



## Análisis de Impacto al Negocio Táctico

### 1. Introducción

El Análisis de Impacto al Negocio (BIA) es el proceso formal para analizar las actividades críticas de la organización y el efecto que una interrupción en el negocio podría tener sobre ellas. Este BIA Táctico está específicamente enfocado en evaluar la criticidad y las dependencias del proceso *Implementación de seguridad e identidades (IAM)*, el cual soporta la operación de servicios institucionales en la nube, incluyendo gestión de identidades y accesos, cifrado y auditoría.

En conformidad con ISO 22301:2012, el objetivo es documentar los impactos, las interdependencias y los requisitos de recuperación necesarios para salvaguardar la continuidad de los servicios tecnológicos, garantizando la disponibilidad, la integridad y la confidencialidad de la información, así como el cumplimiento normativo y la confianza de los usuarios.

### 2. Objetivo

Determinar el impacto que tendría la interrupción del proceso **Implementación de seguridad e identidades (IAM)** sobre la operación institucional, identificando el tiempo máximo tolerable de interrupción (**MTPoD/MAO**), el tiempo de recuperación objetivo (**RTO**) y el nivel mínimo de continuidad (**MBCO**). Este análisis busca priorizar actividades críticas, establecer dependencias y definir mecanismos que garanticen la continuidad del negocio, reduciendo riesgos asociados a la indisponibilidad de servicios en la nube y asegurando el cumplimiento de los objetivos estratégicos de la organización.

### 3. Procedimiento

#### 3.1. Identificación del proceso.

Proceso:	<b>Implementación de seguridad e identidades (IAM)</b>
Grupo de Productos y Servicios relacionado:	<b>Seguridad en la nube (gestión de identidades y accesos, cifrado, auditoría)</b>
Responsable (Área/Función):	<b>Cómputo/TI</b>
Nombre del responsable:	<b>Juan Pablo Chávez Lacaud</b>
Fecha de llenado:	<b>03/01/26</b>

#### 3.2. Tipo y nivel de impacto al negocio por la interrupción en el proceso.

*Nota: Requisito de ISO 22301:2012: 8.2.2.b) Valorar los impactos a través del tiempo por no ejecutar estas actividades.*

No aplica (**N**) Bajo (**B**) Medio (**M**) Alto (**A**)



**INSTITUTO POLITÉCNICO NACIONAL**  
**ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)**  
Cuestionario para el Análisis de Impacto al Negocio

Fecha

03/01/26

Versión  
1

Página  
2 de 4

Tipo de Impacto	0 - 5 Min.	5-15 Min.	15-30 Min.	30-60 Min.	1-2 Horas	2-5 Horas	5-12 Horas	12-24 Horas	1-2 Días	2-5 Días	>5 Días
Pérdida económica	B	B	M	M	A	A	A	A	A	A	A
Incumplimiento legal y/o regulatorio	B	B	B	M	M	M	M	A	A	A	A
Daño a la reputación / Imagen	N	M	M	M	M	A	A	A	A	A	A
Afectación del servicio al cliente	B	B	M	M	M	A	A	A	A	A	A
Pérdida de calidad	B	B	M	M	M	A	A	A	A	A	A
Pérdida de productividad	B	B	M	M	M	A	A	A	A	A	A
Pérdida de control	B	B	M	M	M	A	A	A	A	A	A
Daño a la salud y/o bienestar de personas	N	N	N	N	N	N	B	B	M	M	A
Daño medio-ambiental	N	N	N	N	N	N	B	B	M	M	A
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓

**3.3. Máximo periodo de interrupción tolerable (MTPoD / MAO) para el proceso.**

(Tiempo que tomaría para que los impactos adversos, que pueden resultar de no proveer un producto/servicio o la no ejecución de una actividad, sean inaceptables)

Marcar con (X) el tiempo seleccionado.

*Nota: Requisito de ISO 22301:2012: 8.2.2.c) Establecer periodos de tiempo y sus prioridades para reanudar estas actividades a un nivel mínimo aceptable especificado, tomando en consideración el tiempo en el que los impactos de no reanudar se volverían inaceptables.*

Máximo periodo de interrupción tolerable (MTPoD / MAO)										
< 5 Min.	< 15 Min.	< 30 Min.	< 1 Hrs.	< 2 Hrs.	< 5 Hrs.	< 12 Hrs.	< 24 Hrs.	< 48 Hrs.	< 120 Hrs.	Tiempo Específico
						X				

**3.4. Identificar tiempo de recuperación objetivo (RTO) para el proceso.**

(Periodo de tiempo después de un incidente en el que se debe reanudar un producto o servicio, reanudar una actividad o recuperar un recurso)

Marcar con (X) el tiempo seleccionado.

*Nota: Requisito de ISO 22301:2012: 8.2.2.c) Establecer periodos de tiempo y sus prioridades para reanudar estas actividades a un nivel mínimo aceptable especificado, tomando en consideración el tiempo en el que los impactos de no reanudar se volverían inaceptables.*



**Tiempo de recuperación objetivo (RTO)**

< 5 Min.	< 15 Min.	< 30 Min.	< 1 Hrs.	< 2 Hrs.	< 5 Hrs.	< 12 Hrs.	< 24 Hrs.	< 48 Hrs.	< 120 Hrs.	Tiempo Específico
										< 4 Hrs.

- 3.5. Identificación de objetivo de continuidad del negocio mínimo (MBCO) para el proceso.  
(Nivel mínimo de servicio que es aceptable para la organización para lograr sus objetivos de negocio durante una interrupción).

*Nota: Requisito de ISO 22301:2012: 8.2.2.c) Establecer periodos de tiempo y sus prioridades para reanudar estas actividades a un **nivel mínimo aceptable especificado**, tomando en consideración el tiempo en el que los impactos de no reanudar se volverían inaceptables.*

Mantener la operación habilitando el modo degradado con autenticación/IAM funcional (incluye MFA para cuentas privilegiadas), alta disponibilidad básica habilitada, auditoría activa, cifrado en tránsito/reposo operativo y capacidad de gestión de accesos esencial, manteniendo RPO  $\leq 1$  h y MTTR  $\leq 4$  h.

- 3.6. Identificar actividades que soportan la operación de este proceso.

*Nota: Requisito de ISO 22301:2012: 8.2.2.a) Identificar **actividades** que soportan la provisión de productos y servicios.*

Actividades que soportan el proceso	ID
Definir y aplicar roles/políticas IAM (principio de menor privilegio)	1
Cifrado en tránsito y en reposo de datos y credenciales	2
Revisión y auditoría de accesos administrativos (mensual para cuentas privilegiadas)	3
Parches críticos $\leq 72$ h en componentes que soportan IAM (control de seguridad base)	4
MFA obligatorio para cuentas privilegiadas y acceso remoto.	5
Integración con SIEM (eventos y logs para cumplimiento)	6

- 3.7. Identificar opciones actuales de continuidad operacional ej. Procesos manuales, contratistas, trabajo desde casa, etc. (en caso de contar con ellas).

ID	Actividad	Estrategia(s) / mecanismo(s) de continuidad operacional actual
1	Migración de aplicaciones y datos	<ul style="list-style-type: none"><li>- DR en nube, respaldos cifrados y versionados, restauraciones probadas (trimestrales).</li><li>- Automatización (IaC/CI-CD) para reprovisionar políticas/roles y</li></ul>



ID	Actividad	Estrategia(s) / mecanismo(s) de continuidad operacional actual
		accesos, con repositorio de infraestructura como código - Trabajo remoto de equipo TI/seguridad y cuentas “break-glass” para contingencias de acceso administrativo (alineado a gobierno de cambios CAB).

### 3.8. Interdependencia con otros procesos y/o actividades.

*Nota: Requisito de ISO 22301:2012: 8.2.2.d) Identificar **dependencias** y recursos de soporte para estas actividades, incluyendo proveedores, terceros asociados y otras partes interesadas relevantes.*

Procesos / actividades de los que se **recibe** información.

ID	Proceso / actividad
1	VPC y Conectividad (NUBE_NET_01) – redes, VPN/IPSec, segmentación (necesario para federación y control de acceso)
2	Aplicaciones críticas (NUBE_APP_01) – catálogos de servicios/roles que requieren provisión de identidades/políticas
3	Almacenamiento en la nube (NUBE_STO_01) – políticas de acceso a repositorios/buckets
4	Base de datos gestionada (NUBE_DB_01) – cuentas y roles de acceso, auditoría de consultas críticas [Inventario...de Activos   Word]

Procesos / actividades a los que se **envía** información.

ID	Proceso / actividad
1	Monitoreo de seguridad / auditoría (NUBE_SIEM_01) – eventos y logs (cumplimiento)
2	Monitoreo de disponibilidad (NUBE_MON_01) – métricas y health checks (integraciones de autenticación)
3	Políticas y procedimientos (NUBE_POL_01/CAB) – trazabilidad de cambios de roles y accesos
4	Plataforma de respaldos/DR (NUBE_BAK_01) – inclusión de configuraciones IAM en planes de respaldo/restauración