UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

V Jornada de Coordinación del SIC

Incidentes de Seguridad Informática

Servicio de Informática y Comunicaciones

Autores:

Sigfredo Paz - Sergio Velázquez

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

Índice

1. Introducción
2. Tipos de Incidentes
3. Gestión
4. Estadísticas
5. Líneas de trabajo actuales

Introducción

- **Definiciones:**
  - **CERT**

    Computer Emergency Response Team
  - **IRIS-CERT**

    Servicio de seguridad de las redes de centros de RedIRIS
  - **Comité de Seguridad del SIC**

    Grupo de trabajo encargado de decidir las medidas de seguridad informática en la ULPGC

Tipos de Incidentes

- **Clasificación:**
  - **Externos: IRIS-CERT u otros organismos**
    - **SPAM, Virus, Troyanos, Gusanos**
    - **Descarga ilegal material con Copyright**
    - **Escaneos a puertos y otros**
  - **Internos: detectados por el SIC**
    - **SPAM, Virus, Troyanos, Gusanos**
    - **Detección de tráfico anómalo**

Tipos de Incidentes. Ejemplos.

- Infección por virus
- Escaneo de puertos

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

Ejemplo incidente. Infección por virus

Asunto:
[IRIS-CERT #31341] infected customer report 2005/05/04
De:
"IRIS-CERT [Franciso J. Monserrat]" <cert@rediris.es>
Fecha:
Wed, 4 May 2005 19:05:13 +0200
Para:
cert@ulpgc.es

----------Spanish version----------
##
IRIS-CERT es el servicio de seguridad de RedIRIS (Red
Académica y de investigación Española. Nuestra finalidad,
la detección de problemas que afecten a la seguridad de
las redes de centros de RedIRIS, así como actuación
coordinadacon ellos para poner solución a estos problemas.
IRIS-CERT actua como punto de contacto y coordinación
de incidentes para otros servicios de seguridad. El ámbito
de coordinación es toda España. El ámbito de representación#
es todo el mundo.
Para más información:
http://www.rediris.es/cert/index.es.html
##
Hola,

Nos ha llegado una notificación relativa a un incidente de seguridad en el que hay involucrado un equipo de su organización.

Por favor, investigue el incidente, tome las medidas oportunas para que no se vuelva a producir y manténganos informados.

Ejemplo incidente. Infección por virus

Equipos Nuevos

ULPGC | 766 | 193.145.141.31 | 2005-04-29 16:09:54 SPAM | REDIRIS RedIRIS Autonomous Sys
ULPGC | 766 | 193.145.150.10 | 2005-04-27 07:18:29 BEAGLE | REDIRIS RedIRIS Autonomous Sys
ULPGC | 766 | 193.145.150.110 | 2005-04-27 08:16:30 BEAGLE | REDIRIS RedIRIS Autonomous Sys
ULPGC | 766 | 193.145.150.44 | 2005-04-27 09:08:07 BEAGLE | REDIRIS RedIRIS Autonomous Sys

Equipos Repetidos (y cuando se ha repetido)

193.145.145.201
2005-04-28:ULPGC | 766 | 193.145.145.201 | 2005-04-26 14:33:55 BEAGLE | REDIRIS RedIRIS Autonomous Sys
HOY |ULPGC | 766 | 193.145.145.201 | 2005-04-27 14:26:04 BEAGLE | REDIRIS RedIRIS Autonomous Sys
ULPGC | 766 | 193.145.145.201 | 2005-04-28 08:18:29 BEAGLE | REDIRIS RedIRIS Autonomous Sys
193.145.150.120
2005-04-28:ULPGC | 766 | 193.145.150.120 | 2005-04-26 19:34:52 BEAGLE | REDIRIS RedIRIS Autonomous Sys
2005-04-26:ULPGC | 766 | 193.145.150.120 | 2005-04-24 16:12:49 BEAGLE | REDIRIS RedIRIS Autonomous Sys
2005-04-25:ULPGC | 766 | 193.145.150.120 | 2005-04-20 16:41:06 BEAGLE | REDIRIS RedIRIS Autonomous Sys
2005-04-25:ULPGC | 766 | 193.145.150.120 | 2005-04-21 19:08:14 BEAGLE | REDIRIS RedIRIS Autonomous Sys
2005-04-21:ULPGC | 766 | 193.145.150.120 | 2005-04-19 09:34:04 PHATBOT |

Ejemplo incidente. Escaneo de puertos

Asunto:
[IRIS-CERT #30404] Escaneos SSH desde 193.145.141.2 puerto 22/TC
De:
"IRIS-CERT [Franciso J. Monserrat]" <cert@rediris.es>
Fecha:
Thu, 21 Apr 2005 14:57:46 +0200
Para:
cert@ulpgc.es

----------Spanish version----------
##
IRIS-CERT es el servicio de seguridad de RedIRIS (Red
Académica y de investigación Española. Nuestra finalidad,
la detección de problemas que afecten a la seguridad de
las redes de centros de RedIRIS, así como actuación
coordinadacon ellos para poner solución a estos problemas.
IRIS-CERT actua como punto de contacto y coordinación
de incidentes para otros servicios de seguridad. El ámbito
de coordinación es toda España. El ámbito de representación#
es todo el mundo.
Para más información:
http://www.rediris.es/cert/index.es.html
##
Hola,

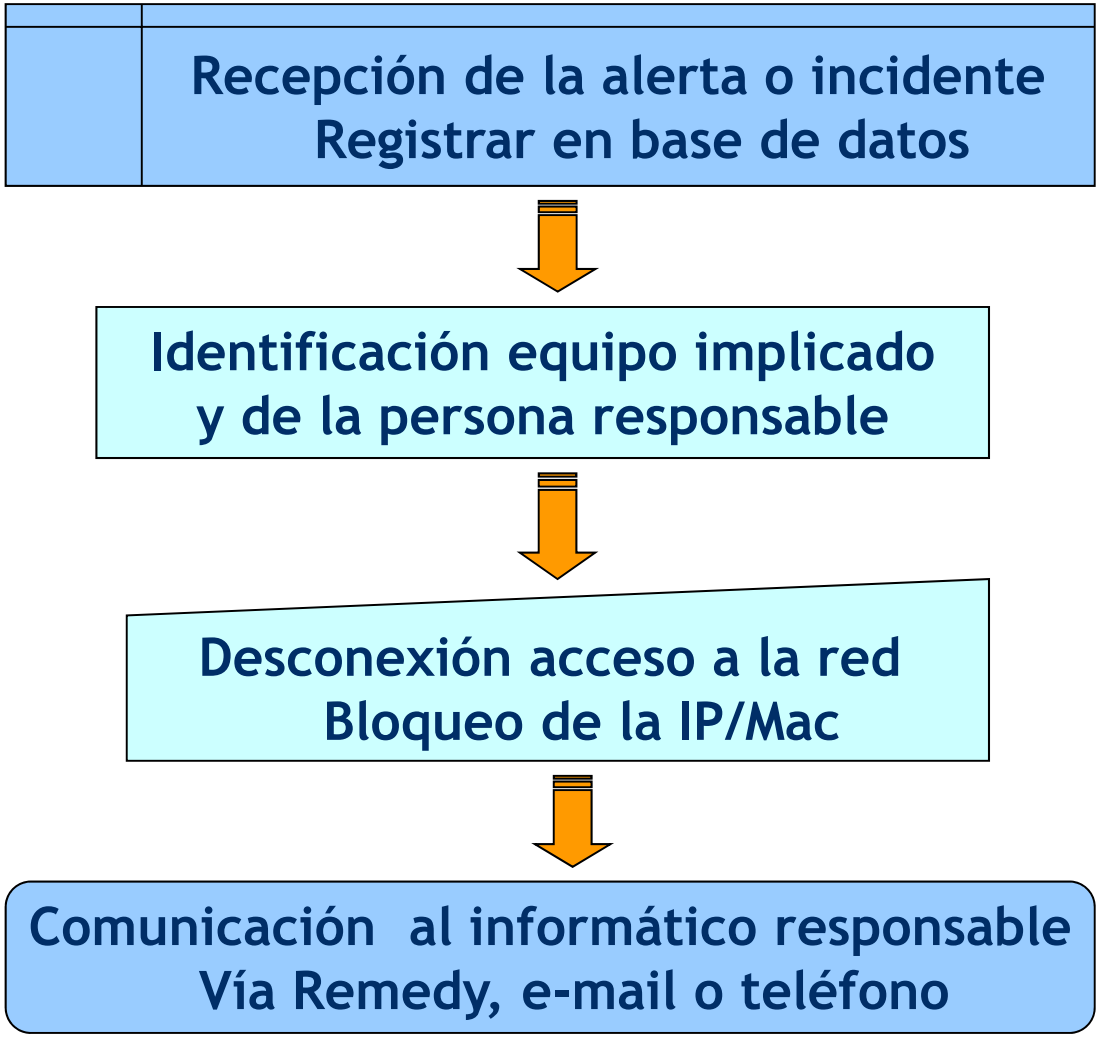
Nos ha llegado una notificación relativa a un incidente de seguridad
en el que hay involucrado un equipo de su organización.

Por favor, investigue el incidente, tome las medidas oportunas para
que no se vuelva a producir y manténganos informados.

Ejemplo incidente. Escaneo de puertos

```
>> Please stop this stuppid things!
>>
>> Logfile Firewall
>>
>> Apr 20 15:15:06 proxy sshd[32285]: Disabling protocol version 1. Could
>> not load host key
>> Apr 20 15:15:06 proxy sshd[32287]: Disabling protocol version 1. Could
>> not load host key
>> Apr 20 15:15:07 proxy sshd[32285]: Invalid user emory from 193.145.141.2
>> Apr 20 15:15:07 proxy sshd[32285]: error: Could not get shadow
>> information for NOUSER
>> Apr 20 15:15:07 proxy sshd[32285]: Failed password for invalid user
>> emory from 193.145.141.2 port 52850 ssh2
>> Apr 20 15:15:07 proxy sshd[32287]: Invalid user enda from 193.145.141.2
>> Apr 20 15:15:07 proxy sshd[32287]: error: Could not get shadow
>> information for NOUSER
>> Apr 20 15:15:07 proxy sshd[32287]: Failed password for invalid user enda
>> from 193.145.141.2 port 52861 ssh2
>> Apr 20 15:15:07 proxy sshd[32289]: Disabling protocol version 1. Could
>> not load host key
>> Apr 20 15:15:07 proxy sshd[32291]: Disabling protocol version 1. Could
>> not load host key
>> Apr 20 15:15:08 proxy sshd[32289]: Invalid user enda from 193.145.141.2
>> Apr 20 15:15:08 proxy sshd[32289]: error: Could not get shadow
>> information for NOUSER
>> Apr 20 15:15:08 proxy sshd[32289]: Failed password for invalid user enda
>> from 193.145.141.2 port 52947 ssh2
>> Apr 20 15:15:08 proxy sshd[32291]: Invalid user endah from 193.145.141.2
>> Apr 20 15:15:08 proxy sshd[32291]: error: Could not get shadow
```

Gestión

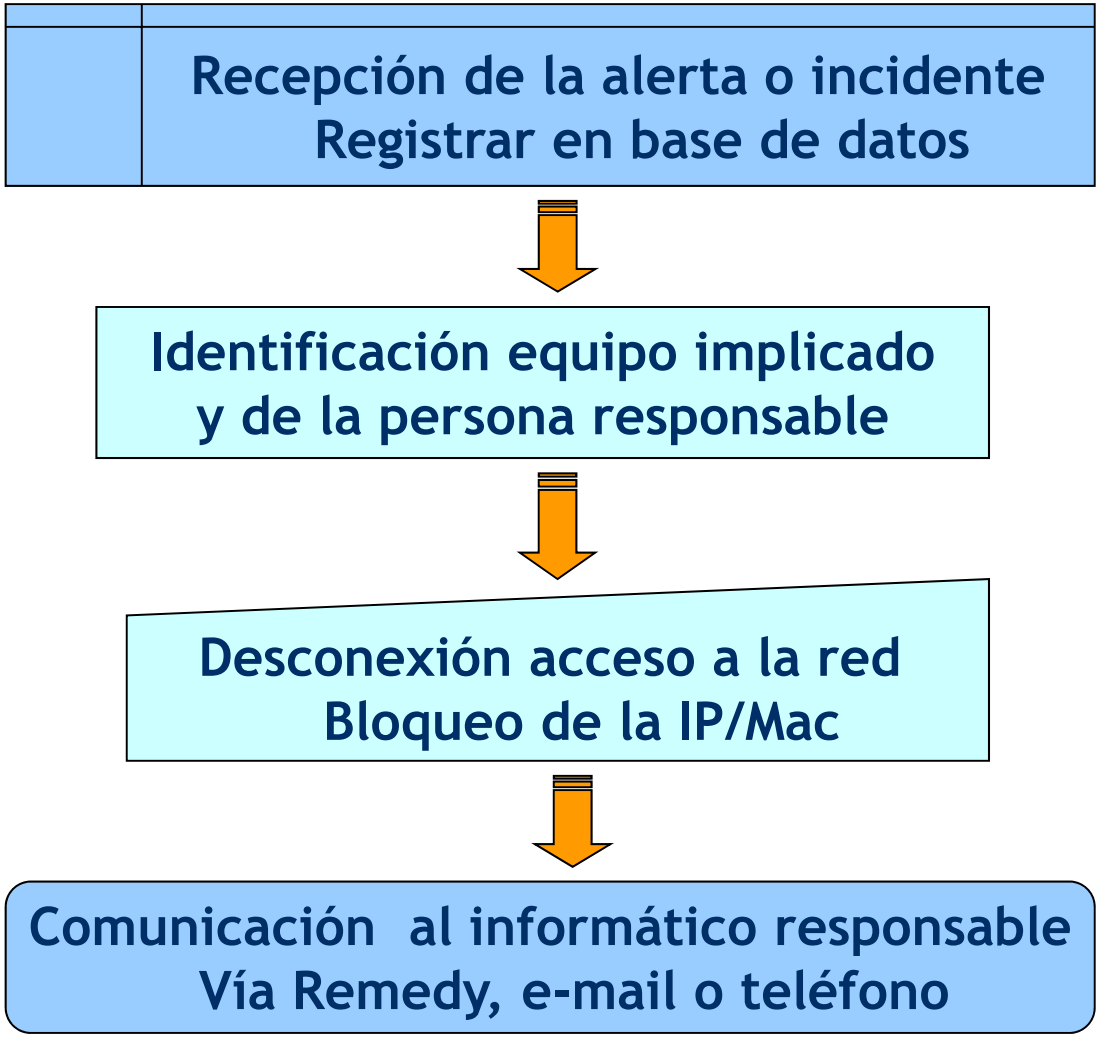

Recepción de la alerta o incidente
Registrar en base de datos
Identificación equipo implicado
y de la persona responsable
Desconexión acceso a la red
Bloqueo de la IP/Mac
Comunicación al informático responsable
Vía Remedy, e-mail o teléfono

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

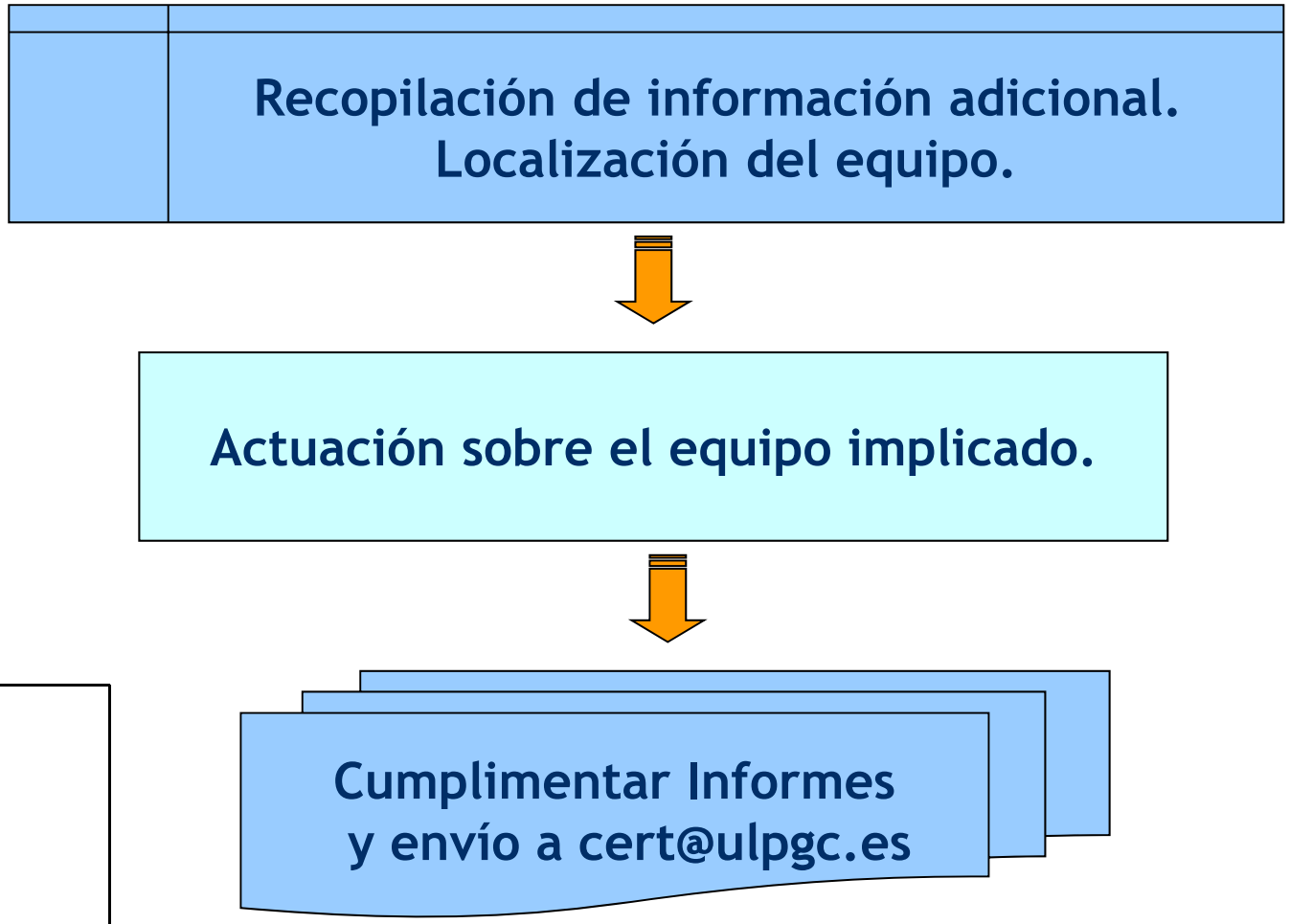
Gestión. Identificación equipo implicado.

	A	B	C	D
1	Mon May 23 00:04:45 2005	:	10.18.11.145:	193.145.150.165:
2	Mon May 23 00:11:44 2005	:	10.18.11.145:	193.145.150.165:
3	Mon May 23 00:24:19 2005	:	10.18.11.145:	193.145.150.165:
4	Mon May 23 00:29:20 2005	221.10.201.162:39096	10.18.11.145:	193.145.150.165:
5	Mon May 23 00:45:33 2005	218.66.104.132:38264	10.18.11.145:	193.145.150.165:
6	Mon May 23 00:54:15 2005	:	10.18.11.145:	193.145.150.165:
7	Mon May 23 00:54:16 2005	61.172.240.137:32824	10.18.11.145:	193.145.150.165:
8	Mon May 23 01:08:04 2005	:	10.18.11.145:	193.145.150.165:
9	Mon May 23 01:26:06 2005	:	10.18.11.145:	193.145.150.165:
10	Mon May 23 01:29:39 2005	:	10.18.11.145:	193.145.150.165:
11	Mon May 23 01:41:48 2005	61.235.154.103:56617	10.18.11.145:	193.145.150.165:
12	Mon May 23 01:53:03 2005	222.174.34.158:33026	10.18.11.145:	193.145.150.165:
13	Mon May 23 02:02:43 2005	:	10.18.11.145:	193.145.150.165:
14	Mon May 23 02:11:23 2005	:	10.18.11.145:	193.145.150.165:
15	Mon May 23 02:11:21 2005	195.221.101.208:29605	10.18.11.145:	193.145.150.165:
16	Mon May 23 02:34:59 2005	:	10.18.11.145:	193.145.150.165:
17	Mon May 23 02:34:59 2005	:	10.18.11.145:	193.145.150.165:
18	Mon May 23 02:51:23 2005	61.152.158.123:45426	10.18.11.145:	193.145.150.165:
19	Mon May 23 02:58:18 2005	221.10.201.162:39096	10.18.11.145:	193.145.150.165:
20	Mon May 23 02:58:18 2005	221.208.208.78:32885	10.18.11.145:	193.145.150.165:
21	Mon May 23 03:12:47 2005	:	10.18.11.145:	193.145.150.165:
22	Mon May 23 03:25:11 2005	:	10.18.11.145:	193.145.150.165:
23	Mon May 23 03:31:01 2005	:	10.18.11.145:	193.145.150.165:
24	Mon May 23 03:44:28 2005	:	10.18.11.145:	193.145.150.165:
25	Mon May 23 03:55:36 2005	61.152.158.151:55749	10.18.11.145:	193.145.150.165:
26	Mon May 23 04:04:08 2005	:	10.18.11.145:	193.145.150.165:
27	Mon May 23 04:04:08 2005	61.152.158.122:36512	10.18.11.145:	193.145.150.165:

Gestión


Recepción de la alerta o incidente
Registrar en base de datos
Identificación equipo implicado
y de la persona responsable
Desconexión acceso a la red
Bloqueo de la IP/Mac
Comunicación al informático responsable
Vía Remedy, e-mail o teléfono

Gestión


Recopilación de información adicional.
Localización del equipo.
Actuación sobre el equipo implicado.
Cumplimentar Informes
y envío a cert@ulpgc.es

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

Gestión. Informes.

Informe Definitivo

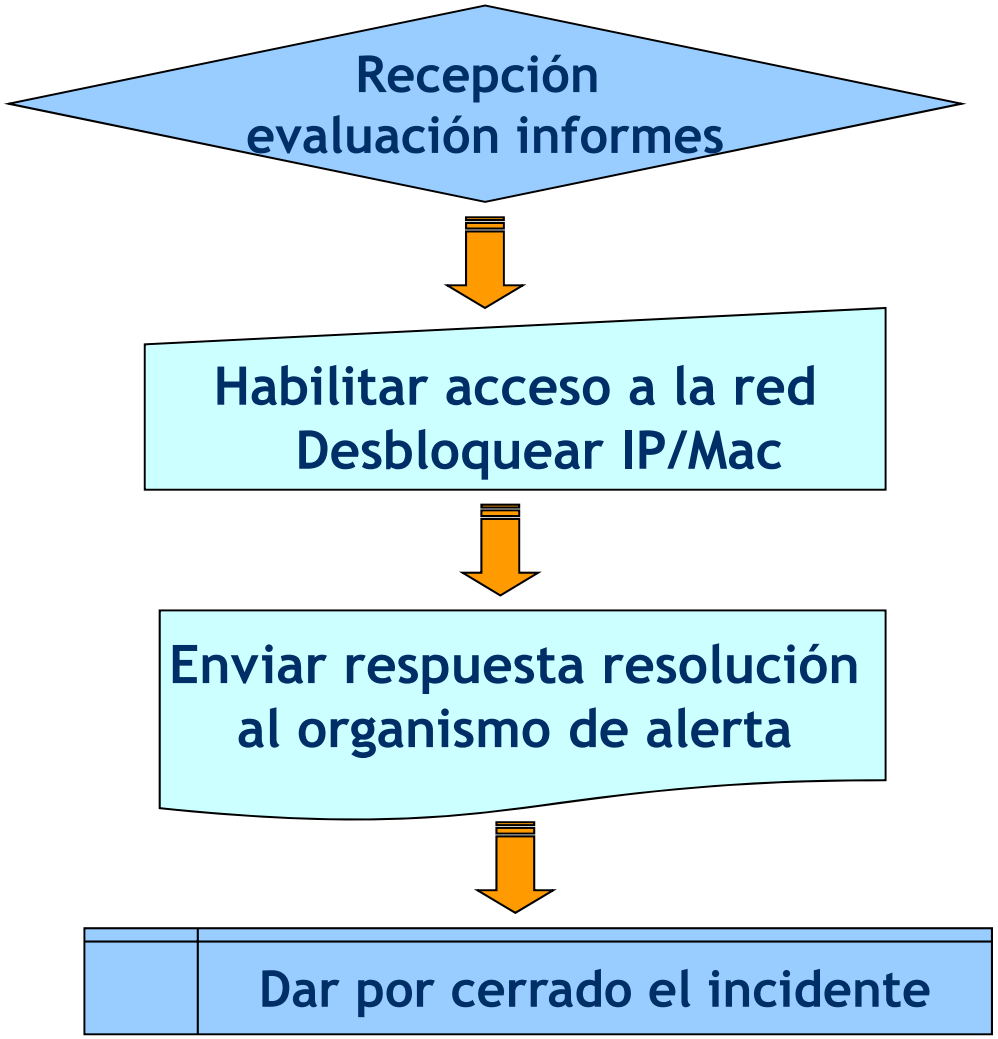
Envíe esta hoja cumplimentada tan pronto solucione el incidente.

Incidencia de la que se informa: **Incidencia de seguridad enviada desde rediris** Nombre y apellidos de la persona que envía este informe: **Miguel Déniz Carrero**
Fecha de solución del incidente: **24 de febrero del 2005**
Explique con detalle el motivo que causó el incidente: **El ordenador tenía cantidad de troyanos considerables (17) de los cuales algunos según la información que pongo en otro documento de word que adjunto son de cierta importancia.**
Explique con detalle los pasos que ha realizado para solucionar el incidente y para evitar que vuelva a suceder en el futuro: **Se paso el panda con discos de arranque hechos al día de hoy y luego el panda desde el sistema operativo, no encontrando ningún virus.** **Se instalo el spyware de Microsoft y se paso con la opción completa detectando y eliminando gran cantidad de entradas en el registro de diversos troyanos.** **El Internet Explorer ha quedado inoperativo instalándosele otro navegador.**

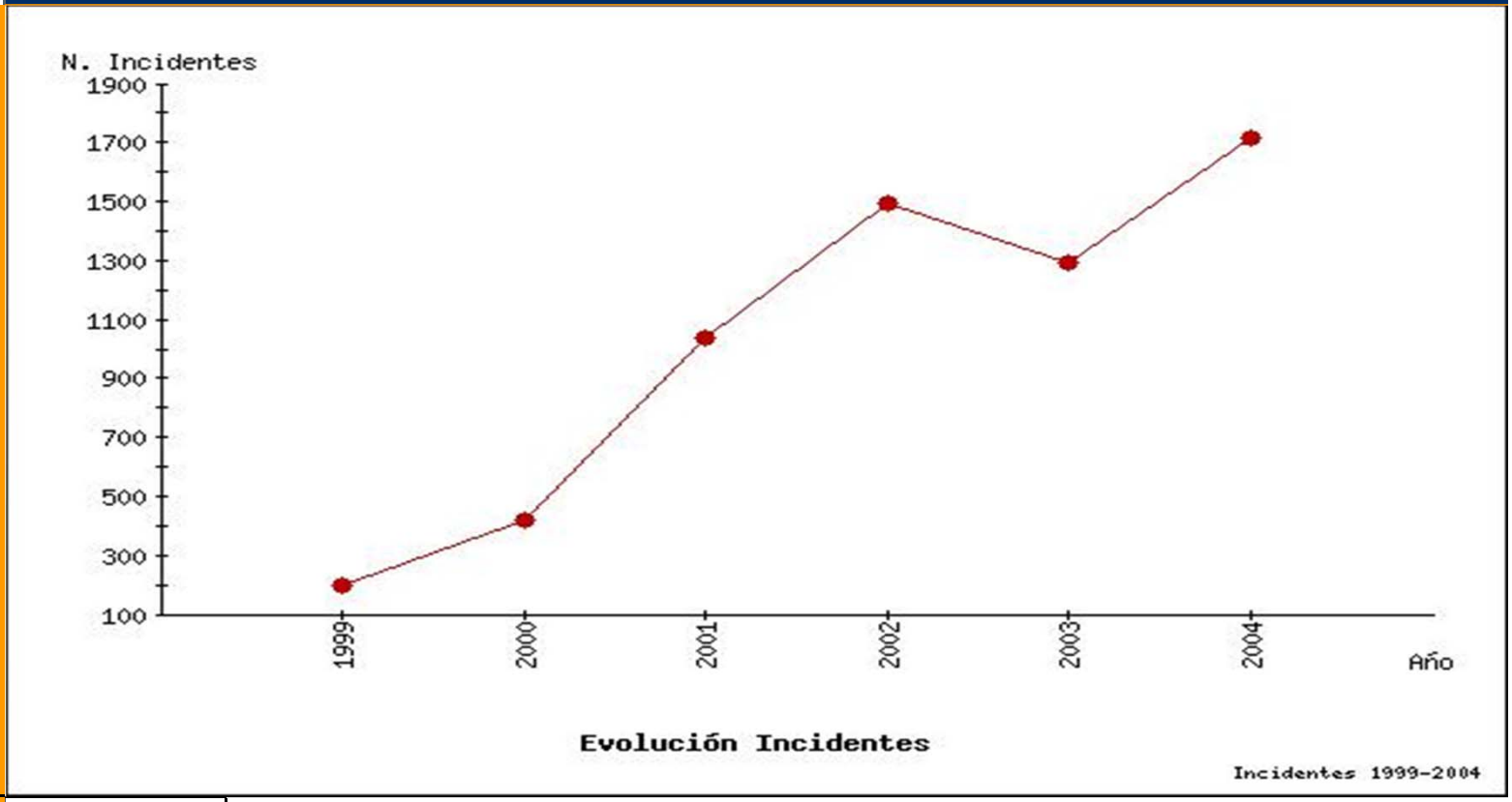
Por favor, añada cuanta información extra, comentario o sugerencia le parezca pertinente.

Enviando el presente informe, solicita se dé por cerrado el incidente y se vuelva a permitir el acceso a la red del ordenador implicado en el incidente.

Gestión


Recepción
evaluación informes
Habilitar acceso a la red
Desbloquear IP/Mac
Enviar respuesta resolución
al organismo de alerta
Dar por cerrado el incidente

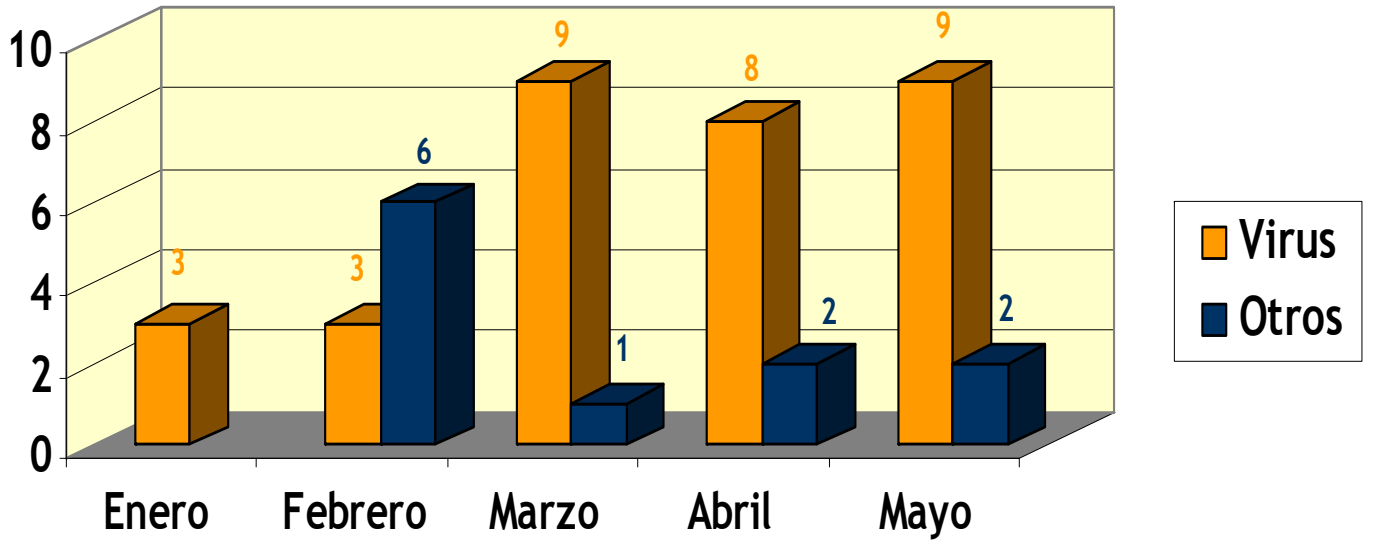
Estadísticas



IRIS-CERT Incidentes 1999 - 2004

Estadísticas

Evolución Incidentes en la ULPGC

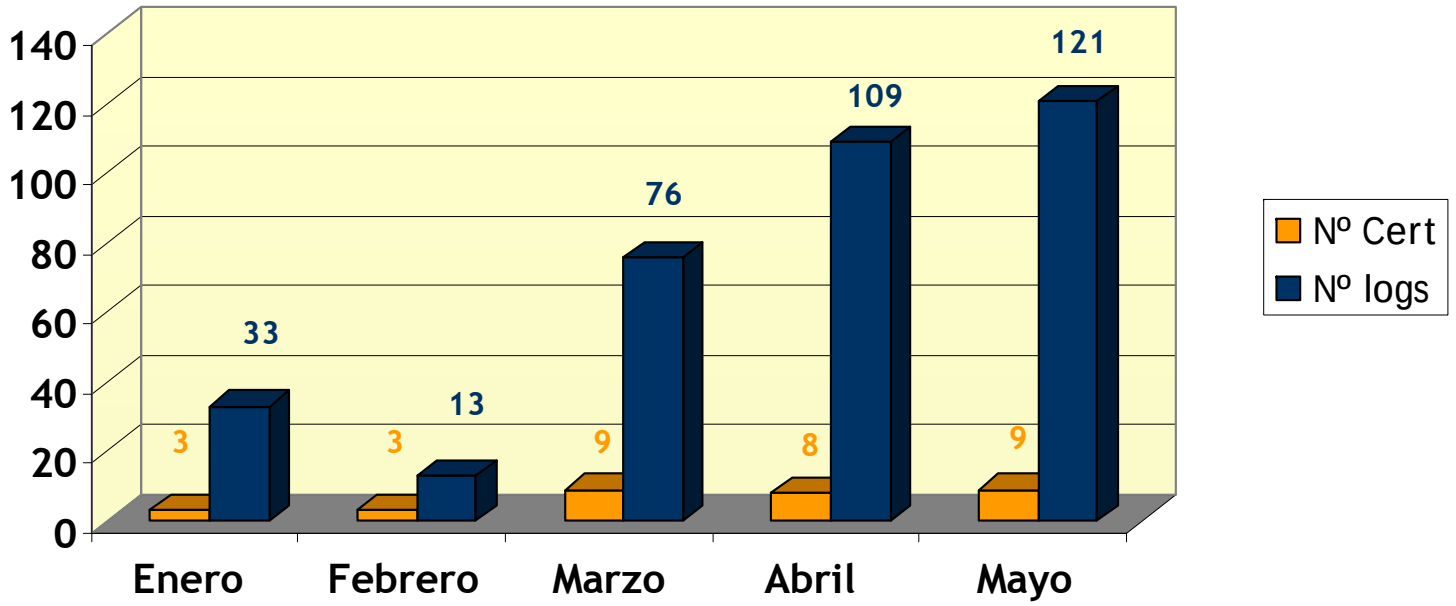


Año 2005

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

Estadísticas

Evolución Incidentes ULPGC

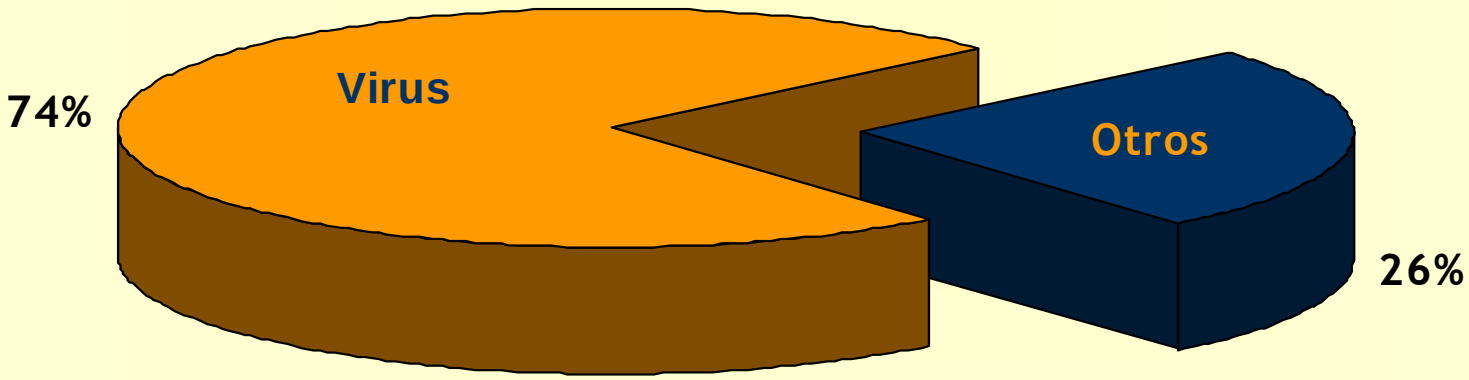


Año 2005

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

Estadísticas

Porcentajes Incidentes ULPGC



Año 2005

Líneas de trabajo actuales

- Identificación de los equipos asignando IPs individuales de salida a Internet.
- Aplicación de filtros para bloquear el acceso a IPs utilizadas por algunos gusanos para propagarse por la red.
- Notificación al usuario del bloqueo del equipo.
- Salida de Residencias Universitarias por líneas ADSL.

UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Servicio de Informática y Comunicaciones

Para obtener más información o para aclarar cualquier pregunta que se les pueda plantear, no duden en ponerse en contacto con:

cert@ulpgc.es

Incidentes de Seguridad Informática

Autores:

Sigfredo Paz - Sergio Velázquez

MUCHAS GRACIAS