.48.18.205	No responde	No
server2.secreta.gov.ar	200.48.187.206	No responde	No
ns1.secreta.gov.ar	200.48.187.207	OK	Si
ns2.secreta.gov.ar	200.48.187.208	OK	Si

Dominios que aceptan transferencia de zona → 36%



Servidores que aceptan consultas recursivas → 28%



Reporte de Incidentes

Se reciben reportes que:

- Afecten al Sector Público o Bancario Argentino
- Estén relacionados con ataques originados desde nuestro país
- No estén vinculados con SPAM

Fuentes:

- Organismos de gobierno
- Sector bancario
- ISPs
- Ciudadanos
- Equipos de respuesta a incidentes y organizaciones afectadas a nivel mundial.
- Fuentes de información públicas y privadas
- Recolección y análisis de malware
- Herramientas de detección

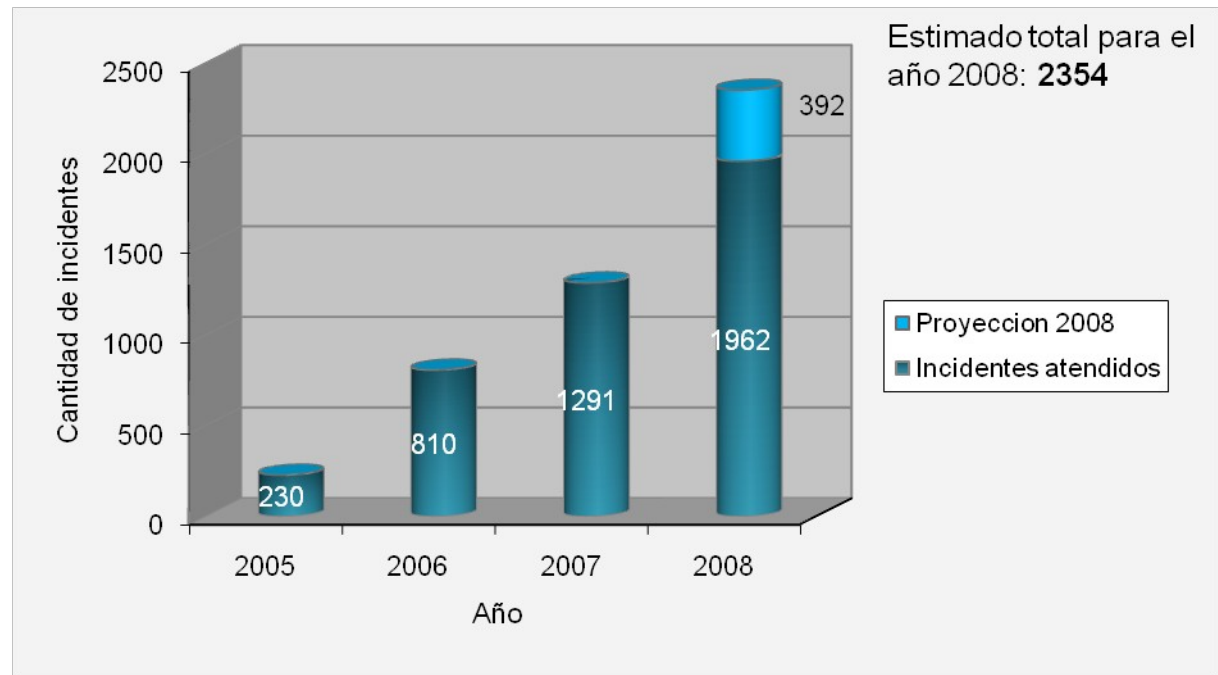
Algunos casos tratados

- Alteración de Sitios Web (Defacement)
- Phishing (engaños)
- Código malicioso (Virus, gusanos, troyanos, etc)
- Botnets y Ataques de DDoS
- Intrusiones de mayor complejidad
- Casos especiales (ej.: DNS Cache Poisoning)

Casos reportados: algunos datos

Reportes de incidentes recibidos vía email

Año	Incidentes atendidos
2005	230
2006	810
2007	1291
2008	1962



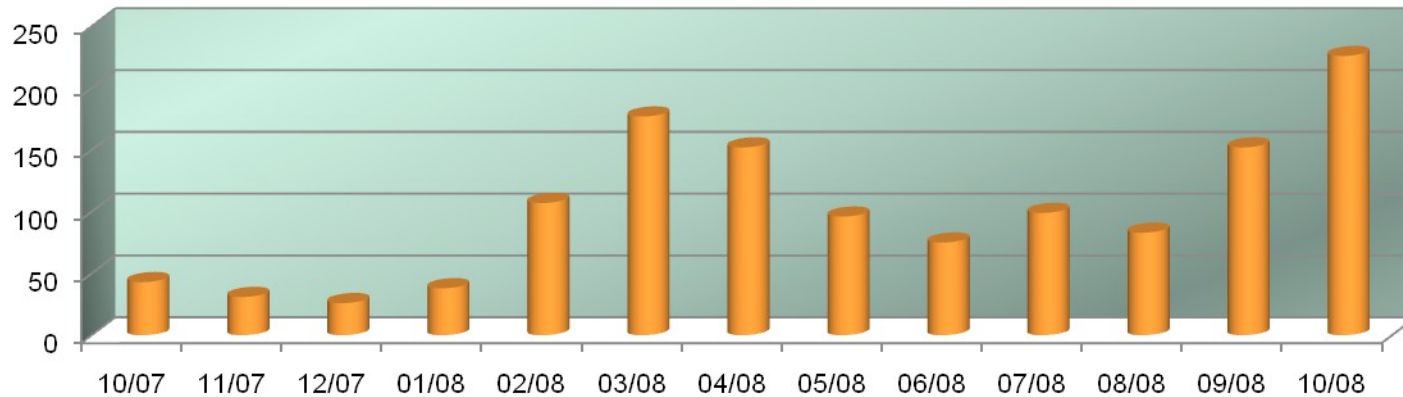
Estimado total para el año 2008: 2354

■ Proyeccion 2008
■ Incidentes atendidos

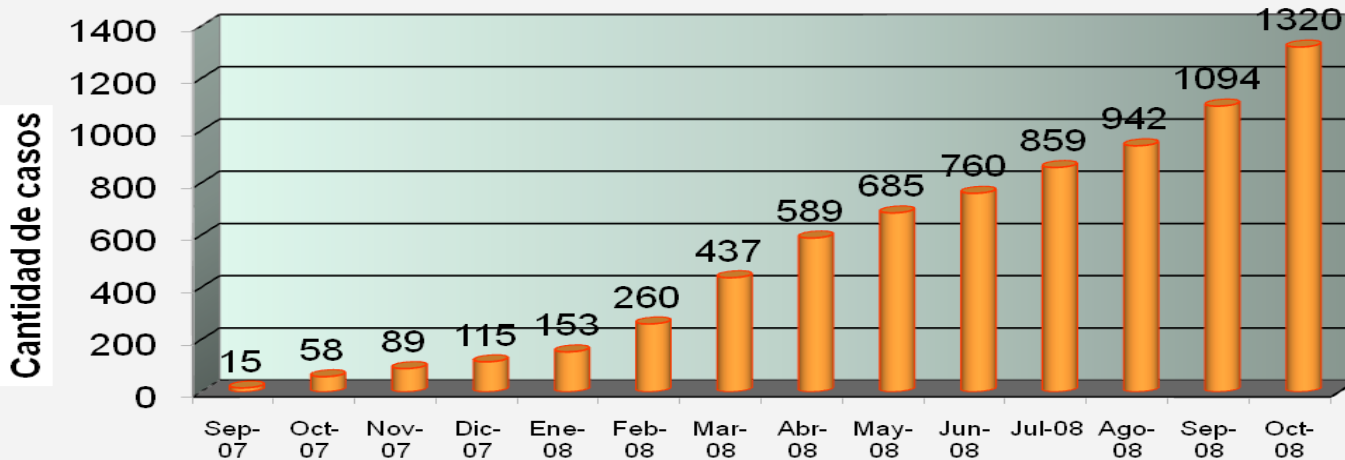
➤ A la fecha superamos en un 35% la cantidad de incidentes reportados en 2007

Phishing: algunos datos

Phishing mens.



Cantidad de casos mensuales

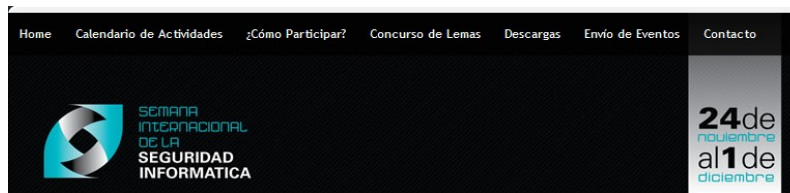


Cantidad de casos acumulados

Capacitación y concientización

- Generación y traducción de Alertas y Documentos.
- Dictado de cursos de Formación, Capacitación y Concientización.
- Publicación y difusión de información en el sitio web y en la Lista de Seguridad.
- Organización y participación en eventos y charlas.
- Participación en programas de radio y televisión.
- Jornada de Seguridad – julio de 2008.
- Video de concientización en desarrollo

“Semana de la Seguridad Informática”

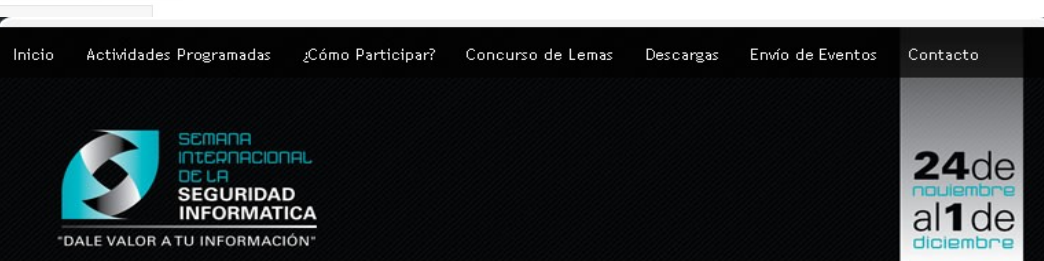


OCT 8 ¡Bienvenidos!

En el año 1988, la Association for Computing Machinery (ACM) declaró al 30 de Noviembre como el “Día Internacional de la Seguridad Informática”, con el objetivo de concientizar respecto de las amenazas que atentan contra la seguridad de la información.

La explosión que en los últimos años han experimentado las redes informáticas, fundamentalmente Internet, es el factor fundamental que ha hecho que la Seguridad Informática cobre vital importancia. Si bien Internet nos proporciona una gran cantidad de información, nuevos servicios y facilidades, también acarrea una serie de nuevos tipos de ataques y amenazas a la seguridad de la información. De hecho, conectarnos a Internet sin las debidas precauciones puede convertirnos en un blanco fácil de estos ataques. Del mismo modo, las organizaciones también pueden encontrarse expuestas a una serie de riesgos derivados de la protección inadecuada de su información y de sus sistemas.

Acceptando ser simplistas, podríamos decir que la Seguridad Informática consiste en un conjunto de procesos cuyo objetivo es minimizar los riesgos a los cuales se



Pró
event

Documentos de Interés

Recomendaciones de ArCert

- Recomendaciones para evitar ser víctima del “phishing”.
- Recomendaciones para el uso seguro del correo electrónico en los organismos de la Administración Pública Nacional.
- Botnets: qué son, cómo funcionan y cómo se detectan.
- Seguridad en sitios web.
- Principales amenazas.
- Algunos prejuicios y falsas afirmaciones vinculadas a la seguridad.
- Investigaciones vinculadas a Redes Informáticas e Internet (traducido por ArCert).

Tamaño de fuente



Secciones

- Actividades Programadas
- Concurso de Lemas
 - Lema ganador de la edición 2008
- Contacto
- Descargas
 - Banners y Logos
 - Documentos de Interés
 - Wallpapers



SECRETARÍA DE GABINETE Y GESTIÓN PÚBLICA
Subsecretaría de Tecnologías de Gestión
Oficina Nacional de Tecnologías de Información

<http://seguridadinformatica.sgp.gov.ar>



Se suman a la cruzada...

Segu Kids
juntos en la red

Inicio Comunidad Nosotros Recomendar Contacto

JÓVENES

PADRES

DOCENTES

Consejos

- No chatees con extraños
- No brindes información por Internet
- Confía en tus mayores

Te acompañan ...

Bienvenidos

Segu-Kids es un nuevo espacio creado para brindar información a Jóvenes, Padres y Docentes, sobre Seguridad en Internet.

Este nuevo emprendimiento de **Segu-Info** brinda información en forma libre y gratuita y, es el primer sitio pensado con el objetivo de apoyar y acompañar a la familia y a los educadores.

El nacimiento de **Segu-Kids** se debe a la gran cantidad de riesgos existentes en Internet y a la necesidad de crear concientización y educación sobre las

<http://www.segu-kids.org>



Definición y Metodología

Gestión de incidentes de seguridad

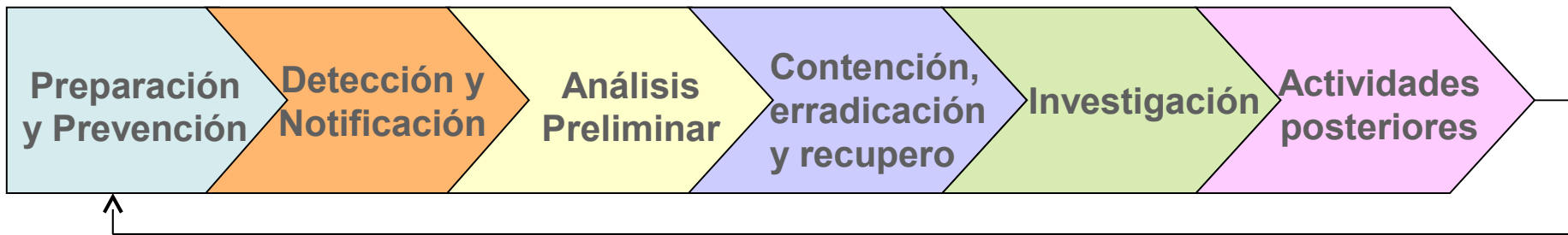
Gestión de incidentes de seguridad

Consiste en la asignación oportuna de los recursos necesarios y su uso adecuado, con el objeto de prevenir, detectar y corregir incidentes que afectan la seguridad de la información.

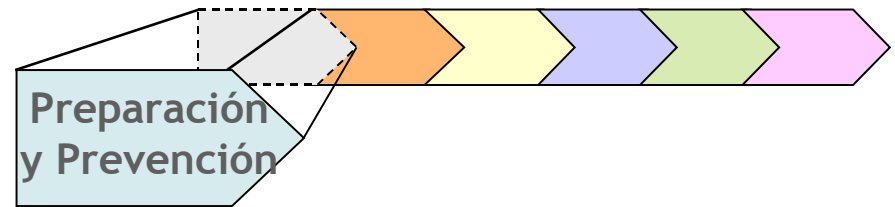
- ✓ Prevención de incidentes
- ✓ Detección y el reporte del incidente
- ✓ Clasificación del incidente
- ✓ Análisis del incidente
- ✓ Respuesta al incidente
- ✓ Registro de incidentes
- ✓ Aprendizaje a partir de la experiencia
- ✓ Concientización y capacitación

Gestión de incidentes de seguridad

Metodología



Gestión de incidentes de seguridad



➤ Categorización de incidentes

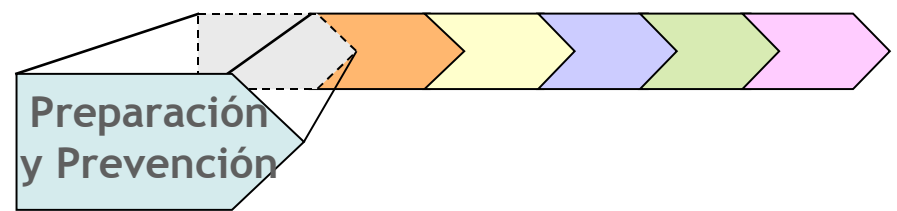
Ejemplo de clasificación por TIPO DE INCIDENTE:

- Denegación de servicio
- Código malicioso
- Acceso no autorizado
- Uso inapropiado
- Incidente múltiple

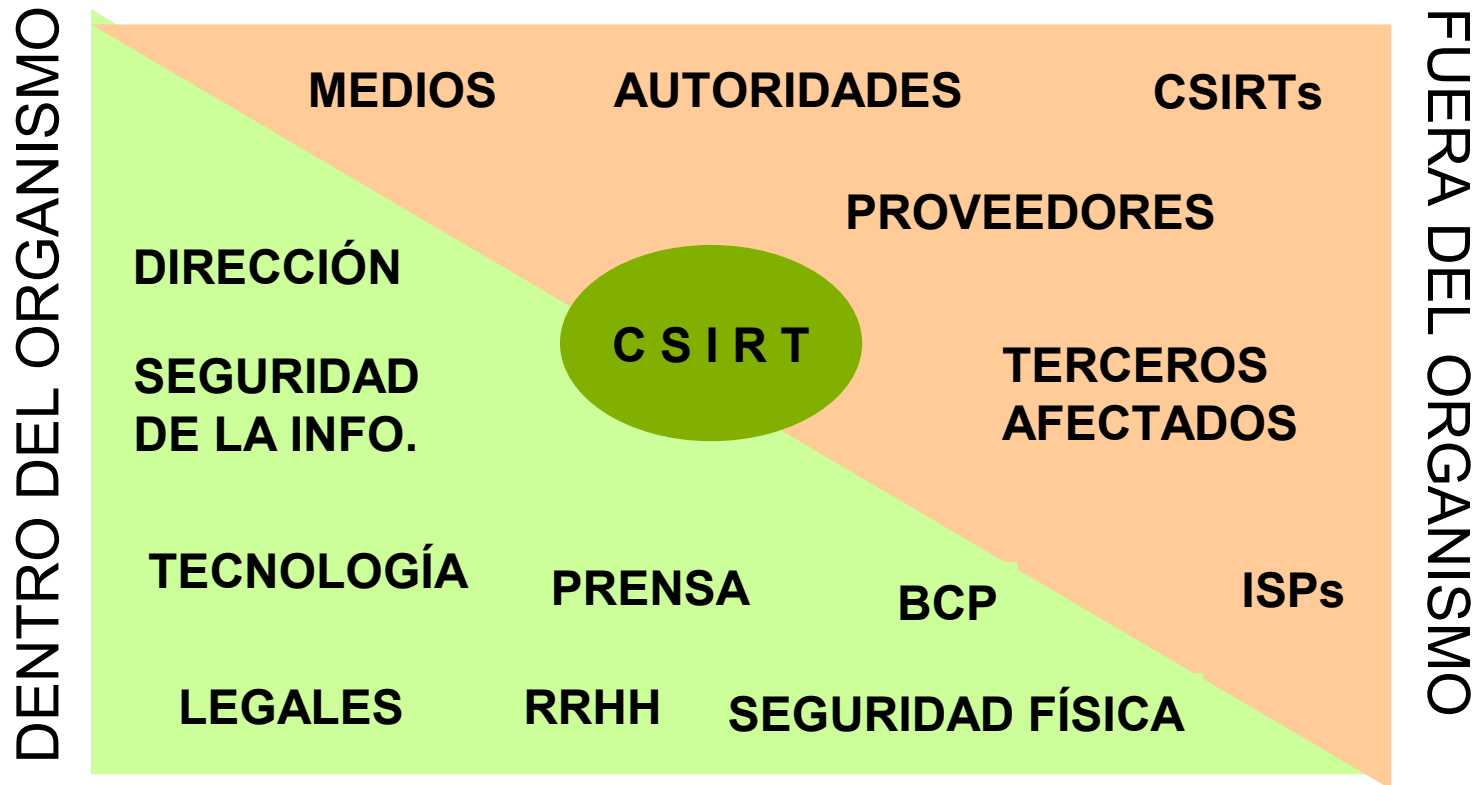
➤ Clasificación de incidentes

Efectos negativos producidos por el incidente o potenciales + Criticidad de los recursos afectados = **CRITICIDAD DEL INCIDENTE**

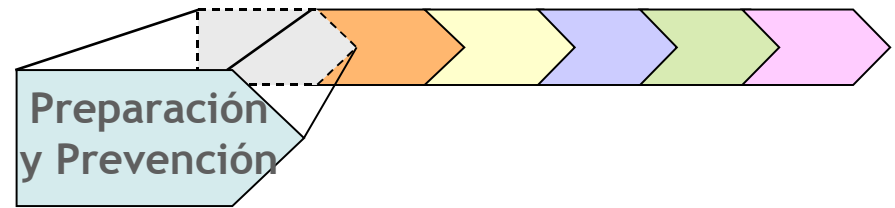
Gestión de incidentes de seguridad



➤ Manejo de información con terceras partes



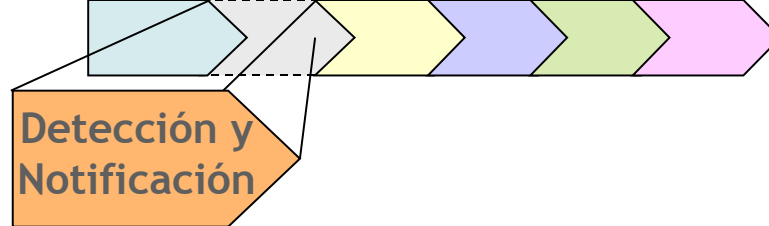
Gestión de incidentes de seguridad



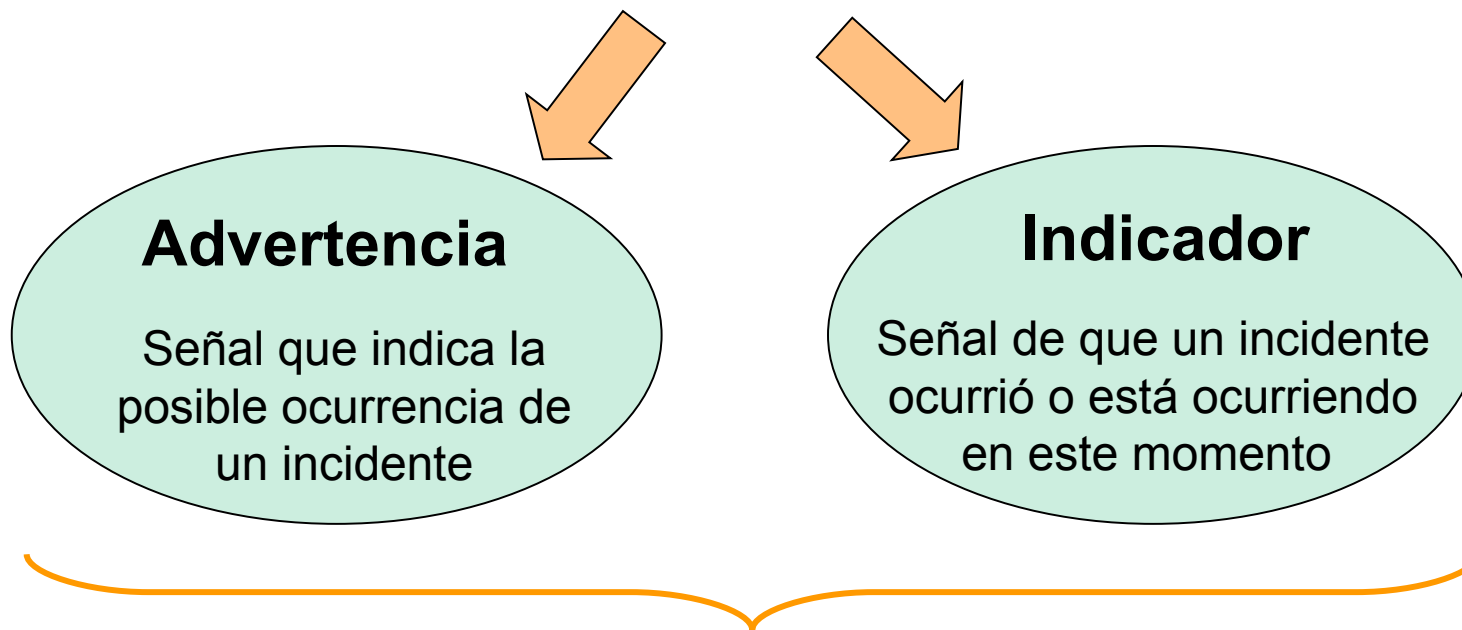
➤ Otras medidas de preparación

- Definir políticas, normas y procedimientos para la gestión de incidentes
- Entrenar al personal
- Documentar un mapa de la topología y arquitectura de la red
- Comprender el funcionamiento normal de redes y sistemas
- Activar los logs y sincronizar relojes
- Definir e implementar esquemas de resguardos de datos
- Contactos
- Etc.

Gestión de incidentes de seguridad

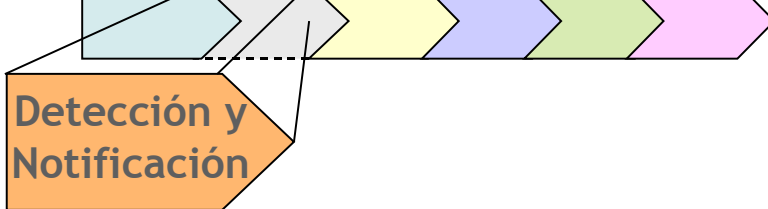


DETECCIÓN DE UN INCIDENTE

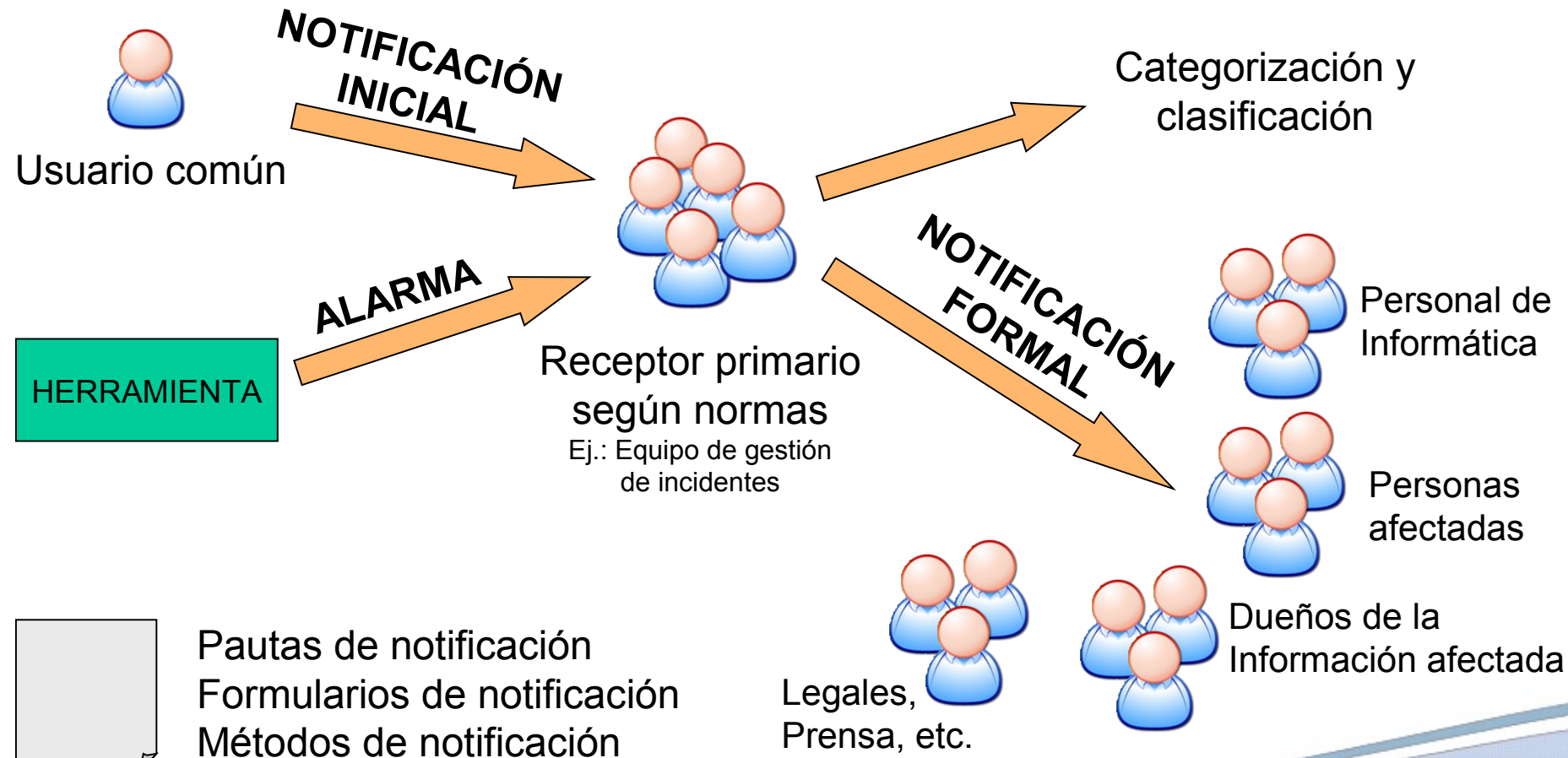


Detección manual o automática

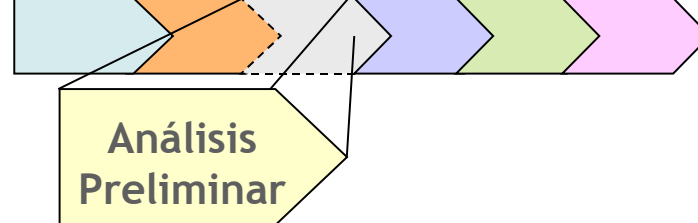
Gestión de incidentes de seguridad



Notificación de incidentes



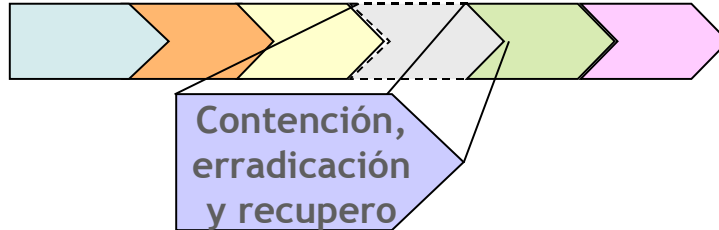
Gestión de incidentes de seguridad



Recolección de información para analizar

- ✓ Alcance del incidente → qué redes, sistemas y aplicaciones afecta
- ✓ Qué originó el incidente
- ✓ Cómo ocurrió (o está ocurriendo) el incidente – métodos, herramientas utilizadas, vulnerabilidades explotadas, etc..
- ✓ El impacto potencial en las actividades del organismo

Gestión de incidentes de seguridad



CONTENCIÓN

Evitar que el incidente siga produciendo daños.

ERRADICACIÓN

Eliminar la causa del incidente y todo rastro de los daños.

RECUPERO

Volver el entorno afectado a su estado original.

Gestión de incidentes de seguridad



Recolección de datos

INFORMACIÓN BASADA EN HOST

- ✓ Live Data Collection Ej.: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la placa de red
- ✓ Forensic duplication Ej.: Backups, archivos copiados recientemente, etc.

INFORMACIÓN BASADA EN LA RED Ej.: Logs de IDSs, logs de monitoreo, información recolectada mediante sniffers, logs de routers, logs de firewalls, información de servidores de autenticación

OTRA INFORMACIÓN Ej.: Testimonio de personal

Gestión de incidentes de seguridad



Recolección de evidencia

AUTENTICIDAD

Quien haya recolectado la evidencia debe poder probar que es auténtica

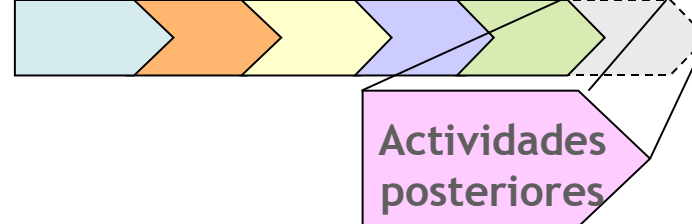
CADENA DE CUSTODIA

Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuando la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.

VALIDACION

Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Gestión de incidentes de seguridad



- Organizar reuniones de autoevaluación
- Mantener la documentación
- Crear bases de conocimiento
- Integrar la gestión de incidentes al análisis de riesgos
- Elaborar Tableros de Control



¡Muchas Gracias!

Preguntas y Comentarios

Ing. Lorena B. Ferreyro

Ing. Marcela I. Pallero

info@arcert.gov.ar

www.arcert.gov.ar



SEMANA
INTERNACIONAL
DE LA
SEGURIDAD
INFORMATICA

"DALE VALOR A TU INFORMACIÓN"

24 de noviembre
al **1** de diciembre

informate en:
seguridadinformatica.sgp.gov.ar