UNIVERSIDAD NACIONAL DE LOMAS DE ZAMORA

FACULTAD DE INGENIERIA

Tecnicatura en Programación

Trabajo práctico N°1 (grupal)

Materia: Seguridad informática

Alumnos: Federico Tito, Maxi De Roo,
Maximiliano Garrett, Roberto Frediani

Profesor: Bruno Diaz

Trabajo practico n°1 – Investigación grupal sobre BIA (Análisis de impacto al negocio):

Consigna:

- Buscar modelo de BIA y definición de RTO, RPO y ALE.

El Análisis de Impacto al negocio (también conocido como Business Impact Analysis, BIA) tiene por objeto analizar los impactos a los que la organización puede enfrentarse ante la discontinuidad de sus operaciones, así como las dependencias de las tecnologías y los sistemas de información corporativos.

Objetivos: El BIA permitirá a su organización identificar para cada proceso o actividad:

- Impacto que tendría la interrupción.
- El período de tiempo máximo después de una interrupción dentro del cual tiene que continuarse la operación.
- El nivel mínimo al que la actividad tiene que ser ejecutada cuando se recupera.
- El periodo máximo de tiempo antes que los niveles normales de operación tengan que haberse recuperado.

¿Por qué realizar un Análisis de Impacto?

Todas las empresas están expuestas a sufrir incidentes o eventos no deseados que pueden generar múltiples consecuencias negativas para una organización. Pueden, por ejemplo, paralizar la productividad, generar pérdidas económicas, crear una mala reputación empresarial o hacer que la organización pierda información sensible y confidencial.

Por tanto, tener identificadas las amenazas más evidentes a los que se enfrenta la organización y el impacto que tendrían en el que caso de que se materializaran es fundamental para minimizar los riesgos y actuar frente a ellos.

Cuestiones preliminares: Un aspecto importante a tener en cuenta en la elaboración de un BIA son los tiempos. En este sentido, cobran especial importancia los siguientes:

- RTO (Recovery Time Objective): Tiempo de recuperación de las actividades que hemos identificado bajo unas condiciones mínimas aceptables. Por ejemplo, supongamos que el responsable del Departamento de Administración nos indica que, en caso de que fallara la plataforma que soporta las aplicaciones para la generación y emisión de la nómina, se deberían recuperar el servicio en un plazo máximo de 24h. En este caso, estableceríamos que el RTO asociado a dicho proceso es de 24h.

- MTD (Maximum Tolerable Downtime): Tiempo máximo tolerable de caída el cual nos determina el tiempo que puede estar caído un proceso antes de que se produzcan efectos desastrosos en la compañía y repercuta en el negocio. Volviendo al caso anterior, supongamos que el proceso de gestión de nóminas no debe estar interrumpido por un periodo superior a 48h. En este caso, estableceríamos que el MTD asociado a dicho proceso es de 48h.

- RPO (Recovery Point Objective): El grado de dependencia de la actualidad de los datos determina la cantidad máxima de información que se podría perder sin llegar a tener consecuencias inaceptables, formando parte de las políticas de respaldo definidas por la organización. En este sentido, imaginemos que el responsable del Departamento de Administración nos indica que podrían tolerar una pérdida de información siempre y cuando no se perdieran los datos generados en más de un día completo. Por lo tanto, estableceríamos que el RPO es de 24h.

- WRT (Work Recovery Time): Es el tiempo invertido en buscar datos perdidos y la realización de reparaciones. Se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos.

- ALE (Annualized Loss Expectancy): es la expectativa de pérdida anual que permite modelar el impacto que los riesgos de seguridad pueden tener sobre los activos de una organización. Para esto se emplea una fórmula algebraica que multiplica el valor de un evento discreto de pérdida (expectativa de pérdida individual o SLE) por su expectativa anual de ocurrencia (ARO), es decir, la pérdida monetaria que se puede esperar para un activo debido a la materialización de una o más amenazas en un periodo de un año. Se define a través de la siguiente fórmula:

$$ALE = SLE \times ARO$$
$$SLE = FE \times VA$$

Donde:

- ALE: Expectativa de Pérdida Anual
- SLE: Expectativa de Pérdida Individual
- ARO: Tasa de Ocurrencia Anualizada
- FE: Factor de Exposición
- VA: Valor del activo

Para obtener el valor de ALE, se multiplica la esperanza de pérdida derivada de un riesgo, por su tasa de ocurrencia anualizada. A su vez, SLE es el resultado del producto entre el factor de exposición del activo por el valor del mismo. En el siguiente ejemplo se muestran los pasos sugeridos para calcular la pérdida anualizada.

¿Por dónde empezamos?

Para llevar a cabo el BIA mantendremos reuniones con los departamentos dentro del alcance de nuestro estudio para recalar la información necesaria. El personal entrevistado (responsables de departamento, coordinadores, personal técnico, etc.) nos facilitará la información de los procesos, y requisitos de recuperación, así como las posibles dependencias con los proveedores, clientes, etc. Deberemos considerar todas estas cuestiones y dejar constancia de ello en el BIA.

Resultado

Como resultado de los trabajos de análisis dispondremos de un conjunto de procesos o actividades para los cuales hemos definido el RTO, MTD y RPO. Con esta información podemos crear la lista ordenada por prioridad y obtener las actividades críticas y si profundizamos en el análisis podemos deducir cuales son los activos críticos de TI.

Como ejemplo de los tiempos de recuperación en un BIA, podemos observar en la siguiente tabla su implicación dependiendo del proceso de negocio, en este caso dentro del departamento de Administración:

Proceso de negocio	RTO	RPO	MTD	Criticidad
Gestión de nóminas	*24 horas*	*24 horas*	*48 horas*	*Alto*
Solicitud de viaje	*1 semana*	*24 horas*	*48 horas*	*Medio*
Validación de vacaciones	*1 semana*	*24 horas*	*48 horas*	*Bajo*

En la tabla anterior, el proceso de Gestión de nóminas nos viene a decir que posee una criticidad alta, proyectándose en el periodo de final de mes, para el pago de las nóminas a los empleados. Determinamos un RTO de 24 horas como tiempo de recuperación para restablecer el servicio, y un RPO de 24 horas como tiempo de la posible pérdida de la información debido a la caída del servicio. Por último, un MTD de 48 horas como tiempo máximo de parada del servicio sin superarlo ya que conllevaría graves riesgos a la organización.

La elaboración y puesta en marcha de un análisis de impacto o BIA para nuestro negocio no es más que conocer las necesidades de negocio expresándolas en términos de recuperación y, atendiendo a los resultados el estudio, implantar planes de recuperación que permitan restablecer los servicios o infraestructuras, etc., cubriendo las necesidades y el cumplimiento de los objetivos de negocio marcados por la compañía.

¿Qué hacemos con la información del BIA?

El BIA es una de las partes fundamentales en el plan de continuidad de negocio.

La información que obtenida en la elaboración del BIA se validará con los distintos departamentos involucrados. Adicionalmente, contrastaremos los requisitos de recuperación con la capacidad de recuperación de los sistemas que intervienen en la prestación de servicios. En última instancia, presentaremos las conclusiones a la Dirección para hacerlos partícipes y así obtener su respaldo de cara a afrontar nuevos proyectos para mejorar la capacidad de recuperación actual.

Principales beneficios obtenidos al desarrollar un análisis de impacto sobre el negocio

- Se delimitan los procesos o actividades críticas dentro de la organización que afectan a nuestro negocio pudiendo descubrir actividades críticas que a priori no lo parecían.
- Permite identificar vulnerabilidades de una organización en materia de continuidad de negocio.
- En caso de disponer de planes de recuperación permitirá verificar si estos cubren las necesidades del negocio.

- Propicia la implicación de un mayor número de áreas de la organización a la hora de implantar planes de continuidad, no solo al personal responsable de llevar a término este tipo de proyectos.
- Reducción de costes ante posibles interrupciones del negocio.
- Aporta información de gran valor a la hora de priorizar el desarrollo de otros proyectos en materia de continuidad de negocio.
- Un mayor conocimiento de los procesos de negocio, contribuirá favorablemente a la mejora de la competitividad y seguridad en el mercado.
- La información obtenida en el desarrollo del BIA es una base fundamental para implantar estrategias de recuperación eficientes.

Tal y como podemos observar, llevar a cabo un análisis de impacto sobre el negocio puede aportar múltiples beneficios para nuestra organización.

Evaluación de impactos operacionales:

Teniendo en cuenta los elementos operacionales de la organización, se requiere evaluar el nivel de impacto de una interrupción dentro de la Entidad.
El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones del negocio; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

- **Nivel A:** La operación es crítica para el negocio. Una operación es crítica cuando al no contar con ésta, la función del negocio no puede realizarse.

- **Nivel B:** La operación es una parte integral del negocio, sin ésta el negocio no podría operar normalmente, pero la función no es crítica.

- **Nivel C:** La operación no es una parte integral del negocio.

La tabla siguiente muestra un ejemplo con los niveles de criticidad en una Entidad, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto, la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Aplicaciones	Sistema de Control de flujo de documentos	B	3	Contenedor de aplicaciones
Web	Sitio web Entidad	A	1	Capa de presentación
Base de Datos	SQL nómina	A	1	Contenedor de aplicaciones en SQL
Seguridad de Información	Firewall	A	1	Servicio de firewall de la Entidad
Sistemas de Almacenamiento	SAN (Storage Área Network)	A	3	Capacidad de almacenamiento en SAN
Comunicaciones	Acceso Local a Internet	C	4	Comunicación de Internet del usuario local
Cuartos de Máquinas	Centro de Datos	A	1	Servicio de Centro de datos de la Entidad
Proveedores de Aplicaciones y/o comunicaciones	Interno/externo	B	2	Desarrollo Interno o contratado por externos. Canales de comunicaciones
Recurso Humano	Internos/externos	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad

Identificación de procesos críticos:

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla.

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

Una vez identificados los procesos críticos del negocio, función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia.

El siguiente ejemplo ilustra esta situación:

Categoría (Función Crítica del Negocio)	Proceso Crítico (Servicios)	MTD (en días)	Prioridad de Recuperación
Aplicaciones	Sistema de Control de flujo de documentos	2 días	3
Soporte Informático	Dispositivos Móviles	2 días	3
Aplicaciones	Sistema de Nómina	0.5 día*	1
Seguridad de Información	Firewall	0.5 día*	1
Sistemas de Almacenamiento	SAN (Storage Área Network)	1 día	2
Comunicaciones	Servicio WiFi	1 día	2
Cuartos de Máquinas	Centro de Datos	0.5 día*	1
Soporte Informático	Equipo PC de usuario	3 días	4

*: Corresponde al tiempo de inactividad del proceso crítico del negocio, que tomaría menos de un (1) día de tolerancia de inactividad del servicio.

Identificación de recursos:

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomas acciones para medir el impacto del negocio de las Entidades.

La siguiente tabla representa un ejemplo de identificación de recursos críticos de Sistemas de Tecnologías de Información.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI
Aplicaciones	Sistema de nómina	Sistema de entrada de novedades administrativas. Interfaces con el Sistema Financiero.
Seguridad de Información	Firewall	Reglas de entrada y salida de puertos. Reglas NAT/PAT. Direccionamiento IP público.
Comunicaciones	Servicio WiFi	Control de identificación usuarios con Portal Cautivo. Control de usuarios locales Vs Invitados.
Cuartos de Máquinas	Centro de Datos	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Eléctrica.

La siguiente tabla muestra un ejemplo de valores RTO/WRT para el proceso crítico de la operación del Centro de Datos de una organización.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación Objetivo – RTO	Tiempo de Recuperación de Trabajo – WRT
Cuartos de Máquinas	Centro de Datos	Control de operaciones de Servidores. Sistemas de Almacenamiento. Sistemas de Backups. Aire Acondicionado Acometida Eléctrica	1 día 0.5 día 1.5 días 1 día 0.5 día	1 día 0.5 días 1 día 0.5 día 0.5 día

Fase de gestión del riesgo:

Ante la posible materialización de algún evento que ponga en riesgo la operatividad de la Entidad y con el fin de establecer prioridades para la mitigación de los riesgos, se hace necesario disponer de metodologías para su evaluación.

La metodología del plan de continuidad del negocio, determina los diversos escenarios de amenazas de una Entidad, el cual permite desarrollar las estrategias de continuidad y los planes para reanudar los servicios que estaban en operación.

La gestión del riesgo debe contemplar el “cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia”.

A pesar de la existencia de diversidad de métodos es recomendable iniciar con los más sencillos, que forman parte de lo que denominamos análisis previos. Una primera aproximación es la de establecer un conjunto de causas que pueden generar dificultades, tales como:

Riesgos Tecnológicos:

- Fallas en el Fluido Eléctrico.
- Sabotaje Informático.
- Fallas en el Centro de Datos.
- Problemas Técnicos.
- Fallas en equipos tanto de procesamiento, telecomunicaciones como eléctricos.
- Servicios de Soporte a Sistemas de Producción y/o Servicios.

Riesgos Humanos:

- Robos.
- Acto Hostil.
- Marchas, mítines.
- Artefactos explosivos.
- Problemas organizacionales (huelgas, leyes aceptadas por el congreso, regulaciones gubernamentales, leyes internacionales)
- Problemas de terceros involucrados en la producción o soporte a un servicio.
- Problemas con los proveedores de insumos o subproductos.

Desastres Naturales:

- Sismos
- Tormentas Eléctricas
- Incendios
- Inundaciones

Clasificación de escenarios de riesgo:

A fin de conocer con precisión los riesgos potenciales de la prestación de servicios de tecnologías de la información en las Entidades, es recomendable clasificar los posibles escenarios de los riesgos potenciales y describir su nivel de impacto por cada función crítica del negocio. La siguiente tabla describe un ejemplo de esta clasificación.

Categorías	Escenarios	Descripción Impacto
Red Eléctrica	Fallas en el fluido eléctrico red normal (no regulada)	Fallas del servicio eléctrico de la entidad que afecta equipos eléctricos normales.
	Fallas en el Fluido Eléctrico red regulada	Fallas en los servicios de Tecnología de Información.
Red Datos, Internet y Seguridad	Problemas dispositivos Red: Falla Parcial	Falla temporal de los servicios de TI de todo un componente por limitación en la comunicación.
	Problemas dispositivos Red: Falla Total	Falla general de los servicios de TI de todos los componentes por ausencia en las comunicaciones
	Problemas en los Dispositivos Seguridad: Falla Parcial	Falla parcial de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware Software) y ausencia de políticas y controles de TI.
	Problemas en los Dispositivos Seguridad: Falla Total	Falla general de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware, Software) y ausencia de políticas y controles de TI.
	Ausencia servicio del canal de Internet Última Milla: Total	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla por ausencia en la
		comunicación. No acceso a internet; impacto directo con el proveedor del servicio.
	Perdida conectividad hacia el NAP Colombia: Parcial	Falla parcial de los servicios de TI por ausencia en la conexión hacia el NAP Colombia. Acceso parcial a la red de internet por parte del proveedor del servicio.
Hardware distribuido	Problema de Hardware de Servidores: Falla Total	Falla total de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problema HW Servidores: Falla Parcial	Degradación de la calidad (lentitud) de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problemas en sistema Almacenamiento	Falla de los servicios de los sistemas de Información que usan la plataforma de almacenamiento de información.
	Problemas Hardware de Servidores	Falla de los servicios de los sistemas de información que usan la plataforma de servidores.
Aplicaciones infraestructura distribuida	Problemas Capa de Aplicaciones	Falla o degradación del servicio prestado en el sistema de información afectado por problemas en las aplicaciones.
	Problemas Capa Media	Falla o degradación de la aplicación soportada por las herramientas de software y el sistema de almacenamiento masivo de datos – SAN, por tanto se puede presentar degradación o ausencia del servicio prestado por sistema de información afectado por problemas de la capa media.

	Problemas Capa de Bases de Datos	Falla o degradación de las aplicaciones soportadas por las herramientas y motores de Base de Datos, por tanto se puede presentar degradación o ausencia del servicio prestado por los sistemas de información afectados por problemas de la capa de base de datos.
Recurso Humano	Ausencia de funcionarios, incapacidades y rotación	Disminución de capacidad de atención a los clientes y usuarios, lentitud en la atención a requerimientos e incidentes, como también el retraso en la puesta en marcha de nuevos servicios.
	Errores humanos en operación	Contempla desde la degradación de un servicio hasta la pérdida del mismo, como también la ejecución de procedimientos de manera errada que de cómo resultado la pérdida del servicio de uno o todos los sistemas de información del proyecto.
Desarrollo de aplicaciones	Falla en la aplicación por desarrollo no adecuado de parte de terceros	Contempla la degradación de un servicio por fallas en la funcionalidad de los sistemas de información.
	Falla en la aplicación por desarrollo no adecuado por parte de la Entidad	Contempla la degradación de un servicio por fallas en la funcionalidad en los sistemas de información de la Entidad.

Identificación de vulnerabilidades:

Las vulnerabilidades son las debilidades de seguridad de Información asociadas a los activos de información y se hacen efectivas cuando una amenaza la materializa en los sistemas de información de las Entidades.

Estas no son causa necesariamente de daño, sino que son condiciones que pueden hacer que una amenaza afecte a un activo de información en particular. Para cada amenaza identificada en el punto anterior se debe realizar un análisis de riesgo para identificar la(s) vulnerabilidad(es).

La siguiente tabla muestra un ejemplo de las amenazas y vulnerabilidades por cada Activo de Información.

Sistema TI	Activo de Información	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto
Servicio Web de la Entidad	Página Web Entidad	Defacement (desfiguración página web)	Mal diseño del sitio web	Medio	Alto
Servicio de correo electrónico	Correo electrónico Exchange	Virus, listas negras	Carencia de parches de seguridad	Alto	Alto
Sistema de Almacenamiento	SAN o NAS	Falla en el fluido eléctrico	No hay buena acometida eléctrica	Bajo	Alto
Sistema de Base de datos	Bases de datos interna	Usuario no autorizado	Mala configuración	Bajo	Alto
Servicio Red de comunicaciones	Equipos Switches de la Entidad	Falla de comunicaciones	Bloqueo de puertos	Medio	Alto

Conclusión:

El análisis de impacto del negocio – BIA, hace parte importante del plan de continuidad del negocio y a su vez presenta consideraciones importantes para la gestión del riesgo dentro de las organizaciones, que establecen un marco de políticas, procedimientos y estrategias que permiten asegurar que las operaciones de carácter crítico puedan ser mantenidas y recuperadas a la mayor brevedad posible, en caso de fallas graves dentro de los sistemas de información y las comunicaciones.

En este sentido, las distintas organizaciones deben considerar que el BIA es un instrumento operacional muy importante que permite la toma de decisiones en momentos críticos de la organización en virtud del cese de operaciones debido a una situación anómala presentada. De esta manera dicho instrumento, contribuye a identificar las operaciones y servicios considerados críticos dentro de la entidad, que contribuyen a restablecer en el menor tiempo posible los servicios y operaciones con el apoyo de un plan de continuidad del negocio de las entidades.

Corroborando lo anterior, el análisis de impacto del negocio - BIA, podrán ayudar a identificar dentro del marco de la seguridad de la información, las vulnerabilidades potenciales de la organización, podrá delimitar las actividades críticas que afectan el negocio y ayudará a las entidades a definir los planes adecuados de recuperación de los servicios que afectan el objeto del negocio; de otro lado las entidades podrán tener mayor información sobre el estado de los procesos contribuyendo favorablemente a mejorar la competitividad y proyectar estrategias adecuadas para una recuperación exitosa de la información.

Finalmente, es responsabilidad de las empresas disponer de un recurso humano suficientemente capacitado y especializado, capaz de enfrentarse a los eventos inesperados que atentan con la operatividad, seguridad y disponibilidad de los sistemas de información y las comunicaciones.