
	<p>UNIVERSIDAD NACIONAL DEL CENTRO DEL PERÚ</p> <p><b>FACULTAD DE INGENIERÍA DE SISTEMAS</b></p> <p>DEPARTAMENTO ACADÉMICO DE INGENIERÍA DE SISTEMAS.</p>	
---	---	---

Nombre de la asignatura: **CONTINUIDAD DE T.I.**

**Código: ETI03**

**Fecha: 19/05/2024**

**Tiempo: 90 minutos.**

**Nombres:**

- **Espinoza Morales Keyla Xiomara**
- **Fernandez Rojas Gabriel André**
- **Ganoza Gutarra Juan Carlos**
- **Leon Garcia David Daniel**
- **Samaniego Inga Alex Piero**
- **Torres Vilcapoma Jhonny Ihan**

## PRÁCTICA CALIFICADA

Analice detenidamente los siguientes datos relevados sobre el Contexto Externo e Interno de la organización.

### Preguntas de esta tarea

Indique brevemente de qué forma cada uno de los factores relevados del contexto externo e interno podrían influir en la Gestión de Riesgos de TI/Operativos, por ejemplo: aumentando la probabilidad de determinados escenarios o afectando ciertos Planes de Tratamiento de Riesgos.

<b>CONTEXTO INTERNO</b>	1. La organización acaba de fusionarse con un competidor.
	2. Se están reestructurando las áreas y reduciendo personal.
	3. Dirección designada por el Gobierno (elecciones en 2 meses).
	4. La función de Gestión de Riesgos de TI se creó hace 1 mes.
	5. Se decidió adoptar tecnología innovadora para la región.

<b>CONTEXTO EXTERNO</b>	1. Hay crisis económica y social.
	2. Se genera un efecto emigratorio de recursos de TI calificados.
	3. Hubo una gran devaluación de la moneda local.
	4. El acceso a la Tecnología importada está limitado.
	5. Diariamente salen numerosos cambios regulatorios.

<b>FACTORES DEL CONTEXTO</b>	<b>INFLUENCIA EN LA GESTIÓN DE RIESGOS DE TI/OPERATIVOS</b>	<b>CONSECUENCIAS POSIBLES</b>
<b>CRISIS ECONÓMICA Y SOCIAL</b>	Aumenta la exposición a riesgos operativos y de ciberseguridad. Se dificulta la inversión en infraestructura y mantenimiento.	Incidentes por falta de actualización de sistemas, reducción en los controles de seguridad, aumento de fraudes internos o sabotajes. Los planes de tratamiento se ven limitados por falta de recursos financieros.
<b>EMIGRACIÓN DE RECURSOS DE TI CALIFICADOS</b>	Disminuye la capacidad de respuesta ante incidentes, retrasa proyectos y debilita el conocimiento institucional.	Fallas prolongadas por falta de personal técnico capacitado, pérdida de continuidad en los planes de tratamiento, dependencia de terceros.
<b>DEVALUACIÓN DE LA MONEDA LOCAL</b>	Impacta directamente en el presupuesto de TI. Aumentan los costos de licencias, soporte, renovación de equipos.	Cancelación o postergación de iniciativas de mitigación, uso de software desactualizado, mayor exposición a vulnerabilidades. Planes de tratamiento se postergan o se ajustan a soluciones menos efectivas.
<b>ACCESO LIMITADO A TECNOLOGÍA IMPORTADA</b>	Obstaculiza la renovación tecnológica y el cumplimiento de estándares internacionales.	Implementación de soluciones no óptimas o incompatibles, retrasos en la implementación de controles tecnológicos. Los planes deben adaptarse a lo disponible en el mercado local.
<b>CAMBIOS REGULATORIOS FRECUENTES</b>	Dificultan la planificación y adaptación de los controles de cumplimiento. Se genera incertidumbre normativa.	Invalidez de controles actuales, exposición a sanciones, necesidad de constantes revisiones y ajustes a los planes de tratamiento.

<b>FACTORES INTERNOS</b>	<b>INFLUENCIA EN LA GESTIÓN DE RIESGOS DE TI/OPERATIVOS</b>	<b>CONSECUENCIAS POSIBLES</b>
<b>FUSIÓN CON UN COMPETIDOR</b>	Incrementa la complejidad del entorno TI, requiere integración de sistemas, procesos y políticas.	Fallos de interoperabilidad, pérdida o exposición de datos durante migraciones, conflictos de configuración.
<b>REESTRUCTURACIÓN Y REDUCCIÓN DE PERSONAL</b>	Limita los recursos humanos disponibles para implementar y mantener controles, afecta la moral del personal.	Omisiones en monitoreo, retrasos en la gestión de incidentes, errores por sobrecarga de tareas.
<b>DIRECCIÓN DESIGNADA POR EL GOBIERNO (CON ELECCIONES PRÓXIMAS)</b>	Genera incertidumbre en la continuidad de políticas y proyectos estratégicos, posible cambio de prioridades.	Interrupción de planes de mitigación en marcha, proyectos detenidos por cambio de enfoque de la alta dirección.
<b>NUEVA FUNCIÓN DE GESTIÓN DE RIESGOS DE TI (1 MES DE ANTIGÜEDAD)</b>	Alta inmadurez del proceso. Falta de políticas claras, experiencia limitada y escasa integración con otras áreas.	Riesgos no identificados adecuadamente, controles mal definidos o ineficaces, planes de tratamiento incompletos.
<b>ADOPCIÓN DE TECNOLOGÍA INNOVADORA</b>	Introduce riesgos tecnológicos y operativos asociados a la novedad y falta de referentes locales.	Problemas de compatibilidad, falta de soporte técnico regional, errores en la implementación, curva de aprendizaje prolongada.

