



Uruguay

SEGURINFO 2011

XII Congreso Interamericano de Seguridad de la Información

"SEGURIDAD, UNA PLATAFORMA DE VALOR PARA EL
NEGOCIO"

Cybercrimen y Manejo de Incidentes



USUARIA



Uruguay

SEGURINFO 2011

XII Congreso Interamericano de Seguridad de la Información

"SEGURIDAD, UNA PLATAFORMA DE VALOR PARA EL
NEGOCIO"

Presentada por:

Julio César Ardita

CTO CYBSEC

jardita@cybsec.com



Aclaración:

- © Todos los derechos reservados. No está permitida la reproducción parcial o total del material de esta sesión, ni su tratamiento informático, ni la transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, sin el permiso previo y por escrito de los titulares de los derechos. Si bien este Congreso ha sido concebido para difusión y promoción en el ámbito de la profesión a nivel internacional, previamente deberá solicitarse una autorización por escrito y mediar la debida aprobación para su uso.

Agenda

- Estado del arte de los incidentes de seguridad
- Estrategias para el manejo de incidentes
- Experiencias concretas de la gestión de incidentes de seguridad

Estado del arte de los incidentes de seguridad

Incidentes de seguridad reales

- Robo de información sensible
- Robo y pérdida de notebooks / smartphones con información sensible
- Denegación de servicio sobre equipos de networking, afectando la operación diaria de la Compañía
- Denegación de servicio por el ingreso y propagación de virus y worms que explotan vulnerabilidades
- Fraude financiero



Estado del arte de los incidentes de seguridad

Incidentes de seguridad reales

- Sabotaje Corporativo a través de modificaciones de programas por parte del personal interno que generó problemas de disponibilidad en servicios críticos (programa troyano)
- Amenazas y denuncias falsas a través de mensajes de correo electrónico anónimos
- Ataques locales de phishing a Empresas



Estado del arte de los incidentes de seguridad

¿Por qué se generan más incidentes que antes?

- Crecimiento de la dependencia tecnológica
- No hay una conciencia sobre la privacidad
- Amplia disponibilidad de herramientas
- No hay leyes globales (y pocas locales)
- Falsa sensación de que todo se puede hacer en Internet
- Gran aumento de vulnerabilidades de seguridad (sólo en el 2010 se reportaron 9.428 según CERT)



Estado del arte de los incidentes de seguridad

¿Por qué se generan más incidentes que antes?

- Traslado de negocios con dinero real a Internet (servicios financieros, juegos de azar, sitios de subastas, etc.)
- Oferta y demanda de información confidencial más abierta



Estado del arte de los incidentes de seguridad

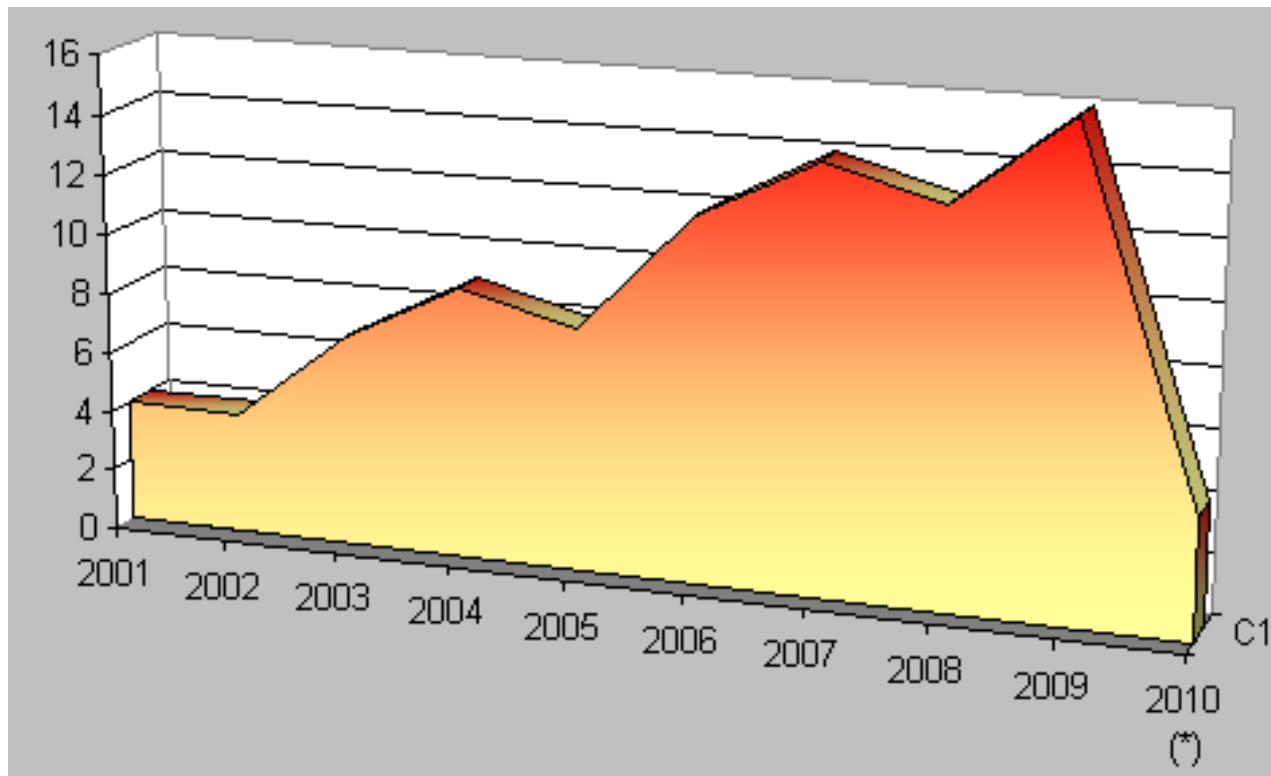
Tendencias en incidentes

- Los intrusos “saben” más técnicas para evitar que los rastreen
- Nuevo origen de incidentes: redes wireless abiertas
- Casos de publicación de venta en Internet de información sensible de empresas argentinas
- Casos individuales de robo de identidad basados en información disponible en Internet



Estado del arte de los incidentes de seguridad

Cantidad de incidentes graves manejados por CYBSEC



Estado del arte de los incidentes de seguridad

CSIRT internos en compañías de Latinoamérica

Detectamos “CSIRT’s internos” en bancos, empresas financieras, seguros, retail y e-commerce.

¿Cuándo un CSIRT interno es (o debe) ser creado?

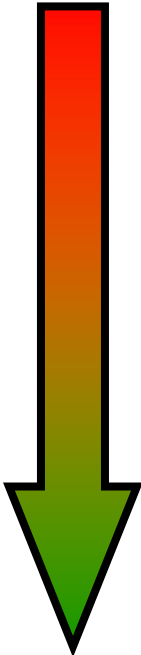
Colaboración entre el CSIRT interno y el CSIRT país.

Impacto cultural: Planificación, documentación, confianza en personas, comunicación, etc.



Estado del arte de los incidentes de seguridad

Madurez de los CSIRT's internos



No poseen (85%)



Manejo de incidentes desorganizado (8%)



Manejo de incidentes formal para la foto (compliance) (4%)

Manejo de incidentes formal real (2%)



CSIRT interno (<1%)



Estado del arte de los incidentes de seguridad

Tendencias en CSIRT's internos

Desde el año 2009 cada vez más compañías están comenzando a crear un CSIRT interno.

Razones principales:

- Las compañías han tenido y tienen incidentes graves.
- La regulación le exige Manejo de Incidentes.
- El CSO proactivamente muestra la necesidad.



Estrategias para el manejo de incidentes

Manejo de incidentes de seguridad

Hacemos todo lo posible para tener un elevado nivel de seguridad en la Compañía, pero surge un incidente de seguridad grave.



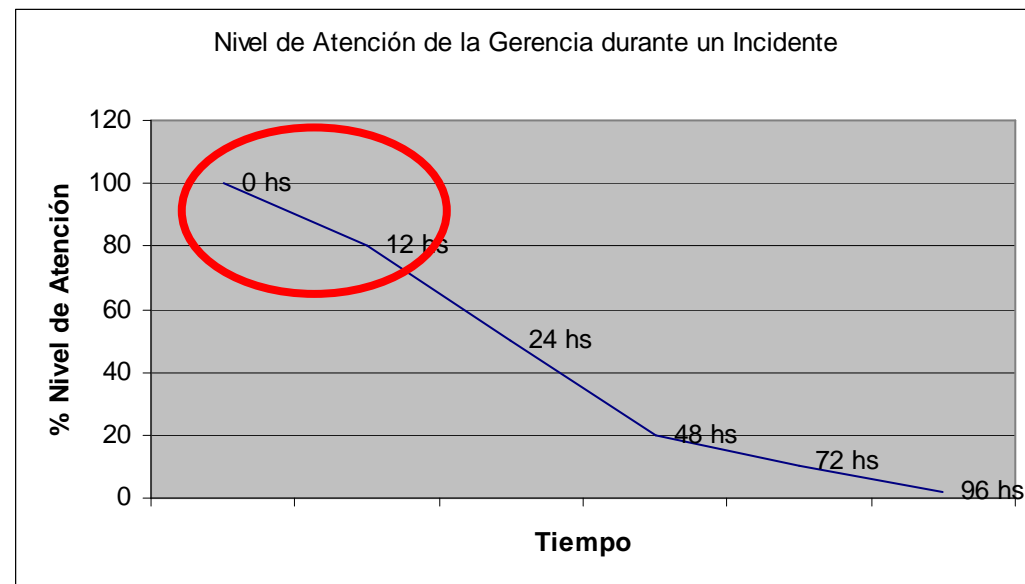
Tips:

- No ocultarlo.
- Mantener la calma por la situación personal del CSO
- No comenzar buscando culpables
- Obtener información de primera mano y verificarla
- Establecer un Plan de Acción y coordinarlo

Estrategias para el manejo de incidentes

Manejo de incidentes de seguridad

Durante las primeras horas tendremos la atención de la Compañía puesta en nosotros. Es clave aprovechar este momento.



Estrategias para el manejo de incidentes

Pasos a seguir cuando sucede un incidente

1. Reunión de relevamiento on-site con todos los referentes e involucrados.



2. Verificar la información.

3. Consolidar y revisar toda la información relevada.

4. Análisis preliminar de impacto del incidente.

5. Elaborar el diagnóstico detallado de la situación.

Estrategias para el manejo de incidentes

Pasos a seguir cuando sucede un incidente

6. Definir los mensajes de comunicación a transmitir a través de canales de comunicación externos e internos.
7. Elaborar un Plan de Acción detallado y consensuado con todas las áreas participantes.
8. Organizar grupos de trabajo para llevar adelante las actividades planificadas en el Plan de Acción coordinados por el CSO.



Estrategias para el manejo de incidentes

Pasos a seguir cuando sucede un incidente

9. Implementar y gerenciar el Plan de Acción priorizando las actividades más críticas con el objetivo de bajar lo mas rápido posible el nivel de exposición al riesgo que afecta a la Compañía.

10. Documentar detalladamente TODO lo realizado.

11. Vuelta a la normalidad.



Estrategias para el manejo de incidentes

Pasos a seguir cuando sucede un incidente

12. Luego del cierre del incidente:

- Aplicar “lecciones aprendidas”.
- Estimar las pérdidas económicas.
- Ajustar los procedimientos.
- Informe ejecutivo al Directorio y áreas de negocio.

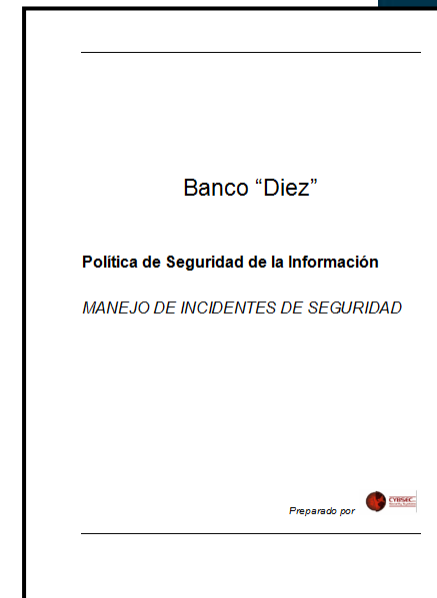


Estrategias para el manejo de incidentes

Política de Manejo de Incidentes de Seguridad Informática

Temas a tener en cuenta:

1. Detección y notificación de Incidentes de Seguridad Informática
2. Rastreo de Incidentes de Seguridad Informática
3. Recolección de evidencia
4. Proceso de recuperación de los sistemas afectados
5. Proceso disciplinario



Estrategias para el manejo de incidentes

Procedimientos de Manejo de Incidentes de Seguridad Informática

Diagrama de flujo del Procedimiento.

Responsabilidades:

- Usuarios
- Auditoría Interna
- Recursos Humanos
- Dirección de la Organización
- Asuntos Legales
- Seguridad Física
- Mesa de Ayuda
- Administrador del Sistema
- Seguridad Informática
- Otras Áreas



Experiencias concretas en la gestión de incidentes

CASO 1: Denegación de servicio

Descripción del incidente:

El viernes 22 de diciembre de 2009 una Empresa de Retail fue atacada por un intruso que impidió la continuidad del negocio en sus casi 120 sucursales.

En un análisis preliminar de la situación determinó que un intruso había dejado un programa que se ejecutó el día viernes a las 19:00hs horas y que bloqueaba el acceso al sistema de Ventas.

Se comenzó a trabajar en dos líneas:

- Volver a la operación normal.
- Detección, análisis y rastreo del intruso.



Experiencias concretas en la gestión de incidentes

CASO 1: Denegación de servicio

Metodología de Investigación:

En relación a la **vuelta a la operación normal**:

1. Análisis forense inmediato de los equipos afectados.
2. Detección de programas que impedían el normal funcionamiento del Sistema de Ventas.
3. Análisis de programas y modificaciones realizadas por el intruso.
4. Planteo de soluciones.
5. Pruebas sobre una sucursal de los cambios.
6. Aplicación masiva de cambios y vuelta a la operación normal.



Experiencias concretas en la gestión de incidentes

CASO 1: Denegación de servicio

Metodología de Investigación:

En relación a la **detección, análisis y rastreo del intruso:**

1. Ingeniería reversa de los programas que dejó el intruso
2. Determinación de las actividades que realizó el intruso.
3. Detección de rastros de pruebas 4 días antes.
4. Determinación de pruebas que podrían indicar el perfil del intruso.
5. Análisis de los sistemas de acceso remoto.
6. Evaluación de las computadoras personales de los potenciales sospechosos.



Experiencias concretas en la gestión de incidentes

CASO 1: Denegación de servicio

Metodología de Investigación:



7. En el equipo de José se detectaron varios elementos (**repetición del patrón de comportamiento del intruso por la forma en que ejecutaba los comandos**).
8. Se detectó que otra computadora que contenía evidencia y se encontraba al lado del equipo de José misteriosamente fue formateada y re-instalada dos días después del incidente y en la misma se detectó el patrón de comportamiento del intruso.

Experiencias concretas en la gestión de incidentes

CASO 1: Denegación de servicio

Resultados obtenidos :

Se logró detectar la intrusión y se volvió la operación normal en el plazo inmediato.

De acuerdo a las características detectadas del patrón de comportamiento, información encontrada, re-instalación de un equipo, conocimiento de las claves de acceso necesarias, existe una gran probabilidad de que el intruso fuera José.



Experiencias concretas en la gestión de incidentes

CASO 2: Phishing a un Banco

Descripción del incidente:



Un Banco Argentino comenzó a recibir llamados de Clientes alertando sobre un mensaje que estaban recibiendo pidiendo que se actualizaran sus datos a las 9:30 am de un jueves de febrero de 2010.

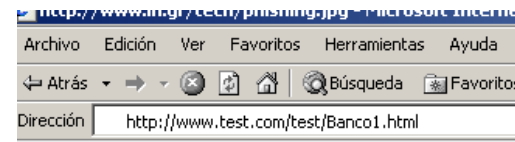
En el análisis preliminar de uno de los mensajes recibidos vía correo electrónico por parte de un Cliente, se determinó que el Banco estaba sufriendo un ataque de Phishing.

A las 10:20 am se comenzó a investigar el incidente.

Experiencias concretas en la gestión de incidentes

CASO 2: Phishing a un Banco

Metodología de Investigación:



1. Se analizó el mensaje de correo electrónico que estaba siendo recibido por los Clientes. Dentro del mail figuraba un link al sitio web del Banco. El link que aparecía era correcto, pero la referencia apuntaba a otro sitio web que se encontraba en Singapur.
2. Se determinó que una vez que se realizaba un click sobre el link, el sitio falso del intruso explotaba una vulnerabilidad en el Explorer que le hacía aparecer en la dirección del navegador el sitio original del Banco.

Experiencias concretas en la gestión de incidentes

CASO 2: Phishing a un Banco

Metodología de Investigación:

3. Se analizaron los scripts que se ejecutaban y se determinó que el sitio falso pedía el usuario y la clave del sistema de Home Banking y luego enviaba esa información a una cuenta determinada de Gmail. Finalmente lo redirigía al sitio original del Banco con un mensaje para que vuelva a ingresar los datos.
4. Ante esta situación, se trabajó en dos líneas:
 - Generación de datos falsos para el intruso.
 - Tomar contacto con la Empresa del sitio web afectado.



Experiencias concretas en la gestión de incidentes

CASO 2: Phishing a un Banco

Metodología de Investigación:

4.1 Generación de datos falsos para el intruso.

Para confundir y sobrecargar la cuenta de mail del intruso, se generaron lotes de datos que cumplían con los requerimientos formales, pero que no eran válidos. Se enviaron unos 37.000 mensajes de forma automatizada.

4.2 Contacto con Singapur.

Debido a la diferencia horaria, cerca de las 19:00hs (GMT-3) pudimos contactarnos telefónicamente y vía mail con el proveedor de hosting que colaboró activamente, dando de baja los scripts del intruso del sitio web y enviándonos la información de los logs de acceso.



Experiencias concretas en la gestión de incidentes

CASO 2: Phishing a un Banco

Metodología de Investigación:

5. Con la información de los logs de acceso, se filtró la información basura que habíamos generado a propósito y junto con otra información se entrecruzaron los datos determinando qué Clientes habían ingresado sus datos.
6. Paralelamente se comenzó a investigar el origen del intruso.



Experiencias concretas en la gestión de incidentes

CASO 2: Phishing a un Banco

Resultados obtenidos:

En pocas horas **se logró frenar el ataque de phishing** y determinar cuáles habían sido los Clientes del Banco afectados. Se detectó que el intruso había accedido solamente a dos cuentas.

Se logró rastrear el origen del intruso. Provenía de Venezuela.



Experiencias concretas en la gestión de incidentes

CASO 3: Modificación de información

Descripción del incidente:

Un **intruso** ingresó en la Base de Datos de personal y ejecutó un script SQL que **augmentó el sueldo en un 70% a todo el personal** el día 27 de julio de 2008.

Un día después, el sistema de liquidación generó los pagos causando graves problemas a la Organización.

Se comenzó la investigación analizando el Servidor de Producción de Personal.



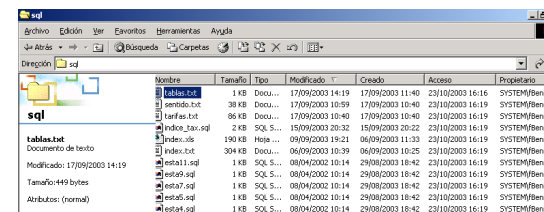
USUARIA

Experiencias concretas en la gestión de incidentes

CASO 3: Modificación de información

Metodología de Investigación:

1. Análisis del Servidor UNIX de Producción que contiene la Base de Datos.
2. Detección en el directorio principal del usuario **Maria** lo que parecía ser el script SQL que se había ejecutado.
3. Restricción de las PC's de los usuarios que accedieron en ese momento.
4. Evaluación de 9 PC's de los usuarios buscando archivos creados, modificados y accedidos el día del incidente.



Nombre	Tamaño	Tipo	Modificado	Creado	Acceso	Propiedades
tablas.txt	1 KB	Docu...	17/09/2003 14:19	17/09/2003 11:40	23/10/2003 16:16	SYSTEM/Beni
sendido.txt	38 KB	Docu...	17/09/2003 10:59	17/09/2003 10:40	23/10/2003 16:19	SYSTEM/Beni
tarifas.txt	86 KB	Docu...	17/09/2003 10:40	17/09/2003 10:40	23/10/2003 16:19	SYSTEM/Beni
index_2001.sql	2 KB	SQL S...	15/09/2003 20:32	15/09/2003 20:22	23/10/2003 16:19	SYSTEM/Beni
index_05	190 KB	Hols...	09/09/2003 19:21	06/09/2003 11:33	23/10/2003 16:19	SYSTEM/Beni
index.txt	304 KB	Docu...	06/09/2003 10:39	06/09/2003 10:25	23/10/2003 16:19	SYSTEM/Beni
esta11.sql	1 KB	SQL S...	08/04/2002 10:14	29/08/2003 18:42	23/10/2003 16:19	SYSTEM/Beni
esta6.sql	1 KB	SQL S...	08/04/2002 10:14	29/08/2003 18:42	23/10/2003 16:19	SYSTEM/Beni
esta7.sql	1 KB	SQL S...	08/04/2002 10:14	29/08/2003 18:42	23/10/2003 16:19	SYSTEM/Beni
esta5.sql	1 KB	SQL S...	08/04/2002 10:14	29/08/2003 18:42	23/10/2003 16:19	SYSTEM/Beni
esta4.sql	1 KB	SQL S...	08/04/2002 10:14	29/08/2003 18:42	23/10/2003 16:19	SYSTEM/Beni



Experiencias concretas en la gestión de incidentes

CASO 3: Modificación de información

Metodología de Investigación:

5. Se detectó un solo equipo que tenía **archivos relevantes**, el del usuario **Pedro**. Se detectó dentro del directorio C:\temp, un archivo que contenía parte del script detectado en el directorio del usuario Maria. Ese archivo fue generado por la herramienta SQLPlus.
6. Se analizaron las conexiones al **Servidor UNIX de Producción** el día del incidente y se detectó que el **usuario Maria** había entrado **desde el Servidor de Desarrollo** y tuvo una sesión abierta de 3 horas.
7. Se investigó el Servidor de Desarrollo y se detectó que unos minutos antes de conectarse el **usuario Maria** al UNIX de Producción, **el usuario Pedro** había entrado a Desarrollo desde su PC.

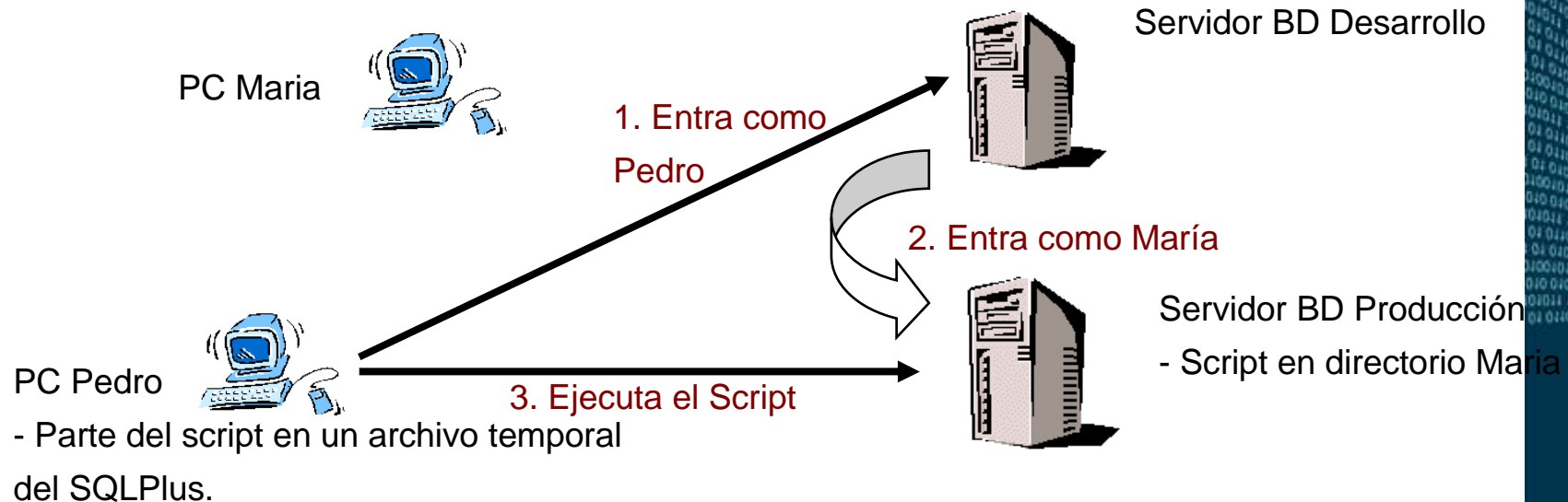


Experiencias concretas en la gestión de incidentes

CASO 3: Modificación de información

Metodología de Investigación:

- Se buscó los registros de la cámara de vigilancia de la entrada del edificio y Maria se había retirado 1 hora antes del incidente.



Experiencias concretas en la gestión de incidentes

CASO 3: Modificación de información

Resultados obtenidos:

Se determinó que el intruso fue Pedro y que trato de incriminar al usuario Maria.



Gracias por asistir a esta sesión...



**Preguntas y
Respuestas...**

Para mayor información:

Julio César Ardita

CTO CYBSEC

jardita@cybsec.com



Para descargar esta presentación visite
www.segurinfo.org

Los invitamos a sumarse al grupo “Segurinfo” en **LinkedIn**®