

TIPO DE RIESGO	Estratégico <input type="checkbox"/>	Proceso <input checked="" type="checkbox"/>	Sistema de Gestión	ISO 9001 <input checked="" type="checkbox"/> , ISO 27001 <input type="checkbox"/> , Acreditación <input type="checkbox"/> , ISO 17025 <input type="checkbox"/> , Atención al paciente <input type="checkbox"/>	Proyectos <input type="checkbox"/>
			Normativo	Corrupción <input type="checkbox"/> Fraude <input type="checkbox"/>	
ALCANCE	<input checked="" type="checkbox"/> Institucional <input type="checkbox"/> Sede	ESTADO RIESGO		<input checked="" type="checkbox"/> Posible <input type="checkbox"/> Materializado	

1. PROCESO/COMPONENTE DEL PLAN ESTRATÉGICO/PROYECTO

CÓDIGO: U-CP-11-001 NOMBRE: Caracterización Gobierno y Gestión de Servicios de TI

OBJETIVO: Evaluar, orientar y supervisar las estructuras, procesos y mecanismos del gobierno de TI para apoyar los objetivos estratégicos de la Universidad, proporcionando los lineamientos para planificar, construir, ejecutar y controlar la plataforma tecnológica con el fin de garantizar la continuidad, disponibilidad y seguridad en los servicios de TI, que satisfagan las necesidades de la comunidad universitaria.

2. IDENTIFICACIÓN DEL ESCENARIO DE RIESGO

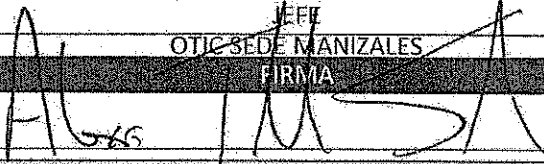
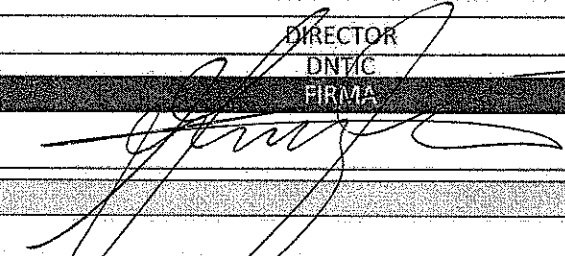
CAUSA(S) (Ver tabla)		ESCENARIO DE RIESGO	CONSECUENCIA(S) (Ver tabla)	
Determine las causas que pueden llevar a que se presente el escenario de riesgo. ESCENARIO DE RIESGO DEBIDO A		Describa claramente el riesgo, teniendo en cuenta los eventos que pueden llegar a ocurrir y el activo/proceso que puede afectar	Efecto que podría llegar a tener la ocurrencia del escenario de riesgo en la UN.	
COD	CAUSA	Infraestructura destruida por desastres de origen tecnológico, ambiental o de orden público.	COD	CONSECUENCIA
E3	Medioambientales: terremotos, incendios, inundaciones, tsunamis.		C1	Pérdidas económicas
E4	Sociales: Protestas, Vandalismo político.		C8	Reprocesos
			C9	Insatisfacción del usuario
I4	Tecnología: Ataques informáticos, virus, ransomware.		C2	Pérdida de imagen
		C5	Daños a la integridad física	

3. ANÁLISIS DEL RIESGO

PROBABILIDAD (Ver tabla)		IMPACTO (Ver tabla)		RIESGO INHERENTE (Ver tabla)	
3	POSIBLE	20	CATASTROFICO	60	EXTREMO

4. EVALUACION DEL RIESGO									
CARACTERÍSTICAS DEL CONTROL					RIESGO RESIDUAL (Ver tabla)				
COD	CONTROL	Responsable	Documentado (S/N)	M: Manual A: Automático	Frecuencia	↓ PROBABILIDAD	↓ IMPACTO	VLR	CALIFICACIÓN
1	Esquema de backúps físicos almacenados en lugares distantes al centro de datos	OTIC sedes Andinas y Profesional responsable de TIC en las Sedes de Presencia Nacional	S	A: Automático	Mensual	3	15	45	Alto
2	Plan Automático de contingencia	OTIC sedes Andinas y Profesional responsable de TIC en las Sedes de Presencia Nacional	S	A: Automático	Diario	3	5	15	Moderado
3	Simulacros de falla eléctrica y de datos al datacenter para comprobar el plan de recuperación de desastres	OTIC sedes Andinas y Profesional responsable de TIC en las Sedes de Presencia Nacional	S	M: Manual	Semestral	3	1	3	Bajo

5. TRATAMIENTO DEL RIESGO				
COD	ACTIVIDAD/PROYECTO	RESPONSABLE	FECHA DE EJECUCIÓN	VALOR APROXIMADO

6. RESPONSABLES DE LA IDENTIFICACION, VALORACION Y TRATAMIENTO DEL RIESGO				
ELABORACIÓN			APROBACIÓN	
NOMBRE:	ALEXIS MIGUEL TABORDA SALAZAR		NOMBRE:	GUSTAVO ADOLFO PÉREZ ZAPATA
CARGO:	JEFE		CARGO:	DIRECTOR
AREA:	OTIC SEDE MANIZALES		AREA:	DN TIC
FECHA:	FIRMA		FECHA:	FIRMA
21/09/2018			4/10/2018	

7. OBSERVACIONES
N/A