Código de Buenas Prácticas para la Gestión de Incidentes de Ciberseguridad

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Motivaciones

Estrategia Nacional de Ciberseguridad
Directiva NIS
Disposición Adicional Novena de la LSSICE

Identificar

Prevenir

Mitigar

Contexto

Código de conducta — **Obligatorio**

Código de buenas prácticas — **Voluntario**

Comentarios a la SETSI hasta el 1 de Octubre

Código de Buenas Prácticas

Objetivos

- ✓ Impulsar e implantar un esquema voluntario de cooperación público-privada
- ✓ Servir como paso previo y facilitador en la adopción de futuras exigencias normativas

Alcance

- ✓ Incidentes de ciberseguridad que afectan a los usuarios finales que hacen uso de los servicios de la SI.

Participantes

- ✓ SETSI
- ✓ INCIBE
- ✓ PSSI

Código de Buenas Prácticas

Información y Aceptación

[R01] Informarán de forma clara y sencilla
[R02] Obtendrán la aceptación del usuario

Prevención y Concienciación

[R03] Prevención y protección
[R04] Campañas de concienciación

Detección

[R05] Detección proactiva
[R06] Integración de la información detectada por INCIBE

Notificación y Soporte

[R07] Sistema de Identificación de usuarios
[R08] Mecanismo de notificación
[R09] Garantía de identidad y autenticidad
[R10] Contenido de la notificación
[R11] Servicio de atención y soporte

Reacción

[R12] Definición de las medidas reactivas y los supuestos de aplicación
[R13] Ejecución de las medidas reactivas

Colaboración

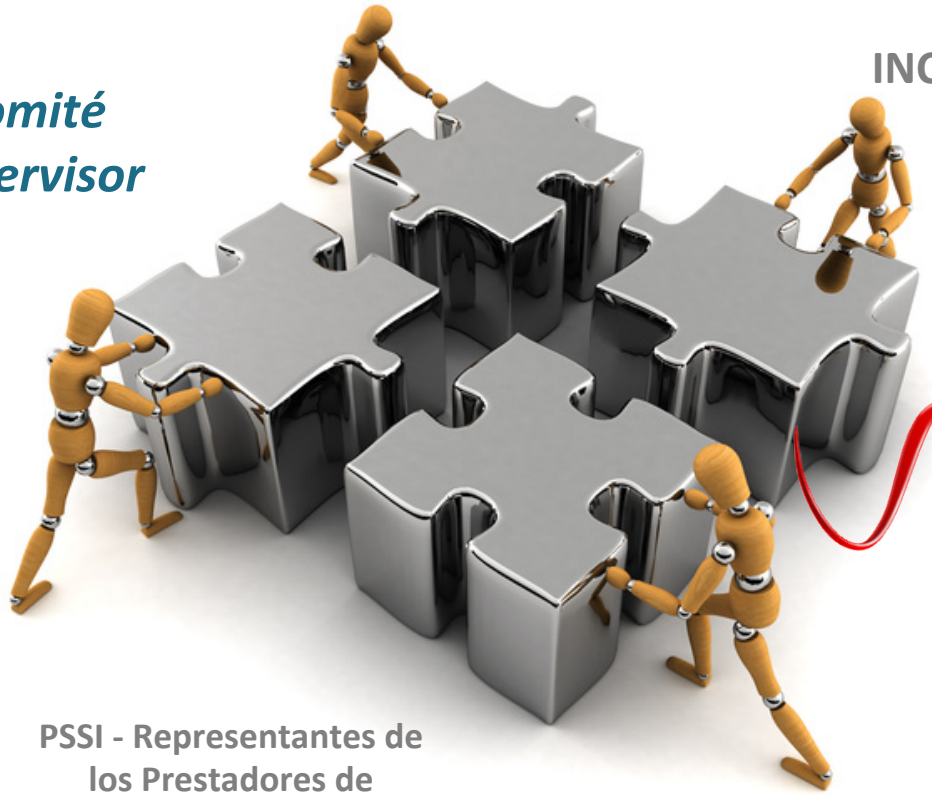
[R14] Punto de contacto
[R15] Intercambio de información
[R16] Reporte a INCIBE (severidad, para la coordinación)
[R17] Reporte a INCIBE (investigación)
[R18] Protocolos de actuación
[R19] Buenas Prácticas

19 Recomendaciones clasificadas en **6 áreas de trabajo**

Modelo de Gobernanza

SETSI

Comité Supervisor



INCIBE

CERTSI (rol de participante para la coordinación de incidentes)

- ***Definir y ejecutar los procedimientos de adhesión, cumplimiento, resolución de conflictos, etc.***
- ***Evaluación y seguimiento***
- ***Mejora continua.***
- ***Comunicación y transparencia***

PSSI - Representantes de los Prestadores de Servicios adheridos al código (participantes).

Servicio AntiBotnet

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Modelo de Inteligencia

✓ Recolección de información:

Interna: Sondas, Honeypots, CERT, Venkman, Whois, ConanMobile.

Externa: eventos de seguridad aportados por terceros.

✓ Análisis de información:

Jennings2: analizador automatizado de muestras y URLs.

Skanna: analizador automatizado de dominios comprometidos.

Flux Detect: detecta dominios fast flux.

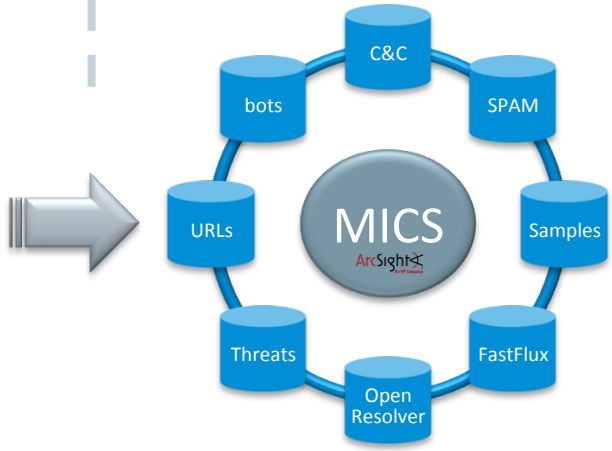
Evidence Seeker: extrae información de sink holes.

Marjory: analizador de correos SPAM.

✓ Motor de inteligencia (MICS):

ArcSight: gestor de información y eventos de seguridad (SIEM).

Feeder: permite consumir la inteligencia generada por el modelo.



✓ Operación de incidentes:

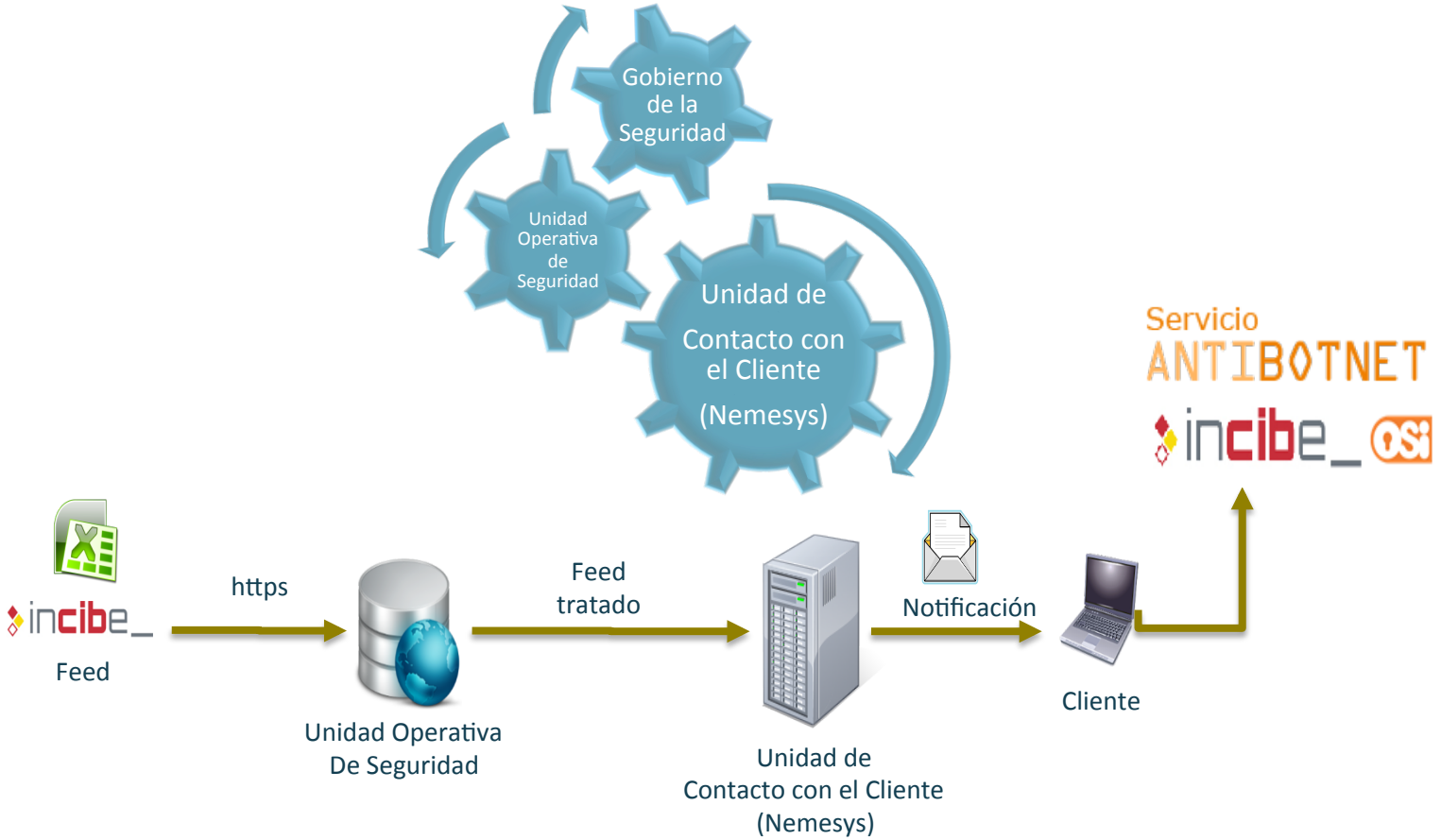
Sensores: correlan la información de MICS con la de la entidad y generan alertas.

Centro Antibotnet: notificación a través de ISPs.

RTIR: gestiona las distintas colas de incidentes de CERTSI

Piloto de Notificación a Usuarios

- *Inicio de notificaciones: 18 de Noviembre 2014*
- *Coordinación entre INCIBE y Telefónica*



Retos enfrentados

INCIBE

- Implementación Técnica: análisis de fuentes y minimización de falsos positivos. Herramientas de desinfección eficaces
- Aspectos legales y organizativos: compartición de información (IPs)
- Impacto en los centros de atención

TELEFÓNICA

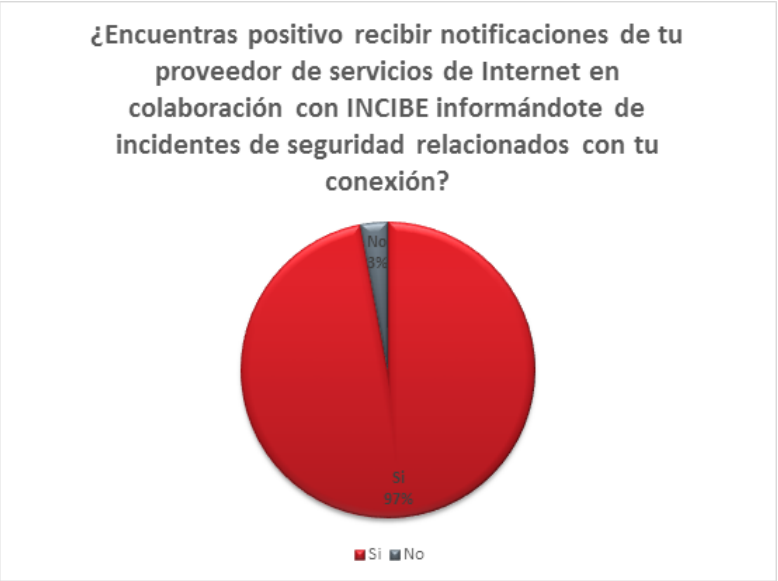
- Convencer a la organización de los beneficios de la iniciativa.
- Impacto en los Centros de Atención
- Impacto en las Unidades Operativas involucradas. Dedicación de recursos.
- Impacto en temas legales. Divulgación y debates internos → Desde el Comité de Seguridad hasta el Comité Ejecutivo

¿Reacción de los usuarios?

Indicadores

Noviembre 2014 – Agosto 2015:

- Volumen de **IP's únicas** notificadas por INCIBE a Telefónica durante el piloto: **1.805.257**
- Se han enviado **132.551 notificaciones** a **19.877 clientes distintos**.
- Cada mes se notifica de media a **1.123 clientes nuevos.**
- **12.498 tickets** consultados en la OSI.
- **12.028 clientes** no han sido notificados en las 5 últimas semanas del piloto => han dejado de aparecer evidencias para dicho cliente => **60%** de los usuarios **notificados se habrían desinfectado**.



Servicio ANTIBOTNET

Piloto de Notificación a Usuarios: Ejemplo

Estimado/a cliente:

Dentro del marco de colaboración público-privada que Telefónica de España, S. A. U. mantiene con la Administración española y en el ánimo de velar por la seguridad de nuestros clientes y del resto de usuarios de Internet, y en cumplimiento con lo dispuesto 34/2002, de 11 de julio[1], nos dirigimos a usted para seguridad por parte del Centro de Respuesta a Incidentes c del cual se nos comunica que alguno de los equipos cone línea [..XXX..] podría estar afectado por un programa ma zombie o botnets.

28/10/14

Según este aviso, con fecha [.....] y con la dirección IP su conexión a Internet, algún equipo o dispositivo habría te zombie [..torpig..], y por lo tanto se pueden esta conocimiento, que podrían afectarle a usted mismo e inclus

Procedimiento de desinfección

Para obtener más información sobre esta amenaza y proce acceder a la web de la Oficina de Seguridad del Internaut Tecnologías de la Comunicación (INTECO).

http://www.osi.es/es/servicio-antibotnet

e introducir el siguiente código en la casilla que figura "Intro

GFzo

[.....]

Información sobre la iniciativa AntiBotnet

La iniciativa AntiBotnet es un proyecto de colaboración público-privada puesto en marcha por los principales prestadores de servicios de la sociedad de la información, la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI) e INTECO.

Servicio ANTIBOTNET

Piloto de Notificación a Usuarios: Desinfección

Servicio Antibotnet: Cleaners

Si has llegado aquí es porque se han identificado incidentes de seguridad relacionados con botnets asociados a tu dirección IP pública, es decir, a tu conexión a Internet. Recuerda que el dispositivo afectado es alguno de los que están o estaban conectados a Internet en tu red en el momento de la detección del incidente.

Por lo tanto, el primer paso para desinfectarte es identificar cual es el equipo afectado. Los datos que te hemos proporcionado: fecha y hora de la detección del incidente y sistemas operativos a los que afecta, te ayudarán a la identificación.

A continuación te facilitamos un listado de herramientas, también llamadas cleaners, que podrán ayudarte a limpiar tu equipo de las principales botnets.

Para maximizar las posibilidades de desinfección, recomendamos utilizar dos cleaners.

Escoge uno de la zona roja, y una vez hayas terminado, desinstálalo y utiliza otro de la zona azul:

Kaspersky Virus Removal Tool	Sophos Virus Removal Tool	Panda Cloud Cleaner	Norton Power Eraser
KASPERSKY	SOPHOS		
Descargar	Descargar	Descargar	Descargar

Recuerda que estas herramientas no sustituyen en ningún caso a los sistemas antivirus o anti-malware. Te recomendamos que estés al día de los consejos para prevenir infecciones y que utilices herramientas de seguridad en tus dispositivos.

Suscripción al feed

- ✓ Proceso sencillo → Firma de NDA
- ✓ Feedback sobre uso de la información
- ✓ Evolución de fuentes → Más amenazas
- ✓ Servicio abierto a comentarios
- ✓ Valor añadido a clientes

¡Gracias!