

PLAN PARA LA SEGURIDAD DE LOS SISTEMAS DE INFORMATICA

A. Introducción

La ACAA cuenta con una variedad de sistemas de información en las áreas de trabajo, que incluye: manejo de correspondencia; búsqueda de datos por Internet; preparación de cartas; adjudicación y pago de beneficios a lesionados; adjudicación y pago de servicios médicos y hospitalarios; proceso de recobro, procesamiento de la nóminas y el sistema financiero. Solamente el personal de la ACAA, debidamente autorizado, podrá utilizar estos sistemas para uso estrictamente oficial.

Todos los sistemas computadorizados están propensos al uso no autorizado y actividades de pirateo electrónico que están dirigidas hacer daño malicioso a los datos y buscar información confidencial del personal, lesionados, proveedores y suplidores. Es por esta razón que, se necesita implantar medidas de control para minimizar los accesos indebidos.

B. Propósito

El objetivo de este procedimiento es establecer medidas para minimizar el uso no autorizado de los sistemas computadorizados y prevenir el daño o acceso a información confidencial. Se establecerá un programa para auditar, monitorear, revisar y fiscalizar los sistemas de información para que se utilicen apropiadamente por el personal y controlar el acceso a los sistemas y al área de Informática, estrictamente para funciones relacionadas con el trabajo. Se adquirirán herramientas para minimizar los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada y/o maliciosa.

C. Normas Sobre el Uso

En la ACAA se han establecido las **Normas sobre el uso de los Sistemas Electrónicos** con el objetivo de que el personal que utiliza los sistemas computadorizados conozcan los deberes y obligaciones del uso de este recurso, para fines de su trabajo. Las normas establecen las penalidades por su violación respondiendo a la necesidad de garantizar que los sistemas se utilicen apropiadamente. Estas normas están publicadas en cada computadora y se muestran al personal luego de entrar el nombre del usuario y la contraseña. El sistema expone las normas de manera que el usuario las lea y confirme su lectura, obteniendo inmediatamente acceso al sistema computadorizado.

D. Análisis de Riesgo

Este Plan de Seguridad les aplica a todos los empleados de la ACAA, consultores y proveedores de servicios de tecnología. El plan tiene como propósito implantar controles que minimicen los riesgos de que los sistemas de informática dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada y/o maliciosa. El análisis de riesgo conlleva un inventario de activos de sistemas de informática e identificar las posibles amenazas contra los sistemas de informática. El Análisis de Riesgos es la base para desarrollar un Plan de Continuidad de los Negocios.

E. Inventario de Activos

El Inventario de Activos de Informática incluye los programas, sistemas, equipos, equipos y datos. Para fines de clasificar los activos de informática los vamos a dividir en Aplicaciones y Equipos. Esta nos facilita el concentrar todos los esfuerzos de seguridad en base a mantener la continuidad del negocio y nos ayuda a estar más capacitados para las situaciones que surjan. Al tener un inventario de los activos podemos establecer que es lo que vamos a proteger.

1. Inventario de las Aplicaciones - Oficina Central

Aplicación	Descripción
Aplicación ACAA21	Sistema ACAA21
Global Workflow	Sistema Global Workflow
InforGlobal MasterPiece	Sistema Financiero
InforGlobal PRMS	Sistema de Nomina
Aplicación GHAS	Sistema Pago Medico
Aplicación HTx	Aplicación Pago Medico HTx
MS Outlook	Mensajería
MS Explorer	Internet
MS Office	Sistema de Oficina
Comunicación	Red de Datos

2. Inventario de Equipo - Oficina Central

Equipo	Descripción
Servidor ACAA21	Servidor Central
Servidor Workflow	Servidor Central
ServidorAS400 PRMS-MP	Servidor Central
Servidor HTx	Servidor Central
Servidor MS Outlook	Servidor Central
Servidor Internet	Servidor Central
Servidor Office	Servidor Central
Comunicación	Red de Datos

3. Inventario de las Aplicaciones - Oficina Regional

Aplicación	Descripción
Aplicación ACAA21	Sistema ACAA21
Global Workflow	Aplicación Workflow
Comunicación	Red de datos
HTx (OR)	Sistema Pago Medico (OR)
HTx	Servidor Oficina Regional
MSOutlook	Mensajería
MSExplorer	Internet
MSOffice	Sistema de Oficina
MS SQL	Sistema de Aplicación

4. Inventario de Equipo - Oficina Regional

Equipo	Descripción
Servidor ACAA21	Servidor OR (1)
Servidor Workflow	
Comunicación	Red de datos
HTx	Servidor Oficina Regional
Servidor MSOutlook	Servidor OR
Servidor Internet	Servidor OR
Servidor Office	Servidor OR

F. Clasificar los Activos

Entre más importante es un activo existe una necesidad de mantenerlo operacional, o sea mantener su continuidad y por lo tanto el activo se convierte en uno más crítico. Entre más importante puede ser más vulnerable a posibles amenazas. Para esto, clasificamos los activos de acuerdo a su nivel de importancia. Las que requieren un mayor control, las distinguiremos como de Confidencialidad y cuán propensos están a un fallo lo identificamos como Amenazas.

1. Nivel de Importancia (P)

Al nivel de importancia le asignamos un valor o el indicador de cuán importante es el activo. El nivel de importancia lo identificamos con la **Prioridad** del activo. A la **Prioridad** le damos un valor de 1 al 3, el 1 con una prioridad mayor o más crítica, a una menor o menos crítica, que es 3.

2. Confidencialidad (C)

Para las aplicaciones y bases de datos es necesario distinguir cuáles requieren de un mayor control. Para esto se incluye otro factor en el que clasificamos los activos de acuerdo a su nivel de **Confidencialidad**. La

Confidencialidad de los datos indica cuales datos requieren de un mayor control y lo identificamos del 1 al 5, o sea que el 1 requiere una confidencialidad mayor y según aumenta el número la confidencialidad disminuye.

3. Posibles Amenazas (A)

Los equipos y aplicaciones están propensos para posibles amenazas y estas las identificamos como **Amenazas**. Las posibles **Amenazas** contra los sistemas y equipos las clasificamos por tipo: Robo (R), Desastres Naturales (D), Fallas de Equipo y Aplicación (F), Vandalismo (V), Virus (VI) y Acceso Indebido (A).

Presentamos más adelante los activos y se incluyen las tres columnas para clasificarlos. En la columna (P) se incluye la **Prioridad** que es la importancia, en la columna (C) se incluye la **Confidencialidad** y en la columna (A) las **Amenazas**.

G. Clasificación de Activos en Prioridad, Confidencialidad y Amenazas

1. Clasificar los Activos - Oficina Central

P	Aplicación/Equipo	Descripción	C	A
1	ACAA21	Sistema ACAA21	1	F,V,VI,A,D,R
1	ACAA21 Server	Servidor Central	5	F,V,R,D
1	Global Workflow	Servidor Central	5	F,V,R,D
1	MS Server	Sistema Operativo	1	F,V,VI,A,D,R
2	InforGlobal MasterPiece	Sistema Financiero	1	F,V,VI,A,D,R
2	AS400 Server	Servidor Central	5	F,V,R,D
2	InforGlobal PRMS	Sistema de Nomina	1	F,V,VI,A,D,R
2	AS400 Server	Servidor Central	5	F,V,R,D
2	GHIAS	Sistema Pago Medico	2	F,V,VI,A,D,R
2	AS400 GHIAS	Servidor Central	5	F,V,R,D
2	HTx	Sistema Pago Medico (IP)	2	F,V,VI,A,D,R
2	HTx Server	Servidor Central	5	F,V,R,D
2	Ley 159 (Recobro)	Sistema Recobro	2	F,V,VI,A,D,R
2	Beneficios Pagados	Sistema SVBPA	2	F,V,VI,A,D,R
2	Servidor	Servidor Central	5	F,V,R,D
3	MSOutlook	Mensajería	3	F,V,VI,A,D,R
3	Servidor MSOutlook	Servidor Central	5	F,V,R,D
3	MSExplorer	Internet	3	F,V,VI,A,D,R
3	Servidor Internet	Servidor Central	5	F,VA,R,D
3	MSOffice	Sistema de Oficina	4	F,V,VI,A,D,R
3	Servidor Office	Servidor Central	5	F,VA,R,D

2. Clasificar los Activos - Oficinas Regionales

P	Sistema/Equipo	Descripción	C	A
1	ACAA21	Sistema ACAA21	1	F,V,VI,A,D
1	ACAA21 Server	Servidor ACAA21 (1)	5	F,V,R,D
1	Global Workflow	Sistema Global Workflow	5	F,V,R,D
3	MS Server	Sistema Operativo (1,2)	5	F,V,VI,A,D
4	Sistema HTx	Sistema Pago Medico	1	F,V,VI,A,D
4	HTx Server	Servidor Pago Medico (1)	5	F,V,R,D
6	MSOutlook	Mensajería	4	F,V,VI,A,D
6	Servidor MSOutlook	Servidor (2)	5	F,V,R,D
5	MSExplorer	Internet	4	F,V,VI,A,D
5	Servidor Internet	Servidor (2)	5	F,V,R,D
7	MSOffice	Sistema de Oficina	5	F,V,VI,A,D.
7	Servidor Office	Servidor (2)	5	F,V,R,D.

Esto permite establecer qué es lo que se va a proteger (Confidencialidad) y cómo se van a proteger (los activos identificados).

H. Políticas de Seguridad

La política de seguridad es el mecanismo para establecer y divulgar directrices generales que permitan establecer controles adecuados en los sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información.

I. Medidas de Seguridad

1. Uso no autorizado de los sistemas computadorizados.
2. Proteger los sistemas y equipos contra daños maliciosos.
3. Proteger los equipos contra desastres naturales.
4. Proteger los sistemas contra daños maliciosos, accesos indebidos y aplicaciones tipo "virus".
5. Proteger los sistemas y equipos contra fallas.

J. Plan de Seguridad

1. Divulgación y orientación de normas de uso y protección de los sistemas tecnológicos.
2. Control de accesos para cada aplicación de acuerdo a los deberes y las responsabilidades del personal autorizado. Se efectuarán inspecciones periódicas para verificar su uso oficial.
3. Control de acceso a las áreas del centro de computas, equipos y red

de datos. Se efectuarán inspecciones periódicas para verificar su uso oficial.

4. Control de acceso a páginas de Internet. Se efectuarán inspecciones periódicas para verificar su uso oficial.
5. Controles generales de acceso para restringir horario de acceso a los recursos de informática.
6. Auditoría de Seguridad contra Intrusión.
7. Penetración Externa Desde el Internet.
8. Penetración por Acceso Remoto.
9. Seguridad de Aplicaciones del Web.
10. Pruebas de Vulnerabilidad Interna de Redes Internas.
11. Análisis de Seguridad de Redes.
12. Pruebas de Seguridad de aplicaciones de redes Internas.
13. Programas computadorizados para la protección.
14. Controles para el uso indebido de los sistemas y los equipos.
15. Controles para el uso de los sistemas.
16. Control de resguardo de datos.

K. Continuidad del Negocio.

El análisis de riesgo lo utilizamos de base para el desarrollo del plan de continuidad de negocio que incluye un plan para la recuperación de desastres y un plan para la continuidad de las operaciones del negocio.

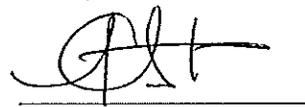
Recomendado por:


Epifanio Delgado Vázquez
Director Ejecutivo Auxiliar
Dirección de Informática

Fecha:

10/15/10

Aprobado por:


Julio Alicea Vasallo
Director Ejecutivo

Fecha:

10/15/2010