ANALISIS DE RIESGO RESPECTO A LA SEGURIDAD INFORMATICA DE UNA ORGANIZACIÓN CORRESPONDIENTE AL SECTOR PÚBLICO 3RA. PARTE

TECNOLOGÍA

SUSANA NOEMÍ TOMASI

TABLA DE VULNERABILIDADES – PROBABILIDAD OCURRENCIA – IMPACTO

ACTIVO	SISTEMA INFORMATICO	VULNERABILIDAD	FUENTE DE LA AMENAZA	ACCIONES DE LA AMENAZA	PROBABILIDAD OCURRENCIA	IMPACTO
BASE DE DATOS CENTRAL	CONTABLE-IMPOSITIVA – PERSONAL – DE USUARIOS – DE PROVEEDOR	FALLA EN LA SEGURIDAD – CONFIGURACIÓN NO ADECUADA – BAJA PROTECCIÓN ACCESOS – FALLA EN EL SISTEMA OPERATIVO	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO	MEDIA (SE ESTA TERMINANDO DE IMPLEMENTAR TODOS LOS SISTEMAS DE CONTROL)	ALTO
BASE DE DATOS PRESTACIONES	PRESTACIONES-TRAMITES-CIUDADANOS	FALLA EN LA SEGURIDAD – CONFIGURACIÓN NO ADECUADA – BAJA PROTECCIÓN ACCESOS – FALLA EN EL SISTEMA OPERATIVO	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO	MEDIA (SE ESTA TERMINANDO DE IMPLEMENTAR TODOS LOS SISTEMAS DE CONTROL)	ALTO
PAGINA WEB INSTITUCIONAL	PRESTACIONES	FALLA EN LA SEGURIDAD – CONFIGURACIÓN NO ADECUADA – BAJA PROTECCIÓN ACCESOS – FALLA EN EL HOSTING	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO	ALTA (EL PROVEEDOR NO CUENTA CON LOS CONTROLES SUFICIENTES)	ALTO
LOGS DE AUDITORIA	SISTEMAS CENTRAL Y DE PRESTACIONES	FALTA DE SEGURIDAD EN EL ACCESO FISICO – FALTA DE UN SISTEMA DE	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO	ACCESO NO AUTORIZADO-INTERRUPCION DEL PROCESAMIENTO	BAJO (TODOS EQUIPOS TIENEN ACTIVADOS LOS LOGS DE	MEDIO

		DETECCIÓN DE INCENDIOS E INUNDACIONES – FALTA DE ESTABILIZADORES – FALLAS EN LA SEGURIDAD DEL SISTEMA OPERATIVO	– CORTE DE ENERGIA – INCENDIO – INUNDACIÓN -	– PERDIDA DE INFORMACIÓN -	AUDITORIA)	
CINTAS BACK UPS	SISTEMAS CENTRAL Y DE PRESTACIONES	FALTA DE SEGURIDAD EN EL ACCESO FISICO – FALTA DE UN SISTEMA DE DETECCIÓN DE INCENDIOS E INUNDACIONES – FALTA DE ESTABILIZADORES – FALLAS EN LA SEGURIDAD DEL SISTEMA OPERATIVO	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA – INCENDIO – INUNDACIÓN -	ACCESO NO AUTORIZADO- INTERRUPCION DEL PROCESAMIENTO – PERDIDA DE INFORMACIÓN -	BAJO (SA REALIZAN BACK UPS POR SEMANA DE TODOS LOS PROCESOS)	ALTO (POR PERDIDA DE INFORMACION)
SERVIDOR DE MAILS		FALTA DE SEGURIDAD EN EL ACCESO FISICO – FALTA DE UN SISTEMA DE DETECCIÓN DE INCENDIOS E INUNDACIONES – FALTA DE ESTABILIZADORES – FALLAS EN LA SEGURIDAD DEL SISTEMA OPERATIVO	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA – INCENDIO – INUNDACIÓN - HACKERS	ACCESO NO AUTORIZADO- INTERRUPCION DEL PROCESAMIENTO – PERDIDA DE INFORMACIÓN -	MEDIA (ALTA IMPLEMENTAR MEDIDAS DE SEGURIDAD)	ALTA

TABLA DE CONTROLES

ACTIVO	SISTEMA INFORMATICO	REQUISITOS DE SEGURIDAD	CONTROL	IMPLEMENTADO	TIPO DE CONTROL
BASE DE DATOS CENTRAL	CONTABLE-IMPOSITIVA – PERSONAL – DE USUARIOS – DE PROVEEDOR	CONTROL DE ACCESO LÓGICO – CONTROL DE ACCESO A USUARIOS-RESGUARDO DE LA INFORMACIÓN-PROCESAMIENTO ININTERRUMPIDO DE LA INFORMACION	LOGIN – BACK UPS-LOGS DE AUDITORIA – ENTORNO ALTERNATIVO DE PROCESAMIENTO DE LOS SISTEMAS	PARA EL ENTORNO ALTERNATIVO DE PROCESAMIENTO DE LOS SISTEMAS SE LLAMO A LICITACIÓN – EL RESTO SE ENCUENTRA IMPLEMENTADO	TÉCNICO PREVENTIVO
BASE DE DATOS PRESTACIONES	PRESTACIONES-TRAMITES-CIUDADANOS	CONTROL DE ACCESO LÓGICO – CONTROL DE ACCESO A USUARIOS-RESGUARDO DE LA INFORMACIÓN-PROCESAMIENTO ININTERRUMPIDO DE LA INFORMACION	LOGIN – BACK UPS-LOGS DE AUDITORIA – ENTORNO ALTERNATIVO DE PROCESAMIENTO DE LOS SISTEMAS	PARA EL ENTORNO ALTERNATIVO DE PROCESAMIENTO DE LOS SISTEMAS SE LLAMO A LICITACIÓN – EL RESTO SE ENCUENTRA IMPLEMENTADO	TÉCNICO PREVENTIVO
PAGINA WEB INSTITUCIONAL	PRESTACIONES	PROCESAMIENTO ININTERRUMPIDO DE LA INFORMACION	ENTORNO ALTERNATIVO DE PROCESAMIENTO DE LOS SISTEMAS	SE ENCUENTRA EN TRATATIVAS CON EL PROVEEDOR DEL HOSTING	TÉCNICO PREVENTIVO
LOGS DE AUDITORIA	SISTEMAS CENTRAL Y DE PRESTACIONES	QUE SE ENCUENTREN OPERATIVOS	VERIFICACIÓN DE LOS MISMOS	SI	TÉCNICO PREVENTIVO
CINTAS BACK UPS	SISTEMAS CENTRAL Y DE PRESTACIONES	QUE SE REALICEN EN EL TIEMPO OPORTUNO	VERIFICACIÓN DE LOS MISMOS	SI	TÉCNICO PREVENTIVO
SERVIDOR DE MAILS		ACCESO RESTRINGIDO DESDE INTERNET – CONTROL DEL ACCESO FÍSICO – ACTUALIZACIONES DEL SISTEMA OPERATIVO	FIREWALLS – ANTIVIRUS – ANTISPAM – CLAVES ESPECIALES – REVISIONES PERIODICAS	SI	TÉCNICO PREVENTIVO

TABLA DE RIESGOS

ACTIVO	SISTEMA INFORMATICO	VULNERABILIDAD	FUENTE DE LA AMENAZA	INCIDENTE	CONSECUENCIA	PROB OCUR	IMPACTO	RIESGO
BASE DE DATOS CENTRAL	CONTABLE-IMPOSITIVA – PERSONAL – DE USUARIOS – DE PROVEEDOR	FALLA EN LA SEGURIDAD – CONFIGURACIÓN NO ADECUADA – BAJA PROTECCIÓN ACCESOS – FALLA EN EL SISTEMA OPERATIVO	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO – ACCESO A LOS ARCHIVOS DEL SISTEMA O DE LA BASE DE DATOS –	MODIFICACIONES A DATOS O ROBO DE INFORMACION	MEDIO	ALTO	MEDIO
BASE DE DATOS PRESTACIONES	PRESTACIONES-TRAMITES-CIUDADANOS	FALLA EN LA SEGURIDAD – CONFIGURACIÓN NO ADECUADA – BAJA PROTECCIÓN ACCESOS – FALLA EN EL SISTEMA OPERATIVO	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO – ACCESO A LOS ARCHIVOS DEL SISTEMA O DE LA BASE DE DATOS –	MODIFICACIONES A DATOS O ROBO DE INFORMACION	MEDIO	ALTO	MEDIO
PAGINA WEB INSTITUCIONAL	PRESTACIONES	FALLA EN LA SEGURIDAD – CONFIGURACIÓN NO ADECUADA – BAJA PROTECCIÓN ACCESOS – FALLA EN EL HOSTING	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	DETERIORO DE LA PÁGINA O NO ACCESO A LA MISMA PARA LOS CIUDADANOS Y USUARIOS DEL ORGANISMO	PERDIDA DE IMAGEN – MODIFICACIÓN O ROBOS DE CIUDADANOS O DE LAS PRESTACIONES DEL ORGANISMO	ALTO	ALTO	ALTO
LOGS DE AUDITORIA	SISTEMAS CENTRAL Y DE PRESTACIONES	FALTA DE SEGURIDAD EN EL ACCESO FISICO – FALTA DE UN SISTEMA DE DETECCIÓN DE INCENDIOS E INUNDACIONES – FALTA DE ESTABILIZADORES – FALLAS EN LA SEGURIDAD DEL SISTEMA	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA – INCENDIO – INUNDACIÓN -	ANULACIÓN DE LOS LOGS DE AUDITORIA – CORTE DE ENERGIA – INCENDIO - INUNDACION	PERDIDA DE INFORMACIÓN Y DE EQUIPAMIENTO	BAJA	MEDIO	BAJO

		OPERATIVO						
CINTAS BACK UPS	SISTEMAS CENTRAL Y DE PRESTACIONES	FALTA DE SEGURIDAD EN EL ACCESO FISICO – FALTA DE UN SISTEMA DE DETECCIÓN DE INCENDIOS E INUNDACIONES – FALTA DE ESTABILIZADORES – FALLAS EN LA SEGURIDAD DEL SISTEMA OPERATIVO	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA – INCENDIO – INUNDACIÓN -	ROBO DE CINTAS- DESTRUCCIÓN DE CINTAS POR INCENDIO INUNDACIÓN O DAÑO INTENCIONAL	PERDIDA DE INFORMACIÓN Y DE EQUIPAMIENTO	BAJA	MEDIO	BAJO
SERVIDOR DE MAILS		FALTA DE SEGURIDAD EN EL ACCESO FISICO – FALTA DE UN SISTEMA DE DETECCIÓN DE INCENDIOS E INUNDACIONES – FALTA DE ESTABILIZADORES – FALLAS EN LA SEGURIDAD DEL SISTEMA OPERATIVO	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA – INCENDIO – INUNDACIÓN - HACKERS	EJECUCIÓN DE PROGRAMAS ESPIAS O DESTRUCTIVOS- ACCESO A TRAVÉS DE LA CONSOLA – CORTE DE ENERGIA – INCENDIO - INUNDACION	PERDIDA DE INFORMACIÓN – ACCESOS NO AUTORIZADO A LA INFORMACIÓN CONFIDENCIAL DEL ORGANISMO – INTERRUPCION DE LA OPERATORIA	BAJO	ALTO	BAJO

3. REUNION DEL COMITÉ DE SEGURIDAD – MODIFICACIONES DETERMINADAS Y JUSTIFICACIÓN DE LAS MISMAS:

El comité entiende que la información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida, de una amplia gama de amenazas, y a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Tal como se especifica en el modelo PSI_Modelo-v1_200507, de la Oficina Nacional de Tecnología de la Información, el comité entiende que seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad, de manera tal que se garantice que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma.

- Integridad, a fin de salvaguardar la exactitud y totalidad de la información y loos métodos de procesamiento.

- Disponibilidad, para garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

- Autenticidad, a fin de asegurar la validez de la información en tiempo, forma y distribución, garantizando el origen de la información, validando el emisor para evitar suplantación de identidades.

- Aceptación de que todos los eventos de un sistema deben poder ser registrados a fin de su control posterior, por medio de la auditoria correspondiente.

- Protección a la duplicación, de manera tal que una transacción solo se realiza una vez, a menos que se especifique lo contrario, de forma de impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- No repudio, respecto a información que la organización haya enviado o recibido de terceros, evitando que éstos aleguen que no la enviaron o no la recibieron.

- Legalidad, respecto al cumplimiento por parte del Organismo de las leyes, normas, reglamentaciones o disposiciones vigentes.

- Confiabilidad de la información generada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Resoluciones respecto a los temas tratados en la reunión anterior:

1. Se decide efectuar el desarrollo de Políticas de Seguridad de la Información, a través de un conjunto de reglas que formarán parte de las Políticas de Seguridad de la Información a fin de proteger al Organismo de una amplia gama de amenazas, y a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

2. Se decide mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

3. Se decide la creación de la Sub -gerencia de Seguridad Informática del Organismo, que estará a cargo del actual Jefe de Sistemas Administrativos, quien será nombrado por la resolución correspondiente, se le otorgarán 3 personas dentro de los recursos disponibles del sector de sistemas del Organismo, ya que por la Decisión Administrativa 699/2004, no se puede incrementar el presupuesto disponible.

4. Se decide la implementación en forma urgente de medidas tendientes a disminuir los riesgos determinados según las distintas tablas efectuadas y llevar adelante la implementación de un nuevo contrato con el proveedor de hosting, a fin de que la seguridad de la página WEB del Organismo que es crítica, se vea solucionada.

5. Se va a completar la licitación de un entorno alternativo para el procesamiento de los sistemas en caso de falla de los mismos.

6. Se decide además verificar el riesgo real de incendios e inundaciones, que afecten a los sistemas de información y su procesamiento.

CONSIDERACIONES FINALES:

Efectuar el análisis del riesgo que tiene una organización respecto de la seguridad informática no es una tarea sencilla, pero debería llevarse a cabo para prevenir eventos que afecten la seguridad de la empresa de que se trate, en el caso ejemplo una organización estatal, pero adaptable a cualquier organización.

Es preferible anticiparse a sucesos que afecten a la seguridad informática antes de que ocurra algún hecho que afecte el normal desempeño de los sistemas de las organizaciones y que impliquen dejar de operar por algún tiempo que significan costos mucho mayores que los que se necesitan para efectuar éste análisis.

Implementar un comité de seguridad, en la organización, contar con un sector de seguridad informática acorde con el nivel de la organización de que se trate, si bien años atrás no parecía necesario, hoy es imprescindible.

Debemos tomar conciencia de que ninguna empresa funciona en la actualidad sin sistemas informáticos, y que los mismos deben contar con las medidas de seguridad apropiadas, para su buen funcionamiento.