Universidad Francisco de Paula Santander	DIRECCIONAMIENTO ESTRATEGICO	CODIGO	FO-DE-05
		VERSION	02
	MAPA DE RIESGOS	FECHA	3/3/2026
		PAGINA	VER PIE PAGINA

ELABORÓ	REVISÓ	APROBÓ
Líder Direccionamiento Estrategico	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
9/04/2026	ACTUALIZACIÓN MAPA DE RIESGO	14	13	1

FASE 1 - IDENTIFICACIÓN DEL RIESGO							FASE 2 - ANALISIS DEL RIESGO INHERENTE						FASE 3 -ANALISIS Y EVALUACIÓN DE LOS CONTROLES							FASE 4 - ANALISIS DEL RIESGO RESIDUAL						FASE 5 - ACCIONES ASOCIADAS AL CONTROL				
RESPONSABLES			RIESGO IDENTIFICADO											ATRIBUTOS													PERIODO DE EJECUCIÓN			
No.	PROCESO SIGC - UFPS	DEPENDENCIA RESPONSABLE	DESCRIPCIÓN DEL RIESGO	IMPACTO DEL RIESGO	CAUSA DEL RIESGO	CLASIFICACIÓN DEL RIESGO	CRITERIOS DE PROBABILIDAD	PROBABILIDAD INHERENTE	%	CRITERIOS DE IMPACTO	IMPACTO INHERENTE	%	ZONA DE RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	TIPO	IMPLEMENTACIÓN	CALIFICACIÓN	DOCUMENTACIÓN	FRECUENCIA ADECUADA	EVIDENCIAS	AFECTACIÓN FINAL	PROBABILIDAD RESIDUAL FINAL	%	IMPACTO RESIDUAL FINAL	%	ZONA DE RIESGO FINAL	TRATAMIENTO	DESCRIPCIÓN DE LAS ACCIONES	FECHA DE INICIO	FECHA DE TERMINACIÓN	REGISTROS / EVIDENCIAS	RESPONSABLES DE LA EJECUCIÓN DE LA ACCIÓN
R1	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	PÉRDIDA DE LA INFORMACIÓN	Económico y Reputacional	Eliminación de datos por parte de un profesional de la dependencia.	Operativo	Rara vez	Muy Baja	20%	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	Capacitación al personal de la dependencia para el manejo adecuado de la base de datos .	Preventivo	Manual	40%	Sin Documentar	NO	Sin Registros	PROBABILIDAD	Muy Baja	12%	Leve	100%	Bajo	Reducir el Riesgo	Capacitación al personal adscrito a la dependencia para el manejo de datos	20/1/2026	20/6/2026	Asistencia a capacitación	JEFE DIVISIÓN DE SISTEMAS
R2	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	PÉRDIDA DE LA INFORMACIÓN	Económico y Reputacional	Alteración o eliminación de la información técnica y administrativa registrada en los sistemas de información en favorecimiento de un tercero. —Eliminación de datos por parte de una persona externa a la dependencia.	Corrupción	Posible	Media	60%	Entre 10 y 50 SMLMV	Menor	40%	Moderado	Políticas de control de acceso para el personal interno y externo a la División de sistemas	Preventivo	Automático	50%	Documentado	Si	Con Registros	PROBABILIDAD	Baja	30%	Menor	40%	Moderado	Reducir el Riesgo	Ejecución del plan de auditoría interna para revisión de acceso a la base de datos	1/1/2026	30/12/2026	Dentro de las evidencias para la auditoria se encuentran **1.** Documento Plan de implementacion De Cambios: Es un archivo que contiiena cada uno de las modificaciones o desarrollos realizados a los portales que la Division De sistemas da soporte en el formato de Plan de implementacion de cambios **2.** Listado Software División de Sistemas: Es un listado de todos los portales y aplicativos a los que la Division De sistemas da Soporte **3.** Formato Auditoria Bicbucket : En esta auditira interna se confirman los cambios realizados a todos los portales y aplicativos a los que la Division De sistemas da Soporte	JEFE DIVISIÓN DE SISTEMAS/ Profesional Universitario
R3	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	PÉRDIDA DE LA INFORMACIÓN	Económico y Reputacional	Daño en la infraestructura tecnológica de la dependencia	Operativo	Rara vez	Muy Baja	20%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Adquisicion de equipos para tener redundancia en caso de daño	Preventivo	Manual	40%	Sin Documentar	SI	Con Registros	PROBABILIDAD	Muy Baja	12%	Moderado	60%	Moderado	Reducir el Riesgo	Presentar propuesta para la compra de equipos de respaldo	21/01/2026	20/06/2026	buscar solicitud por datarsoft	JEFE DIVISIÓN DE SISTEMAS/ Profesional Universitario
R4	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	DEMORA EN LA ENTREGA DE INFORMACION REQUERIDA	Económico y Reputacional	Informacion suministrada para la gestión requerimientos erroneos o incompletos	Operativo	Probable	Alta	80%	Entre 10 y 50 SMLMV	Menor	40%	Moderado	Envio de correos y colocar avisos informativos en los portales detallando la informacion necesaria	Preventivo	Manual	40%	Sin Documentar	SI	Sin Registros	PROBABILIDAD	Media	48%	Menor	40%	Moderado	Reducir el Riesgo	Articulacion adecuada de la informacion suministrada por los solicitantes para la gestion de los requerimiento	21/01/2026	20/06/2026	Correos, Datarsoft con link's donde se indique los datos necesarios para dar solucion al requeerimiento	JEFE DIVISIÓN DE SISTEMAS/ Profesional Universitario
R5	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	DEMORA EN EL PROCESAMIENTO Y GENERACIÓN DE HERRAMIENTAS DE SOFTWARE	Económico y Reputacional	Falta de planificación y gestión oportuna de los requerimientos de software por parte de los líderes de proceso, lo que limita la adecuada definición de necesidades funcionales para la operación de las herramientas tecnológicas.	Operativo	Probable	Alta	80%	Entre 10 y 50 SMLMV	Menor	40%	Moderado	Gestión anticipada de requerimientos, a través de reuniones periódicas con los líderes de procesos, con el fin de identificar, definir y actualizar las necesidades de software que garanticen la disponibilidad y funcionamiento adecuado de las herramientas tecnológicas.	Preventivo	Manual	40%	Sin Documentar	SI	Sin Registros	PROBABILIDAD	Media	48%	Menor	40%	Moderado	Reducir el Riesgo	Programar y realizar reuniones periódicas con los líderes de procesos para la identificación, análisis, definición y actualización de requerimientos de software, así como el seguimiento a los compromisos establecidos para garantizar la disponibilidad y funcionamiento de las herramientas tecnológicas.	21/01/2026	20/06/2026	Actas de reuniones y registros de seguimiento de requerimientos de software, que evidencien la identificación, análisis, actualización y control de los requerimientos, así como los compromisos adquiridos y su respectivo seguimiento.	JEFE DIVISIÓN DE SISTEMAS/ Profesionales Universitarios
R6	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	Sobresaltos de energía por intermitencias.	Operativo	Rara vez	Muy Baja	20%	Entre 100 y 500 SMLMV	Mayor	80%	Alto	Adquisicion de equipos que permitan suprimir los picos de voltaje	Preventivo	Manual	40%	Sin Documentar	SI	Sin Registros	PROBABILIDAD	Muy Baja	12%	Mayor	80%	Alto	Evitar el Riesgo	Solicitud de compra de supresores de picos de voltaje	21/01/2026	20/06/2026	Correo con cotización y envío de solicitud a la alta dirección de la organización	JEFE DIVISIÓN DE SISTEMAS/ Profesional Universitario
R7	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	Falla de la planta electrica por, daño en la bateria, falta de combustible o daño del motor	Operativo	Rara vez	Muy Baja	20%	Entre 10 y 50 SMLMV	Menor	40%	Bajo	Realizacion mantenimiento preventivo cada 2 años	Preventivo	Manual	40%	Sin Documentar	SI	Sin Registros	PROBABILIDAD	Muy Baja	12%	Menor	40%	Bajo	Evitar el Riesgo	Solicitud de mantenimiento a servicios generales de la universidad Francisco de Paula Santander	21/01/2026	20/06/2026	Correo de registros de solicitud de mantenimiento	JEFE DIVISIÓN DE SISTEMAS/ Profesional Universitario
R8	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	falla de la bateria de las ups debido al deterioro	Operativo	Rara vez	Muy Baja	20%	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	Monitoreo diario del estado de alarmas de las ups	Preventivo	Manual	40%	Sin Documentar	SI	Sin Registros	PROBABILIDAD	Muy Baja	12%	Moderado	60%	Moderado	Evitar el Riesgo	Revisar diariamente las alertas visuales y acústicas que tienen las ups	21/01/2026	20/06/2026	Revision visual del sensores de humo instalado, minuta de vigilancia grabación de cámaras y solicitud de compra al de sensores de temperatura	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIERO DE SERVIDORES)
R9	Gestión de Tecnologias y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	Deficiencias en los controles de seguridad de la información, relacionadas con la gestión de accesos, asignación de roles y monitoreo de los sistemas, que pueden facilitar la materialización de amenazas como malware o ransomware.	Operativo	Rara vez	Muy Baja	20%	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	Implementación de políticas de seguridad de la información en los dispositivos informáticos institucionales, que incluyan la gestión de accesos y asignación de roles de usuario, así como la instalación y actualización permanente de software antivirus, actualización de los sistemas operativos y el monitoreo continuo de los equipos, con el fin de prevenir incidentes de seguridad como malware o ransomware.	Preventivo	Manual	40%	Documentado	SI	Con Registros	PROBABILIDAD	Muy Baja	12%	Leve	100%	Bajo	Evitar el Riesgo	Realizar la instalación y actualización de software antivirus en los equipos institucionales, la gestión y bloqueo de cuentas de usuario según corresponda, y el monitoreo diario del estado de conectividad de las computadoras a las herramientas de control de seguridad, con el fin de verificar el correcto funcionamiento del antivirus y la actualización del sistema operativo.	21/01/2026	20/06/2026	**1.** Reportes generados desde el dashboard del antivirus que evidencien el estado de protección y actualización de los equipos. **2.** Inventario actualizado de activos tecnológicos, y registros de usuarios con la asignación de roles y control de accesos, como soporte del monitoreo y gestión de la seguridad de la información.	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIERO DE SERVIDORES)

Universidad Francisco de Paula Santander	DIRECCIONAMIENTO ESTRATÉGICO	CÓDIGO	FO-DE-05
		VERSIÓN	02
	MAPA DE RIESGOS	FECHA	3/3/2026
		PÁGINA	VER PIE PAGINA

ELABORÓ	REVISÓ	APROBÓ
Líder Direccionamiento Estratégico	Equipo Operativo de Calidad	Líder de Calidad

FASE 1 - IDENTIFICACIÓN DEL RIESGO							FASE 2 - ANALISIS DEL RIESGO INHERENTE							FASE 3 -ANALISIS Y EVALUACIÓN DE LOS CONTROLES								FASE 4 - ANALISIS DEL RIESGO RESIDUAL						FASE 5 - ACCIONES ASOCIADAS AL CONTROL				
RESPONSABLES			RIESGO IDENTIFICADO												ATRIBUTOS															PERIODO DE EJECUCIÓN			
No.	PROCESO SIGC - UFPS	DEPENDENCIA RESPONSABLE	DESCRIPCIÓN DEL RIESGO	IMPACTO DEL RIESGO	CAUSA DEL RIESGO	CLASIFICACIÓN DEL RIESGO	CRITERIOS DE PROBABILIDAD	PROBABILIDAD INHERENTE	%	CRITERIOS DE IMPACTO	IMPACTO INHERENTE	%	ZONA DE RIESGO INHERENTE	DESCRIPCIÓN DEL CONTROL	TIPO	IMPLEMENTACIÓN	CALIFICACIÓN	DOCUMENTACIÓN	FRECUENCIA ADECUADA	EVIDENCIAS	AFECTACIÓN FINAL	PROBABILIDAD RESIDUAL FINAL	%	IMPACTO RESIDUAL FINAL	%	ZONA DE RIESGO FINAL	TRATAMIENTO	DESCRIPCIÓN DE LAS ACCIONES	FECHA DE INICIO	FECHA DE TERMINACIÓN	REGISTROS / EVIDENCIAS	RESPONSABLES DE LA EJECUCIÓN DE LA ACCIÓN
R10	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	Posibles fallas en la gestión, operación y supervisión de los controles de acceso físico (biométrico, vigilancia permanente y circuito cerrado de televisión) en la División de Sistemas, particularmente en la sala de servidores, que podrían permitir el ingreso no autorizado a áreas críticas.	Tecnológico	Improbable	Baja	40%	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	Acceso biométrico y vigilancia permanente	Preventivo	Automático	50%	Documentado	Si	Con Registros	PROBABILIDAD	Muy Baja	20%	Leve	100%	Bajo	Evitar el Riesgo	Implementar y garantizar el funcionamiento continuo de los sistemas de control de acceso biométrico y la vigilancia física permanente las 24 horas del día, apoyados en el circuito cerrado de televisión, en la División de Sistemas, especificamente en la sala de servidores.	21/01/2026	20/06/2026	Registros generados por el sistema biométrico de control de acceso, bitácoras de ingreso y salida del personal, reportes de vigilancia 24/7, así como grabaciones y reportes del circuito cerrado de televisión (CCTV) que evidencien el control de acceso a la División de Sistemas y a la sala de servidores.	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIERO DE SERVIDORES)
R11	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	PÉRDIDA DE LA INFORMACIÓN	Económico y Reputacional	Debilidades en la gestión de los procesos de respaldo de la información, relacionadas con la falta de monitoreo, verificación y control en la ejecución de las copias de seguridad de las máquinas virtuales y bases de datos institucionales.	Operativo	Rara vez	Muy Baja	20%	Entre 10 y 50 SMLMV	Menor	40%	Bajo	Gestión de la adquisición y renovación de licencias del software de copias de seguridad, junto con el monitoreo continuo de la infraestructura tecnológica utilizada para la ejecución de los respaldos, y la renovación de la licencia de Google Workspace (G Suite) para garantizar el almacenamiento seguro de la información en la nube.	Preventivo	Manual	40%	Documentado	Si	Con Registros	PROBABILIDAD	Muy Baja	12%	Menor	40%	Bajo	Evitar el Riesgo	Ejecutar procesos automatizados de copias de seguridad de las máquinas virtuales y bases de datos, incluyendo su respaldo en medios físicos externos y almacenamiento en la nube, así como la transferencia controlada de la información del servidor, con el fin de garantizar la disponibilidad, integridad y resguardo de la información institucional.	21/01/2026	20/06/2026	Licencias vigentes del software de copias de seguridad, registros de monitoreo de la infraestructura de respaldo y evidencia de almacenamiento de copias de seguridad en la nube mediante Google Workspace (G Suite).	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIERO DE SERVIDORES)
R12	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	Debilidades en la gestión del monitoreo de las condiciones ambientales (temperatura y entorno) en la sala de servidores, asociadas a la falta de sensores adecuados y control continuo.	Operativo	Rara vez	Muy Baja	20%	Entre 100 y 500 SMLMV	Mayor	80%	Alto	Monitoreo permanente del ambiente de la sala de servidores	Preventivo	Manual	40%	Sin Documentar	Si	Sin Registros	PROBABILIDAD	Muy Baja	12%	Mayor	80%	Alto	Evitar el Riesgo	Instalación de sensores de temperatura y alarmas y vigilancia las 24 horas del día	21/01/2026	20/06/2026	Revision visual del sensores de humo instalado, minuta de vigilancia grabación de cámaras y solicitud de compra al de sensores de temperatura	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIERO DE SERVIDORES)
R13	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	DAÑO EN LA INFRAESTRUCTURA TECNOLÓGICA	Económico y Reputacional	incendio en la sala servidores	Operativo	Rara vez	Muy Baja	20%	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	Monitoreo permanente de las condiciones ambientales y de seguridad en la sala de servidores, incluyendo vigilancia continua y control del entorno.	Preventivo	Manual	40%	Sin Documentar	Si	Sin Registros	PROBABILIDAD	Muy Baja	12%	Leve	100%	Bajo	Evitar el Riesgo	Instalar y mantener sensores de humo, así como garantizar la vigilancia permanente las 24 horas del día en la sala de servidores.	21/01/2026	20/06/2026	Registros de instalación y funcionamiento de sensores de humo, bitácoras de vigilancia, grabaciones del sistema de circuito cerrado de televisión (CCTV) y reportes de monitoreo de la sala de servidores.	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIERO DE SERVIDORES) / PERSONAL DE VIGILANCIA
R14	Gestión de Tecnologías y Sistemas de Información	División de Sistemas	DESACTUALIZACIÓN DE LA PLATAFORMA INFORMÁTICA	Económico y Reputacional	Fin del ciclo de vida del software de desarrollo	Tecnológico	Probable	Alta	80%	Afectación menor a 10 SMLMV	Leve	20%	Moderado		Correctivo	Manual	20%	Documentado	Si	Con Registros	IMPACTO	Muy Alta	80%	Leve	16%	Alto	Reducir el Riesgo	Capacitación en las nuevas tecnologías, solicitud de licencia de los entornos de desarrollo, adquisición de licencias de sistemas operativos, organización en la realización de las solicitudes a la división.	21/01/2026	20/06/2026	Manuales de los módulos de software actualizados , solicitud de capacitación , solicitud de compra de licencias necesarias para el desarrollo de software y renovación de los sistemas operativos	JEFE DIVISIÓN DE SISTEMAS / Profesional Universitario (INGENIEROS DE DE SOPORTE Y DESARROLLO) /