Education Center

Cumplimiento Regulatorio

¿Cómo la tecnología nos ayuda?

Frano Capeta Mondoñedo
I-SEC Information Security, Director Regional

iSEC INFORMATION SECURITY INC. EDUCATION CENTER

Education Center

Cumplimiento Regulatorio

A que estamos obligados:

Sector Gobierno : NTP/ISO 17799:2007 EDI aprobada por resolución 246-2007 PCM 22/08/2007 (Internacionalmente ISO 27002)

Ley 28716 de control Interno de las entidades del estado
Resolución RC 320 Norma de control Interno (Contraloría)
Resolución RC 458 Guía para la implementación (Contraloría)

Sector Banca y Finanzas: Circular G-139-2009 Gestión de la continuidad del negocio
Circular G-140-2009 Gestión de la seguridad de la información

PCI – DSS v2.0 (Payment Card Industry – Data Security Standar)

Cumplimiento Regulatorio

Sector Gobierno : NTP/ISO 17799:2007 EDI aprobada por resolución 246-2007 PCM 22/08/2007 (Internacionalmente ISO 27002)

A5. Política de Seguridad
A6. Organización de Seguridad
A7. Administración de Activos
A8. Seguridad de los Recursos Humanos
A9. Seguridad Física y Ambiental
A10. Gestión de Comunicaciones y Operaciones
A11. Sistema de Control de Accesos
A12. Adquisición, Desarrollo y Mantenimiento de Sistemas de Inf.
A13. Administración de Incidentes de Seguridad de la Información
A14. Plan de Continuidad del Negocio
A15. Cumplimiento

Ley 28716 de control Interno de las entidades del estado y Resoluciones RC 320 y RC 458, como traducimos eso en términos de TI? COBIT

Planificación y organización

Adquisición e implementación

Entrega y soporte

Monitoreo

Education Center

Education Center

Sector Banca y Finanzas:
Circular G-139-2009 Gestión de la continuidad del negocio
Circular G-140-2009 Gestión de la seguridad de la información
PCI - DSS

Desarrollar y Mantener una Red Segura

Requisito 1:	Instalar y mantener una configuración de cortafuegos para proteger los datos de los tarjetahabientes.
Requisito 2:	No usar contraseñas del sistema y otros parámetros de seguridad provistos por los suplidores.

Proteger los Datos de los Tarjetahabientes

Requisito 3:	Proteger los datos de los tarjetahabientes que estén almacenados.
Requisito 4:	Encriptar los datos de los tarjetahabientes e información confidencial transmitida a través de redes públicas abiertas.

Mantener un Programa de Manejo de Vulnerabilidad

Requisito 5:	Usar y actualizar regularmente el software antivirus.
Requisito 6:	Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar Medidas Sólidas de Control de Acceso

Requisito 7:	Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
Requisito 8:	Asignar una Identificación única a cada persona que tenga acceso a un computador.
Requisito 9:	Restringir el acceso físico a los datos de los tarjetahabientes.

Monitorear y Probar Regularmente las Redes

Requisito 10:	Rastrear y monitorear todo el acceso a los recursos de la red y datos de los tarjetahabientes.
Requisito 11:	Probar regularmente los sistemas y procesos de seguridad.

Mantener una Política de Seguridad de la Información

Requisito 12:	Mantener una política que contemple la seguridad de la información

Dominio A11 Sistema de Control de Accesos

A 11.2.2 Gestión de privilegios

A 11.2.4 Revisión de los derechos de acceso de los usuarios

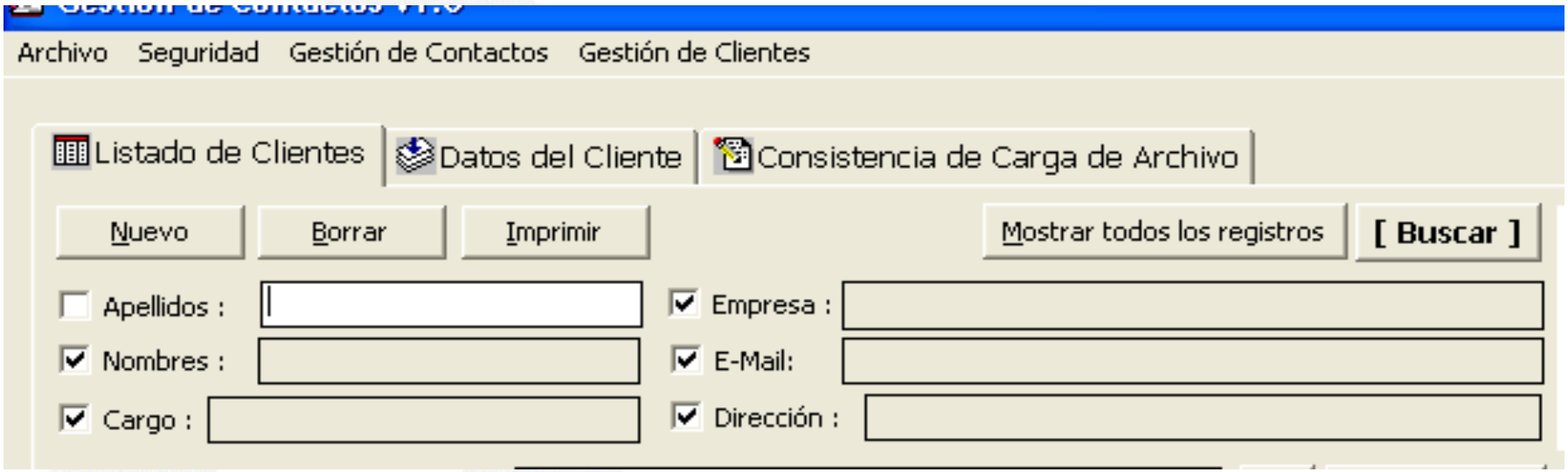
Situaciones que se presentan en relación a la implantación de estos controles

1) **Como controlamos los accesos del personal de TI**
   1) Situación concreta acceso del DBA a la(s) Bases de datos

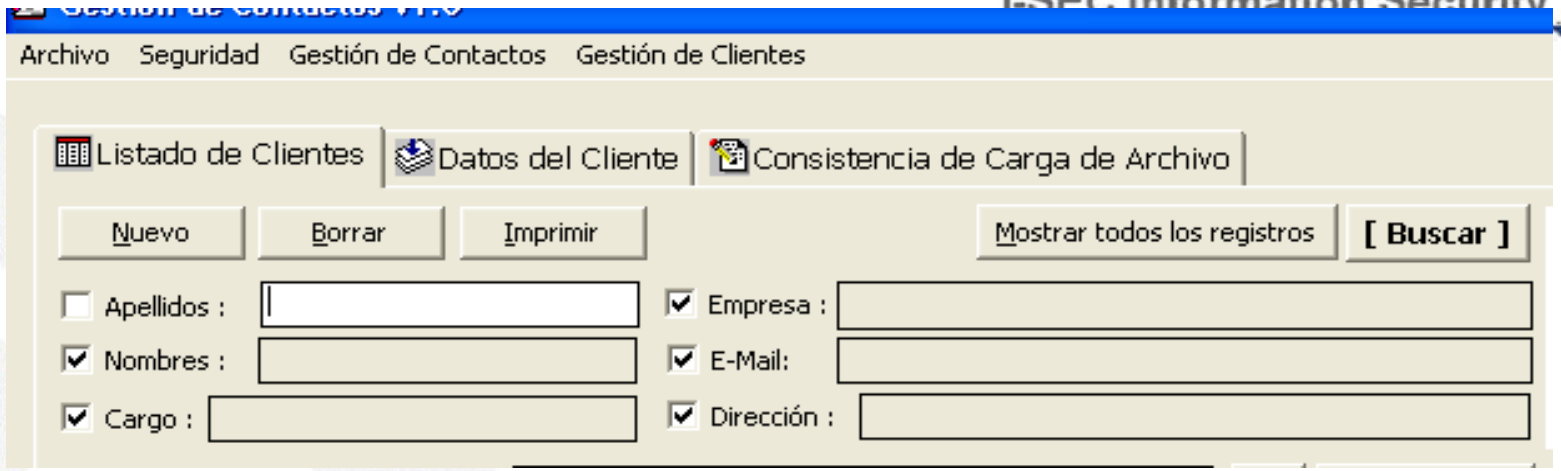
2) **Como controlo que las aplicaciones no accedan en forma indebida a las aplicaciones**
   1) Situación concreta 1 aplicaciones acceden en modo administrador a la base de datos
   2) Situación concreta 2 acceso oculto desde aplicaciones
   3) Situación concreta 3 SQL injection

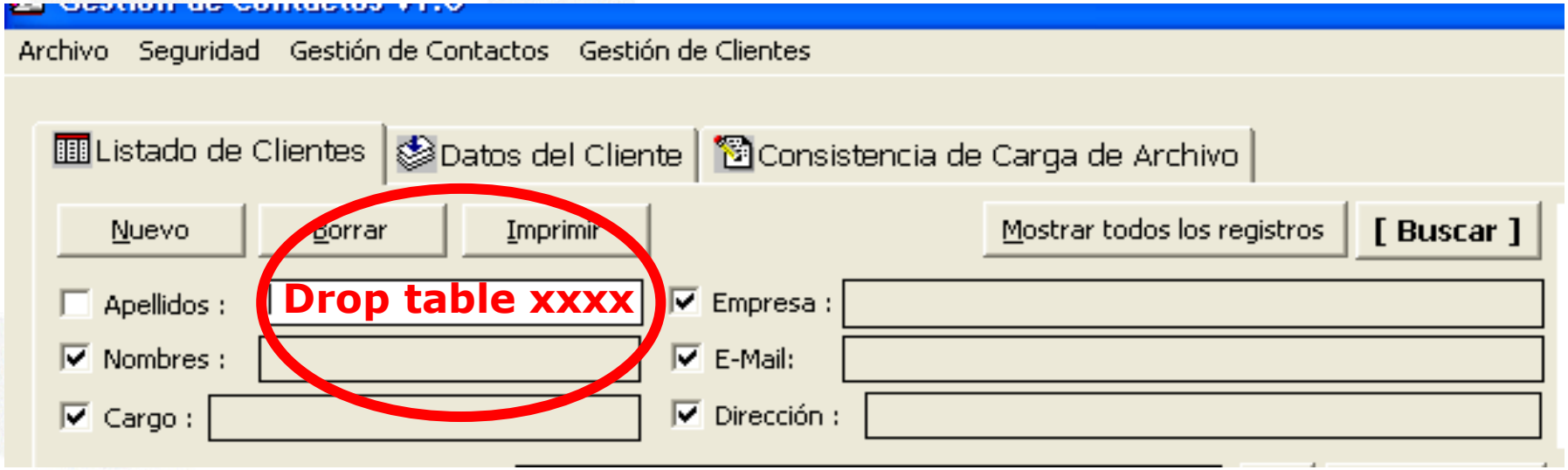
3) **Como mitigo y controlo el Phishing/Pharming/Keyloger**

Education Center



iSEC INFORMATION SECURITY INC. EDUCATION CENTER





Asumiendo que el siguiente código está en una aplicación web y que existe un parámetro "nombreUsuario" que contiene el nombre de usuario que nosotros le demos, la inyección SQL es posible:

consulta := "**SELECT * FROM usuarios WHERE nombre =** '" + **nombreUsuario** + "';"

malintencionado.

Asumiendo que el siguiente código está en una aplicación web y que existe un parámetro "nombreUsuario" que contiene el nombre de usuario que nosotros le demos, la inyección SQL es posible:

consulta := "**SELECT * FROM usuarios WHERE nombre =** '" + **nombreUsuario** + "';"

Si el usuario escribe su nombre, digamos "Alicia", nada anormal sucedería, la aplicación generaría una sentencia SQL similar a la siguiente, que es perfectamente correcta, en donde se seleccionaría al usuario "Alicia":

SELECT * FROM usuarios WHERE nombre = '**Alicia**';

malintencionado.

Asumiendo que el siguiente código está en una aplicación web y que existe un parámetro "nombreUsuario" que contiene el nombre de usuario que nosotros le demos, la inyección SQL es posible:

consulta := "**SELECT * FROM usuarios WHERE nombre =** '" + **nombreUsuario** + "';"

Si el usuario escribe su nombre, digamos "Alicia", nada anormal sucedería, la aplicación generaría una sentencia SQL similar a la siguiente, que es perfectamente correcta, en donde se seleccionaría al usuario "Alicia":

SELECT * FROM usuarios WHERE nombre = '**Alicia**';

Pero si un usuario malintencionado escribe como nombre de usuario:

"**Alicia**'; **DROP TABLE usuarios; SELECT * FROM datos WHERE '-' =** '-", se generaría la siguiente consulta SQL, (el color verde es lo que pretende el programador, el azul es el dato, y el rojo, el código SQL inyectado):

SELECT * FROM usuarios WHERE nombre = 'Alicia';
DROP TABLE usuarios;
SELECT * FROM datos WHERE '-' = '-';

La base de datos ejecutaría la consulta en orden, seleccionaría el usuario 'Alicia', borraría la tabla 'usuarios' y seleccionaría datos que quizá no están disponibles para los usuarios Web comunes. En resumen, cualquier dato de la base de datos está disponible para ser leído o modificado por un usuario malintencionado.

Dominio A10 Gestión de Comunicaciones y Operaciones

A 10.10.1 Registro de auditorias

A 10.10.2 Supervisión de uso del sistema

A 10.10.3 Protección de la información de registro

Situaciones que se presentan en relación a la implantación de estos controles

1) Se requieren activar pistas de auditorias, pero los sistemas críticos en forma nativa no lo implementan.
2) Como podemos monitorear los accesos a operaciones privilegiadas de intentos de accesos no autorizados a diversos recursos de los sistemas.
3) Como implantamos protección para el acceso y la manipulación de los registros.

Dominio A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

A 12.3 Controles Criptográficos

Requisito 3 y 4 PCI DSS

Es necesario identificar en base a un análisis de riesgos información almacenada que debe ser necesariamente protegida mediante adecuados sistemas de encriptación.

Dominio A12 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

A 12.4.2 Protección de los datos de prueba del sistema

Como implementamos un eficiente sistema de protección de la data que se pasa de producción a desarrollo

Dominio A15 Cumplimiento

A 15.1.3 Salvaguarda de los registros de la organización

Ok, ya sacamos el backup pero que pasa si se "pierde" la cinta…

Veamos un Demostración Practica