CONSOLIDADO MAPA DE RIESGOS VIGENCIA 2025

Fecha	31/01/2025

Proceso	Mapa de Riesgos de Seguridad Digital						Acciones preventivas		
	Tipo de riesgo	Causa	Riesgo	Consecuencias	Control	Nivel Residual	Acción	Fecha de inicio	Fecha final
Almecen e Inventarios	Seguridad DIgital	1. Existe la posibilidad de que la información sea perdida o manipulada de manera inapropiada, lo que podría comprometer la exactitud y la integridad de los datos almacenados. 2. Las fallas tecnológicas en el sistema de información Gestasoft pueden ocasionar que los datos se procesen de manera incorrecta, afectando la fiabilidad del sistema y la calidad de la información disponible.	Perdida de la información en el sistema	1. La generación de información inconsistente puede dificultar la toma de decisiones, ya que los datos no reflejan la realidad de manera precisa. 2. El acceso no autorizado a la información podría resultar en la divulgación indebida de datos confidenciales o en su manipulación por parte de personal no autorizado, comprometiendo la seguridad y la privacidad de la información.	el lider del proceso informa a soporte técnologico periodocamente la suspension de roles al personal que no tiene contratación.	Bajo	El líder de la oficina de Adquisiciones y Almacén, junto con el profesional universitario de apoyo, solicita a soporte tecnológico la suspensión de roles para el personal no contratado. Esta actividad se lleva a cabo cada vez que se necesite realizar dicha solicitud.	5 semana del mes de junio	5 semana del mes de diciembre
Apoyo al egresado	Seguridad DIgital	• Uso de datos personales de egresados para fines ajenos a la academia.	Manipulación de los datos de los egresados con fines comerciales.	Pérdida de confianza en la Institución de parte de los graduados por efecto de campañas publicitarias indeseadas en su correo electrónico o teléfono celular	La universidad cuenta con el aplicativo academusoft - modulo adminsitrador egresados, para acceder a los datos del modulo, se debe realizar solicitud mediante el CAT por parte del lider del proceso para la asignación roll Egresado-Administrador.	Moderado	• Solicitar al CIADTI, la relación del personal autorizado para realizar la depuración del personal con acceso al modulo egresado - administrador.	2024-06-01	2024-07-30
							• Incluir en los correos donde se comparta la base de datos de los egresados la Política de privacidad datos sensibles.	2025-01-18	2025-12-15
Asesoría Juridica	Seguridad DIgital	1. Errores humanos en la gestión y administración de las herramientas asociadas a la Oficina de Asesoría Jurídica 2. Ausencia de copias de respaldo de información 3. Falta de conocimiento en el uso de los aplicativos por parte de los funcionarios encargados 4. Falta de monitoreo y mantenimiento en los servicios de la infraestructura tecnológica y equipos 6. Soporte técnico inadecuado. 7. Falta de copias de respaldo de información local	Indebida administración y uso de las herramientas tecnológicas por parte del personal de la oficina	1. Afectación en la imagen y credibilidad de la entidad.2. Afectación en el tratamiento de información, confidencialidad y datos de procesos internos y de terceros 3. sanciones por parte de entes de control 4. Obstaculización del flujo normal de los procesos 5. Pérdida de la información almacenada de manera local	Monitoreo y gestión constante de las herramientas utilizadas para el desarrollo de las actividades de la Oficina de Asesoría Jurídica; en especial de las cuentas de correo electrónico a través del cambio de contraseñas cuando se requiera.	Alto	1) cambio de claves semestral y/o cuando hay cambio de personal y se requiera por seguridad de la información y continuidad de los procesos realizar gestión de contraseña sobre la cuenta asignada. Periodicidad: semestral. 2.) Solicitud de capacitación a la oficina de archivo central para el uso y cargue correcto de los documentos en las bases de datos de la oficina. Periodicidad: Semestral o cada que se requiera. 3. Solicitud y realización de de copia de respaldo de información de archivo local de los equipos de la Oficina de Asesoría Jurídica. Periodicidad: semestral 4.Solicitud de aplicación de soporte y mantenimiento de hadware y software. Periodicidad: semestral	07/01/2025	30/06/2025
Atención al ciudadano	Seguridad DIgital	1, Fallas constantes en el internet de la Universidad. 2, Falla en los servidores que alojan el programa. 3, Fallas en aplicativois internos y/o externos.	6. Pérdida de la capacidad de tramitar PQRSDF debido a fallas tecnológicas y cibernéticas en los aplicativos web de uso constante en la dependencia (MÓDULO PQRSDF, CHAT EN LÍNEA, WHATSAPP Y CORREO ELECTRÓNICO) que generan demora en las respuestas.	1, Demora en la respuesta o información de trámite de las PQRSDF presentadas en los aplicativos web. 2, Sanciones disciplinarias y judiciales por la imposibilidad de gestión de las PQRSDF y vencimiento de términos	La Oficina de Atención al Ciudadano y Transparencia realizará seguimiento a las posibles fallas en los aplicativos web e informará al soporte técnico de cada canal de atención de la dependencia; sea cual sea el canal que falle se mantendrá informadas a las partes interesadas cuando alguna de estas fallas se presente y su motivo; así mismo se informará cuando se habiliten nuevamente mediante sus canales oficiales de publicación y página web institucional. Cabe resaltar que, para conocimiento de la comunidad universitaria esto se plasmará en los resultados del informe PQRSDF.	Moderado	El Jefe de Atención al Ciudadano y Transparencia y el equipo de apoyo realizarán el reporte y seguimiento cada dos meses mediante acta de las fallas tecnológicas hasta lograr el correcto funcionamiento de los canales de atención para garantizar la recepción y trámite de solicitudes mediante medios tecnológicos e informará mediante memorando a soporte técnológico (en caso de módulo PQRSDF) y en chat con (SOPORTE TÉCNICO TAWK.TO) mediante comunicación, Cuando se trate del correo electrónico por caída de internet o virus del equipo de trabajo, se hará reporte al administrador de correos para que se pueda gestionar su reparación, a fin de lograr el correcto funcionamiento de los canales para garantizar la recepción y trámite de solicitudes mediante medios tecnológicos. (10)	Cada dos meses	Cada dos meses
							El Jefe de Atención al Ciudadano y Transparencia su equipo de apoyo mantendrá informadas a las partes interesadas cuando algún canal de atención falle y su motivo, así mismo cuando se habilite nuevamente mediante sus canales oficiales de publicación y página web institucional, de igual forma, se socializará como plan de contigencia la recepción de PQRSDF en formato físico de ser necesario. Para conocimiento de la comunidad universitaria se plasmarán los resultados en el informe PQRSDF Trimestral. (11)	Primera quincena de cada cuatrimestre	Primera quincena de cada cuatrimestre

CEDIMOL	Seguridad DIgital	Bajo nivel de seguridad en los servidores del laboratorio.	Acceso no autorizado a las bases de datos de los pacientes almacenadas en el laboratorio clínico CEDIMOL.	Perdida y/o alteración de la informacion almacenada en las bases de datos de los pacientes. Sanciones y multas	Se realiza la instalación y aplicación de software que permite el control de la información en el servidor contra robo de información o hackeo, Politica de acceso cruzado, ingreso a la plataforma con una IP determinada, acceso basado en tokens, control de acceso basado en roles (niveles de acceso a personal determinado), cifrado de la información y contraseña basado en acceso de datos, CAPTCHA (evita ataques de fuerza bruta), proteccion de puertos con firewall, helmet en ingles evita mostrar que tecnologias hay en el servidor, informacion sensible declarada en variables de entorno, para el mantenimiento del aplicativo se utiliza acceso remoto SSH con credenciales por computadora para poder acceder remoto.	Bajo	Contratación del ingeniero de desarrollo con experiencia y capacitado para crear, actualizar y mantener la seguridad de las plataformas del laboratorio.	De acuerdo al ingreso de personal al laboratorio	De acuerdo al ingreso de personal al laboratorio
							Constante actualización y verificación de la seguridad en las plataformas	Marzo	Diciembre
Cominación Y Prensa	Seguridad DIgital	1. Infraestructura tecnológica para realizar el almacenamiento, protección y catalogación de archivo audiovisual. 2. Daños en los Discos duros extraíbles	Posibilidad de Pérdida de archivo digital: Audivisual y fotográficos.	1. Perdida de la memoria audiovisual y Fotográfica de la Universidad de Pamplona	La oficina de comunicacion y prensa en la actualidad realiza un seguimiento trimestral a través de las reuniones de grupo de mejoramiento lideradas por la directora de la oficina, en la que se revisa la actualización del archivo fotografico y la manera en la cual se esta realizando, esta informacion se esta guardando en la memoria del correo institucional de la oficina ofiprensa@unipamplona.edu.co, donde la persona responsable envia desde su correo institucional la descripcion de las fotos tomadas, el lugar y cantidad de imagenes enviadas esto con el fin de poder hacer uso de las misas, asimismo, cargando al aplicativo de SharePoint	Bajo	La oficina de comunicación y prensa con el objetivo de prevenir el riesgo tomara como acción preventiva la creación y uso de un almacenamiento en línea a través de sharepoint y OneDrive, en donde será cargado el archivo digital: Audiovisual y fotográfico por parte de cada uno de los funcionarios vinculados a la oficina, previa a una capacitación realizada por un profesional designado por la líder del proceso, el acceso a el almacenamiento el línea se realizara a través del correo institucional. De igual modo se cuenta con discos duros en donde se almacena igualmente la información por carpetas por año, mes y actividad. Como evidencia del cumplimiento de esta actividad, trimestralmente a través de reunión se realizara la verificación del cargue de la información y se dejara establecido bajo acta.	11 de marzo - 09 de Junio - 15 de septiembre - 09 de diciembre	Segunda semana de cada trimestre del año 2025
Cominación Y Prensa	Seguridad DIgital	1.Polvo, corrosión, congelamiento y derrame de líquidos debido al consumo de alimentos en los puestos de trabajo. 2. Falta de conciencia en el uso de los equipos tecnológicos. 3. Falta de cuidado de los equipos tecnológicos	Daño físico de los equipos tecnológicos	1. No contar con los equipos apropiados y en buenas condiciones para el apoyo de las diferentes actividades institucionales. 2. Saturación y daño por exceso en el uso de un solo equipo	1. Los profesionales encargados del uso de los diferentes equipos existentes en la oficina de Comunicación y Prensa realizaran mantenimiento preventivo de los equipos que ellos utilicen. 2 El Jefe de la Oficina de prensa revisara de manera trimestral las condiciones de los equipos. 3. El jefe de la oficina de Comunicación y Prensa o el contratista encargado, solicitarán el mantenimiento preventivo de los equipos.	Moderado	La directora de la oficina de Comunicación y Prensa como líder del proceso asignara a un profesional de la oficina para realizar seguimiento y monitoreo de los equipos, dejando como evidencia en un informe semestral, además se solicitara un mantenimiento con la dependencia encargada, para la revisión de software y sistema del equipo.	09 de junio - 09 de diciembre	Segunda semana de junio y segunda semana de diciembre
Control Interno de Gestión	Seguridad DIgital	Falta a la Ética Profesional por parte de los funcionarios de la Institución y del proceso de Control Interno de Gestión. Inadecuado manejo de roles y privilegios del personal con acceso a la información Ausencia de acuerdos de confidencialidad Incumplimiento de políticas de contraseñas seguras	Pérdida de confidencialidad de la información clasificada, reservada o en construcción que está bajo responsabilidad de la dependencia debido al incumplimiento de las políticas de seguridad de la información institucionales	Utilizar información clasificada y reservada en beneficio propio o de terceros. Acceso de la información por parte de personal no autorizado Pérdida de la imagen institucional y del proceso Acceso de la información por parte de personal no autorizado	La jefe de la oficina de control interno, trimestralmente solicita a la dependencia encargada, un reporte de permisos de acceso las carpetas compartidas que contienen información clasificada y reservada, verificando que solamente el personal autorizado tenga acceso a dicha información, con el fin de garantizar los lineamientos de seguridad de la información, en caso de no realizar la verificación, el profesional responsable le generará la alerta a la jefe de control interno a través de correo electrónico	Moderado	La jefe de la oficina de control interno, solicitará al encargado de seguridad de la información una capacitación en materia de información clasificada y reservada, con el fin de fortalecer las competencias de los profesionales. Establecer un compromiso de confidencialidad por parte del pesonal adscrito a la oficina de Control Interno de Gestión.	Segunda semana de febrero	Ultima semana de junio

Control Interno de Disciplinario	Seguridad DIgital	Virus informático, obsolecencia o altos voltajes, borrado de informacion en correos o equipos con intención o sin intención	Pérdida de la disponibilidad de Información Almacenada en el equipo. Por daños en el equipo debido a virus informático, obsolecencia o altos voltajes.	No se pueden hacer diligencias virtuales No se puede interactuar eficiente y eficazmente con los procesos y entidades en las comunicaciones Retraso de las actuaciones de la dependencia Perdida de la información digital No se pueden recibir ni enviar correos ,de procesos o quejas	El líder el proceso al detectar las fallas tecnológicas se dirigirá al proceso correspondiente para realizar el respectivo reporte. El líder de la oficina de control disciplinario, y personal adscrito periódicamente solicitan el mantenimiento a los equipos al área encargas El líder de la oficina de control disciplinario, personal adscrito realizara copias de seguridad semanalmente de la información que considere necesaria para realizar su trabajo que reposa en el equipo a su cargo	Moderado	El líder del proceso realiza mesa de trabajo, con el propósito de analizar, identificar y comunicar las fallas repetitivas con el fin de minimizar los riesgos de pérdida de información o retrasos en las comunicaciones. Así como establecer fechas para ejecutar mantenimiento a los esquipo de computo, este análisis quedará registrado mediante FAC-08 Acta de Reunión semestral	La Cuarta semana de julio - segunda semana de diciembre	La Cuarta semana de julio - segunda semana de diciembre
División Administrativa de Posgrados	Seguridad DIgital	Pérdida de archivos y registros históricos y demás información trascendental para los procesos académicos.	Pérdida de información académica y administrativa almacenada digitalmente	Demandas, tutelas, derechos de petición y perdida del tiempo para dar respuesta a los usuarios.	Archivo físico y digital de los documentos.	bajo	Recomendar realizar una copia de seguridad de toda la información de cada programa para evitar la pérdida de información.	Inicio del semestre	Al finalizar el semestre
Eduación Continua	Seguridad DIgital	1. No actualización de las contraseñas del correo electronico y bases de datos. 2. Rotación del personal	Perdida y/o filtración de información del proceso atraves de medios digitales por falta de cambios en las contraseñas de los correos electronicos y bases de datos	1. Perdida de información confidencial del proceso de Educación Continua y la universidad. 2. Filtración de información confidencial a terceros	El proceso de Educación continua, informa a los ingenieros del CIADTI quitar los roles al personal que va salir, al igualmente el lider del proceso cambiara las claves del correo.	Moderado	Cuando un administrativo/personal termina contrato con la universidad, se solicita al CIADTI quitar los permisos ADMINISTRADOR FORMACION UP Y FORMACION UP al personal que sale de la oficina , y se realiza el cambio de contraseñas/acceso a los correos y bases de datos.	Cada que hay cambio de personal	Cada que hay cambio de personal
Gestión Academica	Seguridad DIgital	Pérdida de archivos y registros históricos y demás información trascendental para los procesos académicos. Correo electrónico, SharePoint, driver	Pérdida de información almacenada digitalmente	Demandas, tutelas, derechos de petición.	Archivo físico y digital de los documentos.	Moderado	Desde el grupo de mejoramiento de la facultad de artes y humanidades se crean grupos en la herramienta SharePoint, con el fin de resguardar la información derivada del proceso académicos. Se realizará seguimiento bimensualmente por parte del grupo de mejoramiento de la facultad	16 de Febrero de 2025	6 de diciembre de 2025
Gestión Administrativa y Financiera	Seguridad DIgital	1. La falta de politicas de seguridad 2. Mal uso que se da al contenido que se consulta o se comparte en el entorno digital.	Pérdida de datos por falta de mantenimiento en equipos y software, contraseñas débiles y acceso a sitios no autorizados	1. Pérdida de información 2. Amenaza informática 3.Suplantación de identidad 4.Demora en la realización de los procesos	Los funcionarios de la Vicerectoria Administrativa y financiera y lider del proceso mantiene contraseñas en los equipos asignados y cambian contraseñas constantemente suben sus documentos de trabajo e impotantes a la Nube , no ingresan a paginas no autorizadas y tiene constantemente el antivirus actualizados de los equipos que manejan.	Moderado	*El funcionario a cargo y el lider del proceso remitiran la solicitud por correo electronico al proceso de la oficina del CIADTI para la revision , actualización y conceptos técnicos de los equipos de computo, contraseñas en los equipod de contuto de la Vicerectoria Administrativa y Financiera	una vez al año	una vez al año
Gestión de Bienestar Universitario	Seguridad DIgital	Violación de la información personal	Manipulación y adulteración de información sensible (historias clínicas) o de roles en el aplicativo.	. Acceso a información privada de la comunidad universitario. 2. Adulteración de rol en el aplicativo desencadenando errores en la información generada.	El líder del proceso solicita al CIADTI la realización de copias de seguridad del aplicativo de historias clínicas, adicional se solicita por medio de CAT semestralmente asignación de rol, usuario y contraseña para el personal vinculado al proceso.	Bajo	Una vez por vigencia, el líder del proceso solicita mediante correo electrónico al CIADTI, copia de seguridad del aplicativo de historias clínicas.	Semestral	Semestral
							El funcionario encargado solicita semestralmente o de acuerdo a la necesidad del proceso la asignación de roles, usuarios y contraseñas para el personal vinculado al proceso.	Semestral	Semestral

Gestión de Contratación	Seguridad DIgital	Acceso por parte de terceros a los sistemas de información empleados en el proceso, como lo son: correos institucionales, GESTASOFT y plataformas de los entes de control (Usuarios y Claves de acceso)	Acceso por parte de terceros a las plataformas institucionales y de los entes de control con la finalidad de realizar cambios en la información publicada o utilizarlos para beneficio propio (datos sensibles, públicos y privados)	Perdida de la información de los diferentes proceso contractuales. Sanciones disciplinarias, sanciones penales y sanciones fiscales.	El jefe de la oficina de Contratación realiza la solicitud de cambio de acceso a la plataforma del SIA OBSERVA a la oficina de control interno cuando el contratista o funcionario que tenga acceso al usuario se desvincule de la oficina. El jefe de la oficina de Contratación, en el caso de la plataforma del SECOP II autoriza la solicitud para crear, modificar o inactivar usuario. De igual manera, cuando algún contratista o funcionario se desvincula de la oficina se realiza el cambio de las claves de acceso a los correos institucionales que se manejan en la dependencia y mediante CAT se solicita al CIADTI la eliminación de las funcionalidades del sistema GESTASOFT.	Bajo	El jefe de la Oficina de Contratación realiza la solicitud de cambio de acceso a la plataforma del SIA OBSERVA mediante correo electrónico a la Oficina de Control Interno de Gestión cuando el contratista o funcionario que tenga acceso al usuario se desvincule de la oficina. El jefe de la oficina de Contratación, en el caso de la plataforma del SECOP II autoriza la solicitud para crear, modificar o inactivar usuario y se deja en acta de grupo de mejoramiento la evidencia. El jefe de la oficina de Contratación o su personal de apoyo solicita a la oficina del CIADTI mediante CAT la asignación de funcionalidades de GESTASOFT a los contratistas o funcionarios que se vinculen a la oficina. De igual manera, el jefe de la Oficina de contratación autoriza el cambio de las claves de acceso a los correos institucionales que se manejan en la dependencia cuando algún contratista o funcionario se desvincula de la oficina y se deja en acta de grupo de mejoramiento. NOTA: Se aclara que esta acción esta sujeta a la rotación del talento humano que se presente en la oficina y la misma se ejecutará solo cuando se desvincule o vincule una nueva persona a la oficina.	Primera semana de agosto última semana de diciembre	Primera semana de agosto última semana de diciembre
Gestión de Contratación	Seguridad DIgital	Daños que se presenten en la unidad de almacenamiento, que permitan la perdida de la información de la oficina (archivo) Posibilidad de perdida o manipulación de información por terceros.	Perdida de la información de la oficina (archivo)	Perdida de la información de la oficina en custodia de archivo de gestión.	La profesional responsable del archivo de la Oficina de Contratación solicita al equipo técnico de Recursos Físicos revisión del equipo de computo con la finalidad de verificar que el ordenador se encuentre en optimas condiciones y no presente ningún tipo de malware	Bajo	La profesional responsable del archivo de la Oficina de Contratación realizará copias de seguridad (backup) anualmente, con la finalidad de contar con respaldos de la información, dejando evidencia en acta de grupo de mejoramiento. De igual manera se debe destacar que los documentos soportes de los procesos contractuales se encuentran cargados en los sistemas de los entes de control (SIA OBSERVA y SECOP) brindando un soporte adicional para salvaguardar la información.	última semana de enero última semana de diciembre	última semana de enero última semana de diciembre
Gestión de la Investigación	Seguridad DIgital	1. Ausencia de un repositorio de información digital de la Vicerrectoria de Investigaciónes. 2. Desactualización de los software intitucionales.	Pérdida de documentos del archivo digital	1. Perdida de la información documental digital. 2. Alteración de la información. 3. Dificultad en el desarrollo de las actividades que realiza cada funcionario. 4. Acceso de la información a terceros.	El lider del proceso establece la revision, control y mantenimiento de los equipos de la Vicerrectoria de Investigaciones anualmente, las cuales se revisara de manera semestral reportando el resultado al proceso de planeación y recursos fisicos, se solicitará a través del correo instituional.	Bajo	1. El jefe de la oficina de vicerectoria de investigaciones y el tecnico administrativo de apoyo, solicitaran la revisión de los equipos al personal de la oficina de recursos fisicos especificamente a los ingenieros de sistemas, para que se emita concepto tecnico del estado de los equipos. 2.El jefe de la oficina de vicerectoria de investigaciones y el tecnico administrativo de apoyo, en reunion de grupo de mejoramiento se determina que se continua el control para la vigencia 2025, para crear el repositorio del archivo digital, con el apoyo de estudiantes que realicen trabajo social en la dependencia.	Primera semana de abril	Segunda semana de diciembre
Gestión de Laboratorios	Seguridad DIgital	1. Inestabilidad del fluido eléctrico y de la red de internet.	Perdida de la información digital por daños en el fluido electrico o de los equipos de cómputo.	1. Perdida de la información 2. Detrimento del patrimonio institucional	El líder del proceso y la secretaria gestionará ante la oficinas de Planeación y CIADTI el mantenimiento de los estabilizadores y equipos de cómputo, asignados a las diferentes unidades de laboratorio, al inicio de cada periodo académico.	Bajo	El líder del proceso y las unidades de laboratorios gestionarán ante la oficina del CIADTI el mantenimiento equipos de cómputo, asignados a las diferentes unidades de laboratorio, al inicio de cada periodo académico, dejando como evidencia el memorando (digital) y el correo electrónico.	Segunda semana de febrero y de agosto	Segunda semana de marzo y de octubre
Gestión de Pagaduría y Tesorería	Seguridad DIgital	Manipulación indebida de los aplicativos	Posibilidad de pérdida o uso indebido de Información de Usuario, por manejo indebido de claves y otros componentes	perdida de la información	El funcionario del área de portales bancarios no debe abrir ni descargar páginas o softwares no autorizados y los funcionarios deben respetando las estrategias de aseguramiento control y tratamiento de la información.	Moderado	Formalización anual de responsabilidad de asignación de la clave de aplicativos y claves del computador entre el jefe de la dependencia y el funcionario encargado del manejo de aplicativo a través de acta de reunion. Nota: Durante el seguimiento a reportar el jefe de la oficina de pagaduría adjuntará carta donde se garantice la elaboración y legalización del año ya que debido a su contenido no es posible compartirla		

Gestión, Servicios y Practica jurida académica	Seguridad DIgital	El constante cambio de asesores, personal administrativo, personal de apoyo, estudiantes y el alto volumen de información que estos manejan, dificultando su conservación, continuidad y seguridad digital y física.	Perdida de información de gestión y mal uso de datos sensibles consolidados en la atención al público y en la representación de terceros	1. Perdida de información por indebido almacenamiento y gestión interna. 2. Mal uso de datos sensibles e información confidencial recopilada en los procesos de atención a los usuarios y representación de terceros.	1. Apoyar a la gestión del proyecto que busca brindar soluciones tecnológicas para el Consultorio Jurídico y Centro de Conciliación "Re-conciliémonos". 2. Bloquear los acceso de los estudiantes que entregan los procesos por sustitución, son suspendidos o cancelan su práctica, con el fin de que no accedan a las carpetas digitales que contienen toda la documentación relativa a los procesos en etapa judicial o administrativa.	Bajo	1. Se crearán almacenamientos en Sharepoint y/o drive para la conservación de la información en los correos institucionales de uso de la dependecia, evitando que se pierda esta información en caso de que cambie el personal. 2. Continuar conel apoyo a la gestión y desarrollo del proyecto que busca brindar soluciones tecnológicas para el Consultorio Jurídico y Centro de Conciliación "Re-conciliémonos"	Siempre que sea requerido por las docentes investigadoras y encargadas del proyecto	Siempre que sea requerido por las docentes investigadoras y encargadas del proyecto
Planeación Institucional	Seguridad DIgital	Apropiación de la información por parte de los funcionarios y contratistas del proceso	Fuga de información	1.Fuga de información a terceros 2.Perdida de la trazabilidad y/o historia del proceso	Actualización en el DRIVE de la dependencia de una carpeta para la vigencia por cada uno de los procesos	Moderado	Revisión y actualización del DRIVE trimestralmente	Marzo	Diciembre
Secretaria General	Seguridad DIgital	Falla del sistemade información en el momento de cierre del acta para el proceso de impresión de diplomas	Error en el sistema de información para la expedición de actas e impresión de diplomas	Perdida de material (Plantillas de diplomas y actas)	Revisión y buen manejo del sistema y reporte de errores a plataforma por medio del CAT, y envío de reporte de errores por medio de correo electrónico a la oficina de admisiones, registro y control academico.	Alto	Revisión, buen manejo del sistema y reporte de errores a plataforma, e imprimir una vez corregidos los errores de datos del acta.	Segunda semana de enero	Tercera semana de diciembre
Sistema Integrado de Gestión	Seguridad DIgital	Daños que se presenten en la unidad de almacenamiento, que permitan la perdida de la información de la oficina (archivo) Falta de protección de las copias de seguridad	Pérdida de información digital(usuarios, contraseñas y documentos)	Perdida de la información de la oficina en custodia de archivo de gestión.	El profesional responsable del archivo de la Oficina de del Sistema Integrado de Gestión, solicita al equipo técnico del CIADTI la revisión del equipo de cómputo con la finalidad de verificar que el ordenador se encuentre en óptimas condiciones y no presente ningún tipo de malware	Moderado	La profesional responsable del archivo del Sistema Integrado de Gestión realizará copias de seguridad de la información digital por lo menos una vez al semestre, con el fin de contar con respaldos de la información, dejando evidencia de su cumplimiento en acta de grupo de mejoramiento.	Cuarta semana de Junio, tercera semana de diciembre	Cuarta semana de Junio, tercera semana de diciembre
		Manipulación de información por terceros, por desconocimiento sobre el manejo de las herramientas tecnológicas Desconocimiento del uso de plataforma digitales (repositorios de información) de cuidado de información sensible por terceros.					El coordinador de la Oficina del Sistema Integrado de Gestión solicitará a la oficina del CIADTI por medio de correo electrónico la Solicitud de Servicio de Mantenimiento y/o concepto técnico de los equipos de cómputo asignados al SIG, con la finalidad de verificar que el ordenador se encuentre en óptimas condiciones y no presente ningún tipo de malware.	mes de febrero	mes de febrero