ANALISIS DE RIESGO RESPECTO A LA SEGURIDAD INFORMATICA DE UNA ORGANIZACIÓN CORRESPONDIENTE AL SECTOR PÚBLICO2DA. PARTE

TECNOLOGÍA

SUSANA NOEMÍ TOMASI

3. RELEVAMIENTO DE LOS SISTEMAS INFORMATICOS.

La sub gerencia de sistemas ordena el relevamiento y la clasificación de los sistemas informáticos, con el armado de una planilla con el nivel de riesgo e importancia que poseen:

El Organismo cuenta con un sistema propio, denominado PRESTACIONES: diseñado por el personal de sistemas del mismo para las prestaciones que realiza y la información personal de los ciudadanos y de trámites que éstos realizan en el organismo, esto se encuentra integrado en una base de datos única, modulada, a la que los ciudadanos acceden a través de la página WEB del organismo, que se encuentra tercerizada a través de un proveedor de hosting, y el personal del Organismo encargado del área de prestaciones.

Además cuenta con un sistema Contable impositivo, de personal y proveedores, denominado CENTRAL: al que tienen acceso el personal del organismo, a través de perfiles y autorizaciones, que fue diseñado por el sector de sistemas del Ministerio del que el Organismo depende, y adaptado por el personal de sistemas del Organismo a las necesidades del mismo.

No se encuentran integradas las bases de datos de los dos sistemas, y utilizan una interface diseñada a tal efecto cuando necesitan actualizar información de una base de datos a otra, como ser los usuarios del sistema.

El personal de un área no tiene posibilidades de acceder al área no correspondiente, excepto, a nivel sub- gerencial y gerencial, el director, y el personal de sistemas, con el que cuenta el Organismo.

ACTIVO	SISTEMA INFORMATICO	INFORMACIÓN QUE CONTIENE	CONF.	INTEG.	DISP.	CRITICIDAD
BASE DE DATOS CENTRAL	CONTABLE-IMPOSITIVA	Abarca la contabilidad, y los estados contables	0	5	2	BAJA
	PERSONAL	Abarca a todo el personal del Organismo, aún los por contrato, como los que tiene el Estado	5	5	3	MEDIA
	DE USUARIOS	Contiene las claves de acceso de los usuarios del sistema- perfiles y autorizaciones	5	5	5	ALTA
	DE PROVEEDOR.	Contiene los datos de los proveedores del Estado autorizados, las licitaciones en trámite, terminadas, y el archivo de materiales	5	5	3	MEDIA
BASE DE DATOS PRESTACIONES	PRESTACIONES-TRAMITES-CIUDADANOS	Abarca los tramites en curso, los que ingresan al Organismo y los	5	5	5	ALTA

		terminados				
MANUAL DE PROCEDIMIENTOS OPERATIVOS DEL ORGANISMO	SISTEMAS CENTRAL Y DE PRESTACIONES	Abarca todo el procedimiento administrativo del organismo	0	3	0	BAJA
PAGINA WEB INSTITUCIONAL	PRESTACIONES	Abarca la información institucional y de tramitaciones del Organismo, su manejo se encuentra tercerizado	0	3	4	MEDIA
LOGS DE AUDITORIA	SISTEMAS CENTRAL Y PRESTACIONES	Contiene la información respecto a las actividades realizadas por los usuarios en los sistemas	2	5	2	MEDIA
CINTAS BACK UPS	SISTEMAS CENTRAL Y PRESTACIONES	Contiene los back ups de la información de ambos sistemas	4	5	2	BAJA
SERVIDOR DE MAILS		Contiene los mails de todo el personal del Organismo	5	5	5	ALTA

Justificaciones:

La evaluación de los sistemas se efectúa dándoles valores de 0 a 5, a Confidencialidad – Integridad y Disponibilidad, calculando la Criticidad de no contar con dicho sistema por determinado tiempo (llámese minutos, horas o días).

1. La información contable – impositiva del Organismo, debe ser pública, y puede estar en conocimiento

de los ciudadanos, y del personal del organismo, lo que no significa que cualquier usuario tenga acceso al sistema para efectuar modificaciones al mismo. Debe mantenerse completa, y la disponibilidad es relativa, ya que no se produciría un gran impacto en el Organismo por dejar de contar por unas horas sin el sistema contable-impositivo, por eso la criticidad es media.

2. La información del personal del Organismo debe ser confidencial, en cumplimiento además de la normativa respecto a la misma, debe mantenerse completa, y la disponibilidad es relativa, ya que no se produciría un gran impacto en el Organismo por dejar de contar por unas horas sin el sistema de personal, excepto cuando se efectúan las liquidaciones del mismo, por eso la criticidad es media.

3. La información respecto a los usuarios de todos los sistemas del Organismo debe ser confidencial, integra y debe estar disponible para que todos los usuarios tengan acceso diariamente a los sistemas para los sistemas a los que están autorizados a acceder, por lo cual el nivel de criticidad es Alto.

4. La información respecto a los proveedores, debe ser confidencial e integra, porque si personas no autorizadas tienen acceso a la misma, las licitaciones podrían ser dirigidas indebidamente, pero el nivel de disponibilidad es medio, ya que se puede estar sin sistema por unas horas.

5. La información del sistema de prestaciones, es altamente confidencial, ya que contiene la base de datos de los ciudadanos que acceden al sistema, debe mantenerse la exactitud y totalidad de la información y debe estar disponible en todo momento, por lo cual el grado de criticidad es Alto.

6. El manual de procedimientos operativos del organismo, es de acceso público, debe estar íntegro, y si no se encuentra disponible en forma permanente , no trae conflictos graves, por lo cual la criticidad es Baja.

7. La página WEB institucional, se utiliza para brindar información a los ciudadanos, respecto a las prestaciones a las que pueden acceder y para que comiencen las tramitaciones, pedido de informes, reserva de números y seguimiento de trámites, por lo cual el nivel de confidencialidad de la página es innecesario (la confidencialidad se encuentra en el sistema de prestaciones), debe estar con la información correcta y disponible para su uso, pero no tiene un grado de criticidad grande, por lo cual es Media.

8. Los logs de auditoria, son medianamente confidenciales, ya que pocos si accedieran a los mismos, podrían leerlos y comprenderlos, deben mantenerse completos y disponibles, para el caso de eventos, por lo cual tiene un nivel de criticidad Medio.

9. Las cintas de back ups, son confidenciales, deben mantenerse completas y disponibles, para el caso de eventos, por lo cual tiene un nivel de criticidad Medio.

10. Y por último, el servidor de mails del personal del organismo, debe ser confidencial y contener la totalidad de la información, y debe estar disponible en forma permanente, ya que el organismo se comunica interna y externamente en la actualidad a través de este medio, por lo cual la criticidad es Alta.

4. CONTINGENCIAS QUE PUEDAN SURGIR POR EL CONTRATO CON TERCEROS:

Se determina que el contrato con la empresa, deberá contener las siguientes cláusulas:

a. Una cláusula de confidencialidad, respecto a la información del Organismo y de los Ciudadanos a la que acceda el proveedor del servicio y sus empleados, que deberá continuarse una vez finalizado el contrato con el Organismo y si éste no se renovara.

b. Respecto a las políticas de seguridad de la información del Organismo, para cuando estén dictadas, conocimiento y cumplimiento de las mismas, para la empresa y su personal a cargo, en los aspectos que le sean aplicables.

c. Respecto a la calidad del servicio, determinar claramente las pautas con que deben contar los proveedores del mismo, respecto a los enlaces provistos como para el mantenimiento del sitio WEB del Organismo.

d. Pautas para el tratamiento de incidentes de seguridad, que va a estar detallado en el manual de políticas de seguridad.

e. Existencia de planes de contingencia ante interrupciones de los servicios.

f. Mantenimiento de la página WEB.

g. Propiedad intelectual del Organismo sobre el sitio WEB hosteado por el proveedor.

h. Definiciones relacionadas con la protección y el tratamiento de los datos ubicados en la base de datos.

i. Que el Organismo pueda verificar los controles existentes a los accesos físicos de las instalaciones del proveedor, donde se ubican los equipos que prestan el servicio de hosting del sitio WEB del Organismo, por parte de los empleados del proveedor.

j. Pautas de administración y de control de acceso lógico implementadas en el equipamiento de comunicaciones que hostea el sitio WEB del Organismo.

k. Medidas de seguridad, como ser Antivirus, Firewall, control de acceso, etc., implementadas en el equipamiento que hostea el sitio WEB del Organismo.

l. Criterios de monitoreo y control de los servicios prestados.

m. Responsabilidades relativas a la instalación y mantenimiento del hardware, software y los servicios, relativos al sitio WEB del Organismo.

5. EVALUACIÓN DEL RIESGO:

a. TABLA DE AMENAZAS

ACTIVO	**SISTEMA INFORMATICO**	**AMENAZA FUENTE**	**ACCIONES DE LA AMENAZA**	**MOTIVACION**	**CAPACI-DAD**
BASE DE DATOS CENTRAL	CONTABLE-IMPOSITIVA – PERSONAL – DE USUARIOS – DE PROVEEDOR	HACKERS-PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS	INGENIERIA SOCIAL – INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO	POPULARIDAD-DINERO – OBTENCIÓN DE DATOS – EMPLEADO DESPECHADO	TÉCNICAS DE HASHING – EQUIPOS DE PROFESIONALES-CONOCIMIENTOS DE PROGRAMACIÓN ETC.
BASE DE DATOS	PRESTACIONES-	HACKERS-	INGENIERIA	POPULARIDAD-	TÉCNICAS DE

PRESTACIONES	TRAMITES-CIUDADANOS	PENETRACIÓN – PERDIDA DE INFORMACIÓN-USUARIOS INTERNOS -	SOCIAL – INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO	DINERO – OBTENCIÓN DE DATOS – EMPLEADO DESPECHADO	HASHING – EQUIPOS DE PROFESIONALES-CONOCIMIENTOS DE PROGRAMACIÓN ETC.
PAGINA WEB INSTITUCIONAL	PRESTACIONES	HACKERS-PENETRACIÓN USUARIOS INTERNOS - DESPRESTIGIO	INGENIERIA SOCIAL – INTRUSIÓN-ACCESO NO AUTORIZADO – CODIGO MALICIOSO	POPULARIDAD-DINERO – OBTENCIÓN DE DATOS – EMPLEADO DESPECHADO	TÉCNICAS DE HASHING – EQUIPOS DE PROFESIONALES-CONOCIMIENTOS DE PROGRAMACIÓN ETC.
LOGS DE AUDITORIA	SISTEMAS CENTRAL Y DE PRESTACIONES	USUARIOS INTERNOS – INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA	ACCESO NO AUTORIZADO-INTERRUPCION DEL PROCESAMIENTO – PERDIDA DE INFORMACIÓN -	EMPLEADO DESPECHADO – BORRAR EVIDENCIA - DESPERFECTO	PROFESIONALES-CONOCIMIENTOS DE PROGRAMACIÓN – FALLA DEL SISTEMA
CINTAS BACK UPS	SISTEMAS CENTRAL Y DE PRESTACIONES	USUARIOS INTERNOS INTERRUPCION DEL PROCESAMIENTO – CORTE DE ENERGIA	ACCESO NO AUTORIZADO INTERRUPCION DEL PROCESAMIENTO – PERDIDA DE INFORMACIÓN -	EMPLEADO DESPECHADO – BORRAR EVIDENCIA - DESPECFECTO	PROFESIONALES-CONOCIMIENTOS DE PROGRAMACIÓN – FALLA DEL SISTEMA
SERVIDOR DE MAILS		INCENDIO - INUNDACION	INTERRUPCION DEL PROCESAMIENTO – PERDIDA DE INFORMACION	DESPECFECTO	FALLA DEL SISTEMA