

Actividad 1:

Análisis y gestión de riesgos de una
instalación IT

Kalio Fernando O'Farril Villalpando

Ciberseguridad Web

Grupo 2001

Configuración

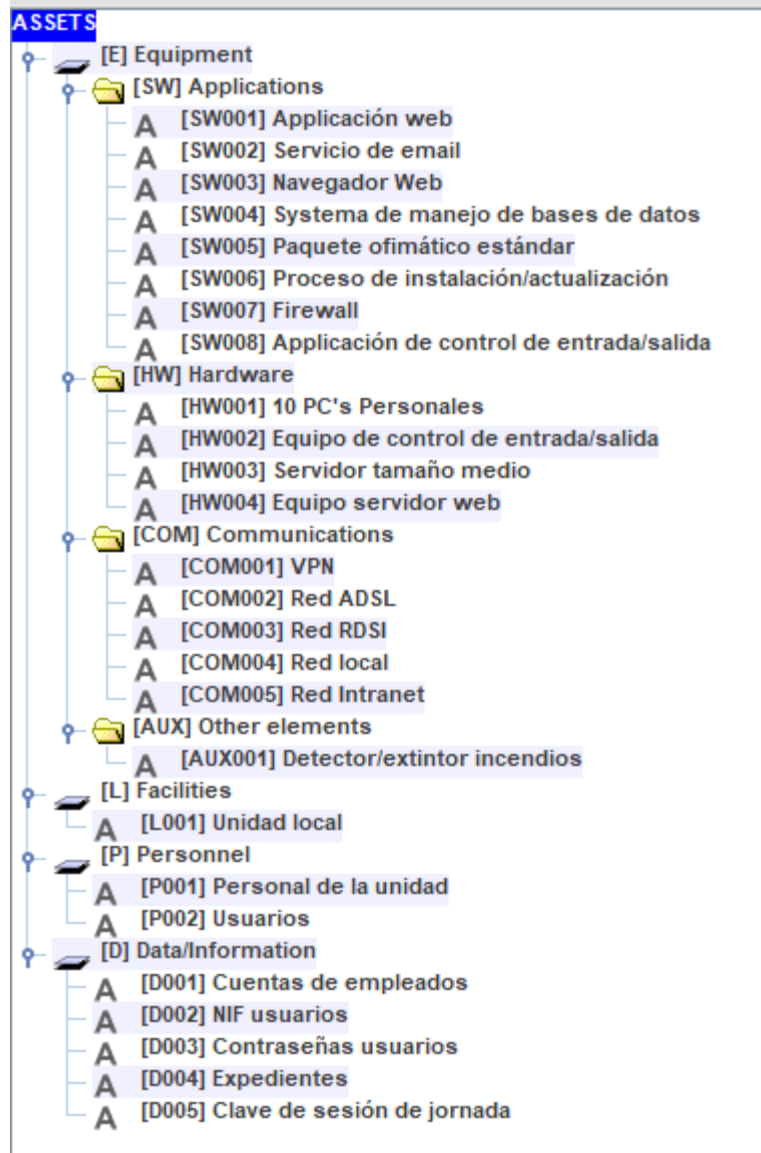
En este documento se lleva a cabo el análisis de riesgo de un servicio público del estado. El alcance del proyecto es el servicio de tramitación electrónica: presencial y remota. Se hará el estudio de la información que se maneja y del equipamiento (equipos y redes de comunicación) usadas.

El proyecto se divide en 3 fases: la fase inicial que plantea la situación actual del servicio y las fases Intermedia1 e Intermedia2 en donde progresivamente se buscará acercarnos lo más posible a lo que se denomina el “target” i.e. la meta. Es importante recalcar que el nombre de meta puede ser engañoso ya que aquí se emplea como el escenario ideal. No en todos los rubros descritos aquí se llegará al escenario ideal puesto que llegar a ello puede involucrar un mayor uso de tiempo y de recursos.

Los objetivos de este análisis es primeramente identificar y clasificar todos los activos relacionados al alcance del proyecto: información y equipamiento. Una vez clasificados, por cuestiones de no ser repetitivos se seleccionan los activos esenciales o aquellos cuyo escenario puede ser muy parecido a los de otros activos. Se valorará el activo basándose en el nivel de impacto que podría generar a la organización al ser víctima de alguna posible amenaza y finalmente se describirá un plan de salvaguarda distribuido en las dos fases intermedias del proyecto para acercarnos lo más posible al escenario ideal.

Activos

Los activos identificados fueron catalogados en cuatro distintas categorías: equipamiento, facilidades, personal y datos/información. De estas categorías la más extensa es la de equipamiento, la cual fue separada en otras cuatro categorías: aplicaciones, hardware, comunicaciones y otras. En la siguiente imagen se muestran los activos y sus respectivas clasificaciones.



No todos los activos aquí catalogados son esenciales, inclusive hay algunos que podrían caer en redundancia debido a su estrecha relación y dependencia entre sí. Por lo mismo se hará la valoración y planes de salvaguardas para solo aquellos que sean cruciales para la operación y tengan escenarios distintos a los que ya se hayan detallado.

Los activos considerados esenciales son:

- Aplicación Web
- Servicio de email
- Firewall
- Pc's personales
- Servidor tamaño medio

- Equipo servidor web
- VPN
- Red local
- Expedientes

El resto de los activos, aunque importantes pueden ser redundantes ante las descripciones y mitigaciones.

Valoración de los activos

A continuación, se muestra una imagen en donde se ha hecho la valoración de los activos considerados como esenciales en la herramienta PILAR.

asset	[A]	[I]	[C]	[Auth]	[Acc]	[PD]
ASSETS						
[E] Equipment						
[SW] Applications						
A [SW001] Aplicación web	[10]	[9]	[9]	[6]	[9]	[9]
A [SW002] Servicio de email	[5]	[9]	[9]	[9]	n.a.	[7]
A [SW003] Navegador Web						
A [SW004] Systema de manejo de bases de datos						
A [SW005] Paquete ofimático estándar						
A [SW006] Proceso de instalación/actualización						
A [SW007] Firewall	[10]	n.a.	[7]	n.a.	n.a.	n.a.
A [SW008] Aplicación de control de entrada/salida						
[HW] Hardware						
A [HW001] 10 PC's Personales	[1]	[1]	[2]	[1]	[2]	[2]
A [HW002] Equipo de control de entrada/salida	[3]	[1]	[2]	[2]	[1]	[1]
A [HW003] Servidor tamaño medio	[5]	[5]	[5]	[5]	n.a.	[5]
A [HW004] Equipo servidor web	[10]	[7]	[9]	[9]	[9]	[9]
[COM] Communications						
A [COM001] VPN	[10]	[6]	[6]	[6]	n.a.	[6]
A [COM002] Red ADSL						
A [COM003] Red RDSI						
A [COM004] Red local	[5]	n.a.	n.a.	n.a.	n.a.	n.a.
A [COM005] Red Intranet						
[AUX] Other elements						
[L] Facilities						
[P] Personnel						
[D] Data/Information						
A [D001] Cuentas de empleados						
A [D002] NIF usuarios						
A [D003] Contraseñas usuarios						
A [D004] Expedientes	[5]	[5]	[5]	n.a.	n.a.	n.a.
A [D005] Clave de sesión de jornada						

La explicación para dichas valoraciones se lista a continuación:

- **Aplicación Web:** En cuanto a disponibilidad, la aplicación web recibió un puntaje de 7 por la amenaza de causar una mayor interrupción de actividades en la organización con impacto en otras organizaciones, ya que si la aplicación web no está disponible se frena todo el proceso, tanto en la planta local como en las actividades de usuarios por su cuenta. Si los usuarios son incapaces de obtener la documentación para la cual hacen el trámite, otros de sus procesos pueden verse afectados.

También se considera un puntaje de 10 en cuanto a logística y operaciones. Una vez más hacemos énfasis en que sin la aplicación, el propósito del departamento y por ende todas sus operaciones son detenidas.

Otro factor importante para en cuanto a amenazas de la aplicación web es la integridad de los datos. Se ha clasificado con un puntaje de 5. Primeramente, se considera que al tener que usar su NIF, los usuarios estarían siendo víctimas de filtrado de su información personal. Esto puede ocasionar un incumplimiento legal u obligaciones reglamentarias al no hacer un buen uso de la confidencialidad de datos personales.

Por último, hacemos referencia a la trazabilidad de los datos, en donde se ha marcado una amenaza con un puntaje de 5 por las mismas razones que se mencionaron en cuanto a la integridad de datos. Esto debido a que si se hace mal uso o alteración de la trazabilidad de los tramites realizados, se podría inculpar a algún usuario de haber generado algo que no hizo o lo contrario, no tener evidencias del trámite realizado.

- **Servicio de email:** El servicio de email es un servicio proporcionado por terceros. En este caso la accesibilidad del activo es importante pero no afecta al servicio de la organización como tal. Se ha hecho saber que la comunicación dentro y fuera de la empresa es hecha a través de emails más no el trámite. Esto ha hecho se le proporcione un puntaje de 5 para la accesibilidad.

Por otro lado, en cuanto a integridad, confidencialidad y autenticidad de usuarios e información se le ha dado un puntaje de 9. En todos estos rubros se ha declarado que la valuación de la amenaza con respecto a la información personal es probable de causar molestias a un grupo de gente por la posibilidad de brindar información falsa que puede ser parte de ingeniería social. Esto mismo conlleva a un incumplimiento legal y de las obligaciones regulatorias de datos personales.

- **Firewall:** Para el firewall se han considerado solo dos aspectos a considerar, pero no por eso han perdido su peso. El primero y más extenso es la cuestión de disponibilidad. Podemos tener dos supuestos acerca de la disponibilidad del firewall: si no está disponible o bien la comunicación será bloqueada, o se permitirá la comunicación de externos al servidor. Por ello tenemos una valuación de 10 para este activo. En el primer caso en donde toda comunicación se pierda tenemos la interrupción de actividades en la organización con el impacto ya mencionado de repercutir en el trámite del usuario deteniendo otros de sus trámites, es decir, un impacto a otras organizaciones. De igual forma esto supondría un severo daño a la operación al detener por completo el flujo de trámites. Por otra parte, si lo que sucede es que se detiene la seguridad del firewall y terceros tienen acceso al servidor web, nos encontramos en el escenario de filtrado de información personal del grupo de usuarios de la aplicación, ocasionando un incumplimiento legal y de las obligaciones regulatorias de datos personales.

El segundo aspecto importante a considerar para el firewall es la confidencialidad de los datos. A este rubro se la ha asignado una puntuación de 7 al poder ser víctima de una amenaza violación a la seguridad de la empresa y estaría sujeto a una investigación legal. Todo esto debido a la información personal manejada por la aplicación.

- **PC personales:** En cuanto a los pc personales usadas en la unidad local, la valuación es baja con un riesgo de puntuación 1 o 2. Esto debido a que las computadoras están limitadas en cuanto a puertos USB o cualquier otra forma de intercambio de información que no sea a través de las aplicaciones designadas. No se hace uso de la memoria del sistema para guardar datos de los expedientes de manera permanente. Al ser 10 unidades en el local existe un bajo riesgo de interrupción de actividades ya que tendría que haber un malfuncionamiento con todas simultáneamente.
- **Servidor tamaño medio:** El servidor tamaño medio es primordialmente usado para la base de datos, archivando el historial de expedientes, así como los registros de las transacciones efectuadas. La valuación en cuanto a accesibilidad se refiere es de 5, ya que la información guardada es histórica la interrupción de actividades e impacto en las operaciones de la organización se verán afectadas solo para consultas del pasado. Para la integridad de información se ha valuado igual en 5 debido a que puede causar conflictos a algún individuo o grupo de individuos al modificar la información histórica de los trámites realizados. De igual forma esto puede ocasionar incumplimiento legal y de las obligaciones regulatorias de datos personales. La confidencialidad es valuada también en 5 ya que al tener un tercero acceso a los registros históricos se puede obtener acceso a los datos personales de los usuarios, cayendo una vez más en los incumplimientos legales ya mencionados.
- **Equipo servidor web:** El servidor web es de los componentes más importantes para la organización, que va mucho de la mano con la aplicación web, al ser éste quien se encarga de mantener la aplicación en producción. Para no caer en redundancias se puede hacer referencia a la aplicación web, en donde se explica la importancia y la valuación dada a la accesibilidad, integridad y trazabilidad. Una de las mayores diferencias entre la valuación de la aplicación web y el servidor se encuentra en el rubro de la autenticidad de los usuarios y la información. Se ha valuado en 9 ya que a un tercero poder tener acceso al servidor web tiene control total sobre la aplicación web y por ende sobre las operaciones de la organización. Esto ocasiona un peligro para los usuarios de la aplicación, así como un incumplimiento legal que seguramente levantará un proceso de investigación.
- **VPN:** La VPN es usada desde el servidor web hacia el servidor usado como base de datos en la capital de la provincia. Esta red es usada para asegurar la comunicación segura. La VPN ha sido valuada con 5 en términos de disponibilidad, ya que la comunicación entre el servidor web y los expedientes sería interrumpida, pero esto no previene que la


























aplicación web genere el trámite, solo afecta a la vista y registro de históricos. Si embargo si representa algo de riesgo al perder algo de la trazabilidad del historial.

Por los mismos motivos, la integridad de los datos mantiene un riesgo con una puntuación de 6 ya que al ser la VPN interceptada podría alterar o conocer el contenido de las peticiones, causando pérdida de información personal que conlleva a un incumplimiento legal y de las obligaciones regulatorias de datos personales. Lo mismo aplica en términos de confidencialidad de datos y autenticación de usuarios.

- **Red local:** La red local es usada en la unidad local donde se brinda atención a clientes de forma presencial mediante los computadores personales. Existen redes de respaldo en el caso de que esta red falle, pero están fuera del alcance de la valuación. La valuación es de 5 en cuanto a disponibilidad y es el único rubro para evaluar. Puede causar molestias en cuanto a interrupción de servicio y a logística y cumplimiento de operaciones, pero no es una interrupción local ya que la aplicación web seguirá funcionando.
- **Expedientes:** Los expedientes contienen información histórica de los trámites realizados. Esta información contiene detalles y datos personales de los usuarios. En cuanto a la accesibilidad de los expedientes se ha otorgado una valuación de 5 debido a los incumplimientos de regulaciones legales que podría implicar su desaparición. El mismo razonamiento se aplicaría con respecto a la integridad de datos, ya que las modificaciones de ellos seguramente será un incidente de seguridad necesario de investigación legal. Por último, el aspecto de la confidencialidad, al igual que los dos rubros pasados tiene una valuación de 5 por motivos similares.

Diseño y valoración de salvaguardas

Se han añadido dos fases intermedias nombradas Intermedio1 e Intermedio2. Tenemos la fase current que es donde actualmente nos encontramos y la target, el escenario ideal. Cabe añadir que no en todos los aspectos se llegará al target, ya que puede incluir costos adicionales que quizás no estén en presupuesto o son un gasto importante en comparación con la mejora. La valoración realizada en la herramienta PILAR puede ser visualizada en la siguiente imagen.

	a...	top	re...	le...	safeguard	d...	s...	b...	c...	c...	In...	In...	ta...	Pl...
<input type="checkbox"/>					SAFEGUARDS						-L2	-L4	-L5	-L5 L2..
<input type="checkbox"/>	M	EL	8		 [A] Identification and authentication						-L2	-L4	-L5	-L5 L2..
<input type="checkbox"/>	T	EL	7		 [AC] Logical access control						L2	L4	L5	L5 L2..
<input type="checkbox"/>	M	PR	7		 [D] Protection of Data / Information						L2	L4	L4	L4 L2..
<input type="checkbox"/>	M	EL			 [K] Protecting cryptographic keys [SC-12]									n.a.
<input type="checkbox"/>	M	PR			 [S] Protection of Services									n.a.
<input type="checkbox"/>	M	PR	6		 [SW] Protection of Software						L2	L3	L4	L4 L2..
<input type="checkbox"/>	M	PR	5		 [HW] Protection of Hardware						L2	L2	L2	L2 L2..
<input type="checkbox"/>	M	PR	8		 [COM] Protection of Communications						L2	L4	L4	L4 L2..
<input type="checkbox"/>	M	PR			 [M] Protection of Media									n.a.
<input type="checkbox"/>	M	PR	4		 [AUX] Auxiliary Means						L2	L2	L2	L2 L2..
<input type="checkbox"/>	PHY	EL	5		 [PPE] Physical protection of equipment						L2	L2	L2	L2 L3
<input type="checkbox"/>	PHY	PR			 [L] Protection of the installations									n.a.
<input type="checkbox"/>	PER	PR			 [P] Personnel									n.a.
<input type="checkbox"/>	M	CR	5		 [IM] Incident management (ICT)						L2	L2	L3	L4 L2..
<input type="checkbox"/>	T	PR	7		 [tools] Security tools						L1	L1	L4	L4 L2..
<input type="checkbox"/>	M	CR	3		 [V] Vulnerability management						L0	L0	L3	L5 L2..
<input type="checkbox"/>	T	MN			 [A] Logging and audit									n.a.
<input type="checkbox"/>	M	RC	3		 [BC] Business continuity (contingency)						L0	L0	L3	L5 L2..
<input type="checkbox"/>	M	AD	4		 [G] Organisation									L2..
<input type="checkbox"/>	M	AD	4		 [E] External Relations									L2..
<input type="checkbox"/>	M	AD	5		 [NEW] Acquisition / development						L0	L0	L2	L3 L2..
<input type="checkbox"/>	M	PR			 [PDS] Potentially dangerous services									n.a.
<input type="checkbox"/>	M	PR			 [IP] Logical border protection system									n.a.
<input type="checkbox"/>	PHY	EL			 [PPS] Physical Perimeter Protection									n.a.
<input type="checkbox"/>	M	EL	1 (...)		 [TEMPEST] Emanation protection (TEMPEST) [PE-19]						L2	L3	L3	L3 L2

El plan de salvaguardas descrito con las acciones y explicaciones de ellas a lo largo de las fases del proyecto se describen a continuación, agrupándose con su tipo de salvaguarda:

- Identificación y autenticación, Control de acceso lógico y Herramientas de seguridad:** En este caso comenzamos con un nivel L2 teniendo como meta general llegar a L5. Los riesgos de este tipo de amenazas son importantes ya que si los activos son infiltrados se puede llegar a levantar un riesgo legal en cuanto a la confidencialidad de datos personales y de igual forma puede llegar a interrumpir las operaciones total e indefinidamente. Para la primera fase intermedia, intentando tomar ventajas de acciones sencillas se implementará un mensaje y validación en donde se le pida a los usuarios cambiar su contraseña regularmente, en un periodo de máximo 30 días. Adicionalmente se agregará un cifrado básico por lo que en cualquier momento que una contraseña sea enviada del cliente al servidor estará cifrada y será almacenada de la misma manera. La segunda fase intermedia será usada para implementar una forma de autenticación multifactorial para los usuarios, dejando de lado el uso de contraseñas que pueden ser interceptadas o encontradas por fuerza bruta. Esto añade una barrera extra y bastante segura. Con esto se alcanzará el target esperado.

- **Protección de datos/información y Protección de comunicaciones:** En este aspecto tenemos dos importantes vertientes y ambas pueden verse en el sentido de asegurar una comunicación segura entre los servidores. Se implementará en la primera fase, Intermedia1, y con ello se completarán las acciones propuestas para llegar el target. El plan consta de hacer las peticiones https, haciendo uso del protocolo TLS. Con esto tenemos mayor seguridad en que la comunicación será cifrada y manteniendo el protocolo actualizado también nos protegería de un ataque de negación de servicios distribuido (DDoS),
- **Protección del software:** En la protección del software, con las medidas ya detalladas previamente nos enfocaremos en el código del mismo. En este caso tenemos una sola aplicación web. No se hace referencia en ninguna parte de tener un controlador de versiones actualmente como lo puede ser git, por lo que cualquier cambio hecho en el código fuente puede romper funcionalidades o ser alterado sin trazabilidad alguna. Para la fase Intermedia1 se comenzará creando el repositorio para el código y se crearán diferentes ramas para mantener versiones funcionales de producción y prueba. Esto también ayudará a tener un mayor control sobre los cambios hechos, quien los hizo y versiones anteriores de ser necesarias.
Para la fase Intermedia2 se agrega el firmado del código. Cuando una aplicación es firmada, se puede asegurar que la versión que se está corriendo bajo firma es la versión aprobada por el equipo de desarrollo y que nadie a intervenido en ella desde el momento de su firma. Esto nos ayudará a tener confianza de que una vez creado el build de la aplicación, ningún intruso hará cambios sobre ella. Con esto se llega al target propuesto.
- **Gestión de incidentes:** La gestión de incidentes (IM) consta de un ciclo en donde tras detectarse algún incidente se registra, clasifica, diagnostica, resuelve y cierra. Al no tener muchos componentes en la operación no se designará algún equipo de soporte especializado a estos temas por lo que el target deseado no será implementado. Actualmente se hace la trazabilidad de ciertos procesos y se almacenan los logs y expedientes en una base de datos que nos ayuda a la parte de registro, clasificación y diagnósticos. Para la segunda fase, Intermedia2, se tendrán regulaciones e instrucciones de cómo crear la documentación necesaria de cada incidente siguiendo el ciclo de IM. También para ello se harán respaldos automáticos de todo lo que esté almacenado en la base de datos periódicamente, esto incluye los documentos de IM, los logs y los expedientes.
- **Gestión de vulnerabilidades:** Por medio de pipelines en aplicaciones como Jenkins, Travis, etc. se puede incluir un escaneo para vulnerabilidades en el código de manera automatizada cada vez que se hace un cambio en el mismo o cada cierto tiempo designado. Ya que la carga que se tiene para la primera fase Intermedia1 se empieza a acumular en este punto y habrá ciertos cambios en las aplicaciones, se dejará la

implementación de los escaneos y corrección de las vulnerabilidades para la segunda fase, Intermedia2. La resolución se hará de manera manual cada que el pipeline arroje nuevas vulnerabilidades. Dependiendo del nivel de riesgo asignado a cada vulnerabilidad se asignará un periodo de tiempo para el cual deben estar remediadas.

- **Continuidad de negocio (contingencia):** De la misma forma que en el rubro pasado, se dejaría esta salvaguarda para la segunda fase. En este caso se buscaría hacer la compra de un segundo servidor web y de ser posible un segundo servidor medio para almacén y respaldos de la base de datos. La configuración de estos no debe ser tardada ya que se replicaría lo que ya se tiene y solo sería cuestión de hacer uso de algún servidor de enrutamiento dinámico junto con una aplicación de registro de servicios para hacer la redirección de un servidor a otro en el caso de que uno dejase de funcionar. El target no se alcanzará en este caso, el cual sería hacer uso de algún servicio de servidor en la nube para delegar todo el aspecto de continuidad y seguridad física. Los precios de esto pueden ser elevados, y cobrados mensualmente y se perdería el propósito de los servidores que ya se tienen.
- **Adquisiciones/desarrollo:** No se hace mención de algún equipo de desarrollo en la documentación, por lo que se partirá de la suposición de que no se tiene uno. Para gran parte de las salvaguardas mencionadas previamente es necesario un equipo de desarrollo por lo que se buscaría algún grupo de terceros que puedan brindar la fuerza de trabajo durante las primeras 2 fases del proyecto (Intermedia1 e Intermedia2) mantener un equipo de desarrollo no es barato por lo que una vez terminadas las fases se mantendría comunicación buscando apoyo sólo cuando sea necesario. Es por ello que no se llegará al estado meta o target.

Por último, se agregan imágenes de la herramienta PILAR en donde podemos ver los valores de los riesgos repercutidos a través de las distintas fases del proyecto. El nombre de la fase puede verse en la parte superior, pero de igual forma se hace saber al lector que vienen acomodadas en sentido cronológico, comenzando con la fase inicial, pasando por las fases intermedia y terminando en el target.

potential	current	Intermedia1	Intermedia2	target	PILAR	
		asset		[A]	[I]	[C] [Auth]
<input type="checkbox"/>		ASSETS		{5.9}	{5.0}	{5.4} {2.8}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW001] Aplicación web		{5.6}	{5.0}	{5.4}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW002] Servicio de email		{2.6}	{4.9}	{5.3}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW007] Firewall		{5.5}		{4.1}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW001] 10 PC's Personales		{0.91}		{0.84}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW002] Equipo de control de entrada/salida				
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW003] Servidor tamaño medio		{2.9}	{2.5}	{2.6}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW004] Equipo servidor web		{5.9}	{2.0}	{4.4}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM001] VPN		{2.7}	{1.2}	{2.3} {2.8}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM004] Red local		{2.7}		
<input type="checkbox"/>	<input checked="" type="radio"/> A	[D004] Expedientes		{0.63}	{2.2}	{3.4}

potential	current	Intermedia1	Intermedia2	target	PILAR	
		asset		[A]	[I]	[C] [Auth]
<input type="checkbox"/>		ASSETS		{5.8}	{4.6}	{4.9} {1.7}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW001] Aplicación web		{5.1}	{4.6}	{4.9}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW002] Servicio de email		{2.2}	{4.5}	{4.9}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW007] Firewall		{5.1}		{3.7}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW001] 10 PC's Personales		{0.90}		{0.84}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW002] Equipo de control de entrada/salida				
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW003] Servidor tamaño medio		{2.9}	{2.5}	{2.5}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW004] Equipo servidor web		{5.8}	{1.9}	{4.3}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM001] VPN		{2.0}	{0.88}	{1.2} {1.7}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM004] Red local		{2.0}		
<input type="checkbox"/>	<input checked="" type="radio"/> A	[D004] Expedientes		{0.44}	{0.99}	{2.2}

potential	current	Intermedia1	Intermedia2	target	PILAR	
		asset		[A]	[I]	[C] [Auth]
<input type="checkbox"/>		ASSETS		{4.2}	{2.2}	{3.0} {0.86}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW001] Aplicación web		{2.7}	{2.2}	{2.6}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW002] Servicio de email		{0.74}	{2.1}	{2.4}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW007] Firewall		{2.7}		{1.3}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW001] 10 PC's Personales		{0.58}		{0.52}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW002] Equipo de control de entrada/salida				
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW003] Servidor tamaño medio		{1.3}	{1.2}	{1.2}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW004] Equipo servidor web		{4.2}	{0.77}	{3.0}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM001] VPN		{0.78}	{0.50}	{0.74} {0.86}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM004] Red local		{0.78}		
<input type="checkbox"/>	<input checked="" type="radio"/> A	[D004] Expedientes		{0.25}	{0.60}	{0.85}

potential	current	Intermedia1	Intermedia2	target	PILAR	
		asset		[A]	[I]	[C] [Auth]
<input type="checkbox"/>		ASSETS		{4.0}	{1.8}	{2.7} {0.77}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW001] Aplicación web		{2.3}	{1.8}	{2.1}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW002] Servicio de email		{0.67}	{1.7}	{2.1}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[SW007] Firewall		{2.3}		{0.98}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW001] 10 PC's Personales		{0.53}		{0.46}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW002] Equipo de control de entrada/salida				
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW003] Servidor tamaño medio		{1.0}	{0.96}	{0.97}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[HW004] Equipo servidor web		{4.0}	{0.73}	{2.7}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM001] VPN		{0.73}	{0.42}	{0.66} {0.77}
<input type="checkbox"/>	<input checked="" type="radio"/> A	[COM004] Red local		{0.73}		
<input type="checkbox"/>	<input checked="" type="radio"/> A	[D004] Expedientes		{0.14}	{0.55}	{0.80}

Resultado de Riesgo

A lo largo de este documento se describieron los que se han considerado los activos esenciales ya sea por su importancia hacia el servicio brindado o porque son el componente “padre” de otros. De lo que se pudo identificar tras el análisis realizado es que la mayor vulnerabilidad del servicio está en las comunicaciones entre aplicaciones y servidores, en la seguridad de la información que se está manejando y en el escenario de planes/servicios de respaldo en caso de que alguno de los activos esenciales llegase a presentar fallas.

Las consecuencias de no tratar las amenazas aquí expuestas pueden repercutir en diversos aspectos. El primero y más obvio es la negación de servicio, escenario en el cual los usuarios no podrán realizar el trámite necesario que puede desencadenar a que los usuarios sean detenidos en sus funciones ajenas a la organización. El segundo y quizás más importante se ve en la seguridad de los datos, al ser una empresa de parte del estado no solo es importante que la información personal del usuario sea confidencial para no tener repercusiones en estafas o implicaciones, sino que mancharía dura y permanentemente el nombre del mismo. Es de extrema importancia que la gente tenga confianza en las herramientas gubernamentales.

Al término del proyecto de mejora para las amenazas encontradas, el servicio estará mucho más seguro en los dos aspectos previamente mencionados, teniendo un sistema robusto y con alta disponibilidad y con un gran énfasis en la protección de los datos de los usuarios.