

 Universidad Francisco de Paula Santander Registo UTPB 2019	DIRECCIONAMIENTO ESTRATEGICO		CODIGO	FO-DE-05
			VERSION	02
	MAPA DE RIESGOS		FECHA	3/3/2026
			PAGINA	VER PIE PAGINA
ELABORÓ		REVISÓ		APROBÓ
Líder Direccionamiento Estratégico		Equipo Operativo de Calidad		Líder de Calidad

CONTROL ACTUALIZACIÓN DEL MAPA DE RIESGOS - PROCESO GESTIÓN DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN				
El presente control, establece el seguimiento a los procesos de actualización del Mapa de Riesgos, conforme al Monitoreo y Revisión definido en la Guía Metodologica de la Función Publica "Administración del Riesgo" versión Julio de 2016				
FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN	TOTAL DE RIESGOS IDENTIFICADOS	RIESGOS DE GESTIÓN IDENTIFICADOS	RIESGOS DE CORRUPCIÓN IDENTIFICADOS
4/16/2018	ACTUALIZACIÓN MAPA DE RIESGO	5	4	1
5/27/2019	ACTUALIZACIÓN MAPA DE RIESGO	5	4	1
12/21/2020	ACTUALIZACIÓN MAPA DE RIESGO	7	7	0
30/08/2023	ACTUALIZACIÓN MAPA DE RIESGO	10	9	1
14/11/2024	ACTUALIZACIÓN MAPA DE RIESGO	15	15	0
29/04/2025	ACTUALIZACIÓN MAPA DE RIESGO	15	14	1
17/09/2026	ACTUALIZACIÓN MAPA DE RIESGO	6	5	1

DIRECCIONAMIENTO ESTRATÉGICO																											CÓDIGO	FO-DE-05			
MAPA DE RIESGOS																											VERSIÓN	02			
																											FECHA	3/3/2026			
																											PÁGINA	VER FIC PÁGINA			
ELABORÓ										REVISÓ										APROBÓ											
Lider Direccionamiento Estratégico										Equipo Operativo de Calidad										Lider de Calidad											
FASE 1 - IDENTIFICACIÓN DEL RIESGO						FASE 2 - ANALISIS DEL RIESGO INHERENTE						FASE 3 -ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES						FASE 4 -ANÁLISIS DEL RIESGO RESIDUAL						FASE 5 - ACCIONES ASOCIADAS AL CONTROL							
RESPONSABLES		RIESGO IDENTIFICADO				CRITERIOS DE PROBABILIDAD	PROBABILIDAD INHERENTE	%	CRITERIOS DE IMPACTO	IMPACTO INHERENTE	%	ZONA DE RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ATRIBUTOS				AFECCIÓN FINAL	PROBABILIDAD RESIDUAL FINAL	%	IMPACTO RESIDUAL FINAL	%	ZONA DE RIESGO FINAL	TRATAMIENTO	DESCRIPCIÓN DE LAS ACCIONES	PERIODO DE EJECUCIÓN		REGISTROS / EVIDENCIAS	RESPONSABLES DE LA EJECUCIÓN DE LA ACCIÓN		
Nº.	PROCESO SIGC - UFPS	DEPENDENCIA RESPONSABLE	DESCRIPCIÓN DEL RIESGO	IMPACTO DEL RIESGO	CAUSA DEL RIESGO									CLASIFICACIÓN DEL RIESGO	TIPO	IMPLEMENTACIÓN	DOCUMENTACIÓN									EFECTIVIDAD	FECHA DE INICIO			FECHA DE TERMINACIÓN	
R1	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	Pérdida, corrupción o recuperación no exitosa de información institucional.	Económico y Reputacional	Errores humanos, eliminación accidental de información, fallas en almacenamiento, errores en bases de datos, respaldos incompletos o fallas durante procesos de recuperación.	Corrupción	Possible	Media	60%	Entre 100 y 500 SMLMV	Mayor	80%	Alto	Se implementan procedimientos para la protección y recuperación de la información institucional mediante la ejecución de copias de seguridad programadas de acuerdo con la criticidad de las plataformas, el uso de herramientas de respaldo, el almacenamiento seguro de la información, la realización de pruebas periódicas de restauración, el control de acceso a la información, la asignación de roles y permisos de acuerdo con las funciones y la capacitación del personal responsable, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información institucional.	Preventivo	Manual	Documentado	SI	Con Registros	PROBABILIDAD	Baja	36%	Mayor	80%	Alto	Reducir el Riesgo	Verificar periódicamente la ejecución de las copias de seguridad, realizar pruebas de restauración y actualizar los procedimientos de respaldo y recuperación de la información institucional.	21/07/2026	18/12/2026	Registros de ejecución de copias de seguridad, informes de pruebas de restauración, bitácoras de respaldo, registros de control de acceso y procedimientos actualizados.	Jefe División de Sistemas / Administrador de Infraestructura Tecnológica
R2	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	Interrupción o indisponibilidad de plataformas y servicios tecnológicos institucionales.	Económico y Reputacional	Fallas eléctricas, daños de hardware, fallas de UPS, fallas de servidores, fallas de comunicaciones, SAN (Storage Area Network), almacenamiento, obsolescencia tecnológica o interrupciones en componentes críticos de infraestructura.	Tecnológico	Possible	Media	60%	Entre 10 y 50 SMLMV	Menor	40%	Moderado	Se implementan procedimientos para garantizar la disponibilidad de las plataformas y servicios tecnológicos institucionales mediante el mantenimiento preventivo y correctivo de la infraestructura tecnológica (servidores, sistemas de almacenamiento - SAN, UPS, planta eléctrica y demás componentes críticos), el monitoreo de los recursos tecnológicos, la protección del suministro eléctrico (UPS, planta eléctrica y DPS), el seguimiento al estado de la infraestructura y la gestión oportuna de las solicitudes de mantenimiento y soporte ante las áreas o proveedores responsables.	Preventivo	Automático	Documentado	SI	Con Registros	PROBABILIDAD	Baja	30%	Menor	40%	Moderado	Reducir el Riesgo	Gestionar y hacer seguimiento a los mantenimientos preventivos y correctivos de la infraestructura tecnológica (servidores, Red de Área de Almacenamiento SAN, Sistema de Alimentación ininterrumpida (UPS), Dispositivo de Protección contra Sobretensiones (DPS), planta eléctrica, red y demás componentes críticos), así como a la renovación de soportes y garantías con las áreas o proveedores responsables.	21/07/2026	18/12/2026	Solicitudes y registros de monitoreo de servidores, Red de Área de Almacenamiento SAN, Sistema de Alimentación ininterrumpida (UPS), Dispositivo de Protección contra Sobretensiones (DPS), planta eléctrica, red y demás componentes críticos), actas de soporte técnico y renovaciones de garantía o soporte.	Jefe División de Sistemas / Administrador de Infraestructura Tecnológica
R3	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	Compromiso de la confidencialidad, integridad y disponibilidad de la información y de los sistemas institucionales.	Económico y Reputacional	Malware, ransomware, vulnerabilidades de software, configuraciones inseguras, credenciales comprometidas o accesos indebidos.	Tecnológico	Possible	Media	60%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Se implementan procedimientos para garantizar la seguridad de la información y de los sistemas institucionales mediante la administración de perfiles y controles de acceso, el uso de herramientas de protección informática (antivirus y demás mecanismos de seguridad), la gestión de actualizaciones, el monitoreo de eventos de seguridad y la capacitación del personal responsable, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información institucional.	Preventivo	Automático	Documentado	SI	Con Registros	PROBABILIDAD	Baja	30%	Moderado	60%	Moderado	Reducir el Riesgo	Verificar la actualización de los mecanismos de seguridad informática, revisar periódicamente los perfiles de acceso, fortalecer la gestión de vulnerabilidades y promover la capacitación del personal en seguridad de la información.	21/07/2026	18/12/2026	Reportes de antivirus, registros de actualizaciones, informes de revisión de perfiles de acceso, bitácoras de incidentes de seguridad y registros de capacitaciones.	Jefe División de Sistemas / Administrador de Servidores
R4	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	Afectación de la infraestructura tecnológica por factores físicos, ambientales o de acceso físico no autorizado.	Económico y Reputacional	Temperatura inadecuada, humedad, filtraciones, incidentes físicos o ingreso no autorizado a áreas críticas.	Tecnológico	Improbable	Baja	40%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Se implementan procedimientos para garantizar la seguridad de la información y de los sistemas institucionales mediante la administración de perfiles y controles de acceso, el uso de herramientas de protección informática (antivirus y demás mecanismos de seguridad), la gestión de actualizaciones, el monitoreo de eventos de seguridad y la capacitación del personal responsable, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información institucional.	Preventivo	Manual	Documentado	SI	Con Registros	PROBABILIDAD	Baja	24%	Moderado	60%	Moderado	Reducir el Riesgo	Gestionar la adquisición, implementación y seguimiento de los controles físicos y ambientales de la sala de servidores (termohigrometro, sensores de temperatura y humedad, alarmas, control de acceso y monitoreo), realizando seguimiento a las solicitudes presentadas ante las dependencias competentes y a las gestiones realizadas para su adquisición e implementación.	21/07/2026	18/12/2026	Registros de ingreso a la sala de servidores, reportes de cámaras de seguridad, solicitudes de mantenimiento de infraestructura, informes de inspección y seguimiento a condiciones ambientales.	Jefe División de Sistemas / Administrador de Infraestructura Tecnológica
R5	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	Incumplimiento o retraso en la prestación de servicios tecnológicos institucionales.	Económico y Reputacional	Alta demanda de solicitudes, limitaciones de recursos, priorización inadecuada, requerimientos incompletos o dependencia de terceros.	Operativo	Possible	Media	60%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Se implementan procedimientos para garantizar la prestación oportuna de los servicios tecnológicos institucionales mediante la recepción, priorización, asignación, seguimiento y control de las solicitudes, el monitoreo de los tiempos de atención, la ejecución de actividades de soporte y desarrollo, y el seguimiento a los indicadores de gestión, con el fin de asegurar el cumplimiento de los compromisos establecidos con la comunidad universitaria.	Preventivo	Manual	Documentado	SI	Con Registros	PROBABILIDAD	Baja	36%	Moderado	60%	Moderado	Reducir el Riesgo	Realizar seguimiento a los indicadores del Gestor de Actividades, revisar periódicamente los tiempos de atención y establecer acciones de mejora para optimizar la prestación de los servicios tecnológicos institucionales.	21/07/2026	18/12/2026	Reportes del Gestor de Actividades, indicadores de gestión, estadísticas de atención, actas de seguimiento y planes de mejora.	Jefe División de Sistemas / Líderes de Grupo de la División de Sistemas

 Universidad del Pacífico UNIVERSITY OF THE PACIFIC		DIRECCIONAMIENTO ESTRATÉGICO																								CÓDIGO		FO-DE-05					
		MAPA DE RIESGOS																								VERSIÓN		02					
																										FECHA		3/3/2026					
		PÁGINA		VER FIE PÁGINA																													
ELABORÓ										REVISÓ										APROBÓ													
Líder Direccionamiento Estratégico										Equipo Operativo de Calidad										Lider de Calidad													
FASE 1 - IDENTIFICACIÓN DEL RIESGO										FASE 2 - ANALISIS DEL RIESGO INHERENTE						FASE 3 -ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES						FASE 4 -ANÁLISIS DEL RIESGO RESIDUAL						FASE 5 - ACCIONES ASOCIADAS AL CONTROL					
RESPONSABLES			RIESGO IDENTIFICADO					CRITERIOS DE PROBABILIDAD	PROBABILIDAD INHERENTE	%	CRITERIOS DE IMPACTO	IMPACTO INHERENTE	%	ZONA DE RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	ATRIBUTOS					AFECTACIÓN FINAL	PROBABILIDAD RESIDUAL FINAL	%	IMPACTO RESIDUAL FINAL	%	ZONA DE RIESGO FINAL	TRATAMIENTO	DESCRIPCIÓN DE LAS ACCIONES	PERIODO DE EJECUCIÓN		REGISTROS / EVIDENCIAS	RESPONSABLES DE LA EJECUCIÓN DE LA ACCIÓN	
No.	PROCESO SIGC - UFPS	DEPENDENCIA RESPONSABLE	DESCRIPCIÓN DEL RIESGO	IMPACTO DEL RIESGO	CAUSA DEL RIESGO	CLASIFICACIÓN DEL RIESGO	Tipo									IMPLEMENTACIÓN	CAUSACIÓN	DOCUMENTACIÓN	FRECUENCIA ADECUADA	EFECTIVIDAD									FECHA DE INICIO	FECHA DE TERMINACIÓN			
RS	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	Insuficiente capacidad de recuperación y continuidad operativa ante incidentes o desastres tecnológicos.	Económico y Reputacional	Ausencia de infraestructura de contingencia, falta de servidores de respaldo, inexistencia de un plan formal de recuperación ante desastres o recursos insuficientes para recuperación.	Operativo	Improbable	Baja	40%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Se implementan procedimientos para fortalecer la recuperación y continuidad operativa de los servicios tecnológicos mediante la ejecución de pruebas de restauración, la actualización de los procedimientos de recuperación, la identificación de necesidades de infraestructura de contingencia, el seguimiento a los mecanismos de recuperación disponibles y la gestión de las acciones requeridas para mejorar la capacidad de respuesta ante incidentes o desastres tecnológicos.	Preventivo	Manual	Documentado	Si	Con Registros	PROBABILIDAD	Baja	24%	Moderado	60%	Moderado	Reducir el riesgo	Actualizar los procedimientos de recuperación y continuidad operativa, realizar pruebas periódicas de recuperación y gestionar la implementación de infraestructura de contingencia de acuerdo con la disponibilidad de recursos institucionales.	21/01/2026	18/12/2026	Informes de pruebas de recuperación, procedimientos de continuidad y recuperación actualizados, actas de seguimiento, cotizaciones, comunicaciones y seguimiento relacionados con la adquisición e implementación del termohigómetro y demás controles ambientales, relacionados con infraestructura de contingencia.	Jefe División de Sistemas / Administrador de Infraestructura Tecnológica		