PROCEDIMIENTO

1. **NOMBRE DEL PROCEDIMIENTO:** PROCEDIMIENTO GESTIÓN DE INCIDENTES.

2. **PROCESO AL QUE PERTENECE:** GESTIÓN TECNOLÓGICA

3. **UBICACIÓN Y COBERTURA DEL PROCEDIMIENTO**

Nivel	
Estratégico	
Misional	
Apoyo	X
Evaluación	

Cobertura	
Central	
Nacional	X
Seccional	
Evaluación	

4. **OBJETIVO DEL PROCEDIMIENTO**:

Establecer un marco transversal para la identificación, reporte, análisis, gestión, resolución, escalamiento y documentación de incidentes tecnológicos dentro de la entidad. Esto incluye incidentes relacionados con la seguridad de la información, fallos de sistemas, errores de software, y cualquier otro evento que pueda afectar la disponibilidad, integridad, confidencialidad y funcionalidad de los recursos tecnológicos, a fin de mantener la continuidad de los servicios tecnológicos de la Rama Judicial.

5. **MARCO NORMATIVO:**

• Ley 270 de 1996	Ley Estatutaria de la Administración de Justicia
• Ley 872 de 2003	Creación del Sistema de Gestión de la Calidad en la Rama Ejecutiva y en otras Entidades prestadoras de servicios.
• NTC ISO 9001:2015	Norma Técnica de Calidad
• NTC ISO 14001:2015	Norma Técnica de Sistema de Gestión Ambiental
• NTC ISO 45001:2018	Norma Técnica de Seguridad y Salud en el Trabajo
• PSAA14-10161 (junio 12 de 2014)	Acuerdo de actualización del Sistema Integrado de Gestión y Control de la Calidad creado mediante Acuerdo PSAA07-3926 de 2007 y se establece el Sistema Integrado de Gestión y Control de la Calidad y el Medio Ambiente – SIGCMA”
• NTC ISO 6256:2021	Esta norma específica los requisitos para el Sistema Integrado de Gestión cuando una entidad del Poder Judicial
• GTC 286:2021	Directrices para dar cumplimiento al Sistema de Gestión de La Calidad y Ambiental para las Corporaciones y/o Dependencias de la Rama Judicial. Requisitos
• NTC ISO 37001:201	Norma Técnica del Sistema de Gestión Antisoborno
• PSAA14-10279 (diciembre 22 de 2014)	Acuerdo mediante el cual se aprueban las políticas y procedimientos de Seguridad de la Información para la Rama Judicial”
• ACUERDO No. PCSJA20-11631	"Por el que se adopta el Plan Estratégico de Transformación Digital de la Rama Judicial -PETD 2021-2025"
• PCSJA23-12130 DE 2023	Acuerdo, por medio del cual se crean unos cargos con carácter permanente en la planta de la Dirección Ejecutiva de Administración Judicial, …” entre ellas la Unidad de Transformación Digital e Informática”

6. TÉRMINOS Y DEFINICIONES:

- **ANS:** Sigla para Acuerdo de Nivel de Servicio. También corresponde con la sigla SLA en inglés: (Service Level Agreement) es un acuerdo escrito entre un proveedor de servicio de TI y su cliente con objeto de fijar el nivel acordado para la calidad y oportunidad en la atención de dicho servicio.
- **CAMBIO:** Consiste en añadir, modificar o eliminar cualquier cosa que pudiera tener un efecto en los servicios de TI. El alcance debe incluir cambios en todas las arquitecturas, procesos, herramientas, métricas y documentación, así como cambios en los servicios de TI y otros elementos de configuración.
- **CONFIGURACIÓN:** Se refiere al proceso de ajustar, personalizar y organizar elementos, componentes o parámetros de dispositivos, programas o sistemas informáticos de manera específica para lograr un objetivo a una situación particular.
- **ESCALAMIENTO:** Mecanismo que asiste a la resolución de una solicitud de servicio reasignándolo a un especialista o proveedor dependiendo el caso.
- **INCIDENTE:** Cualquier evento que no es parte de la operación normal del servicio y el cual causa o puede causar la interrupción o la reducción de la calidad del servicio.
- **INCIDENTE MAYOR:** Falla en el servicio que causa alto impacto en la operación y que debe ser atendido con mayor grado de urgencia que un incidente normal. Comúnmente estos incidentes afectan directamente la toda la Infraestructura de TI en lo que tiene que ver con redes, aplicaciones, servidores, telecomunicaciones, etc. Se homologa al término de mayor que se referencia en la metodología ITIL.
- **IMPACTO:** Es una medida del efecto de un incidente, problema o cambio en los procesos de la Entidad. A menudo, el impacto se establece en función de cómo los niveles de servicio se verán afectados.
- **PRIORIDAD:** Es una categoría utilizada para identificar la importancia relativa de un incidente, problema o cambio. La prioridad está basada en el impacto y la urgencia, y se utiliza para identificar los tiempos requeridos para tomar acciones.
- **RIESGO:** Es una potencial amenaza de un activo o de un grupo de activos y esta cause daño en la organización.
- **SERVICIO:** actividades que buscan responder a las necesidades de un cliente mediante un cambio de condición en los bienes informáticos (llámese activos), potenciando su valor y reduciendo el riesgo del sistema.
- **TECNOLOGÍAS DE LA INFORMACIÓN (TI):** Las tecnologías de la información y las Comunicaciones (TIC o TIC's), agrupan los elementos y las técnicas utilizadas en el tratamiento y la transmisión de las informaciones, principalmente de informática, internet y telecomunicaciones.
- **USUARIO:** Persona que utiliza un componente o un servicio tecnológico.

7. ALCANCE DEL PROCEDIMIENTO:

La gestión de Incidentes inicia desde la actividad de análisis y direccionamiento de la petición realizada por el usuario donde se identifica una afectación de disponibilidad y se tipifica el incidente y termina con la resolución y documentación de este.

ACTIVIDAD CON LA QUE SE DA INICIO AL PROCESO	Recepción de los incidentes registrados por los usuarios mediante los canales de atención designados
DEPENDENCIA QUE DA INICIO AL PROCESO	División de Servicios Tecnológicos División de Infraestructura de Software División de Seguridad y Protección de Datos División de Infraestructura de Hardware, Comunicaciones y Centros de Datos División de Desarrollo de Productos Digitales
ACTIVIDAD CON LA QUE FINALIZA EL PROCESO	Documentación de la respuesta y comunicación al solicitante en caso de ser necesario.

DEPENDENCIA QUE FINALIZA EL PROCESO	División de Servicios Tecnológicos División de Infraestructura de Software División de Seguridad y Protección de Datos División de Infraestructura de Hardware, Comunicaciones y Centros de Datos
DEPENDENCIAS EN LAS QUE TIENE ALCANCE EL PROCESO	Altas Cortes Despachos Judiciales a nivel nacional Consejo Superior de la Judicatura DEAJ Direcciones Seccionales de administración Judicial Rama Judicial

8. POLÍTICAS DE OPERACIÓN:

Reporte de incidentes:

- Todo el personal involucrado en la Gestión de Incidentes de Tecnología debe referirse al presente documento, conocer las actividades asociadas a la solución de las fallas reportadas, registrar toda la información, todos los datos del incidente incluyendo la respectiva documentación y evidencia de la solución en los medios establecidos.
- Los medios de contacto para comunicar un incidente son los establecidos por la Rama Judicial, entre los que se encuentran herramienta de gestión de mesa de servicios, líneas telefónicas, y correo electrónico. El uso adecuado de estos medios garantiza una respuesta eficiente y oportuna a los incidentes reportados.
- Todo incidente de servicio recibido debe ser gestionado, hasta conseguir la adecuada solución y cierre. Si no se encuentra una solución, debe escalarse a un nivel superior (tanto funcional como jerárquico) y se debe hacer el respectivo seguimiento.
- Todo incidente escalado a un nivel superior (tanto funcional como jerárquico), debe tener un responsable asignado quién realizará el debido control y seguimiento, para la correcta documentación de la gestión y solución.
- Todo incidente debe catalogarse bajo una prioridad asociada a su nivel de servicio.

Atención de incidentes

Para la atención de los incidentes es importante tener en cuenta lo siguiente:

1) Impacto

a) **Incidentes de Alto Impacto: Incidentes que afectan a un gran número de usuarios o que comprometen datos y servicios críticos. Ejemplos: Violaciones de seguridad con exposición de información confidencial, o interrupciones que afectan a múltiples sedes judiciales.**
Respuesta: Intervención inmediata con la participación de equipos de alto nivel.

b) **Incidentes de Impacto Medio: Incidentes que afectan a un grupo de usuarios o a una parte importante de los sistemas, pero que no son críticos para la operatividad general.**
Ejemplos: Problemas en sistemas de soporte que impactan áreas específicas.
Respuesta: Resolución con alta prioridad, asegurando que no escalen a incidentes de alto impacto.

c) **Incidentes de Bajo Impacto: Incidentes que tienen un alcance limitado y afectan solo a un pequeño número de usuarios o funciones no esenciales.**
Ejemplos: Fallos en impresoras, problemas con software de ofimática, o interrupciones en herramientas de apoyo no críticas.
Respuesta: Gestión según disponibilidad de recursos.

2) Urgencia

a) **Incidentes Urgentes: Incidentes que requieren una respuesta inmediata debido al riesgo de escalación o al impacto significativo en los servicios.**
Ejemplos: Ataques cibernéticos en curso, fallos de servidores principales, o caídas de
sistemas esenciales.

Respuesta: Activación inmediata de equipos de respuesta y notificación a las autoridades competentes si es necesario.

b) **Incidentes Importantes: Incidentes que, aunque no sean críticos, necesitan una pronta atención para evitar mayores problemas.**
Ejemplos: Problemas recurrentes en aplicaciones clave, o reportes de fallos en equipos de uso intensivo.
Respuesta: Resolución rápida, pero sin la necesidad de activar protocolos de emergencia.

c) **Incidentes No Urgentes: Incidentes que no requieren intervención inmediata y pueden ser programados para resolución en un período estándar.**
Ejemplos: Solicitudes de mejoras en software, reportes de problemas menores de rendimiento.
Respuesta: Resolución en el tiempo regular, con enfoque en la eficiencia y satisfacción del usuario.

Tipos de incidentes

Para identificar quien puede atender un incidente, se deben tener en cuenta los siguientes conceptos:

a. Falla de hardware: Problemas físicos con dispositivos como computadoras, impresoras, servidores, etc. Ejemplos incluyen discos duros dañados, fallos en la memoria RAM, o problemas con la fuente de alimentación.
b. Falla de software: Problemas relacionados con el funcionamiento de programas o aplicaciones. Esto puede incluir errores de software, fallos en la instalación, o incompatibilidades entre programas.
c. Problemas de red: Incidentes que afectan la conectividad de la red, como caídas de la red, problemas con el Wi-Fi, o interrupciones en la conexión a internet.
d. Errores de usuario: Problemas causados por el uso incorrecto de la tecnología por parte de los usuarios, como la eliminación accidental de archivos importantes, configuración incorrecta de software, o uso inapropiado de dispositivos.
e. Problemas de rendimiento: Incidentes donde los sistemas o aplicaciones funcionan más lentamente de lo esperado, lo que puede ser causado por sobrecarga de recursos, software desactualizado, o problemas de configuración.
f. Interrupciones del servicio: Incidentes donde un servicio o aplicación deja de estar disponible, como caídas de servidores, interrupciones en servicios en la nube, o fallos en sistemas críticos.
g. Problemas de compatibilidad: Incidentes donde ciertos dispositivos o software no funcionan correctamente juntos, como incompatibilidades entre sistemas operativos y aplicaciones, o problemas con controladores de hardware.
h. Problemas de seguridad de la información: Incidentes relacionados con la seguridad informática, como virus, malware, intentos de phishing, o accesos no autorizados a sistemas. Estos incidentes son gestionados a través del procedimiento de incidentes de seguridad.

Niveles de atención

Para el caso de los incidentes atendidos por mesa de ayuda, se cuenta con los siguientes niveles de atención:

Nivel 1: Soporte Básico (Primer Nivel): Este es el nivel inicial de soporte, son el primer punto de contacto con los usuarios que reportan incidentes o solicitudes cuando ocurre un problema técnico y es responsable de resolver incidentes básicos. Este nivel se encarga de atender llamadas y correos electrónicos, así como el escalamiento del incidente a un segundo nivel si lo requiere.

Nivel 2: Soporte Intermedio (Segundo Nivel): Este nivel deben contar con ingenieros y/o técnicos con mayor experiencia y conocimientos especializados (software, redes de comunicación, bases de datos, entre otros) para la atención y soporte en sitio a nivel nacional de los incidentes o solicitudes escalados desde soporte nivel 1. **Este nivel se encarga de:**

- Diagnosticar y solucionar problemas que involucran configuraciones avanzadas, análisis de fallas y soporte de aplicaciones específicas.
- Colaborar con otros equipos.
- Escalar incidentes o solicitudes que requieran un tratamiento mayor.

Nivel 3: Soporte Avanzado (Tercer Nivel): Es el nivel más alto de soporte y se encarga de resolver problemas críticos o altamente complejos que no pudieron ser manejados por los niveles anteriores. El personal de Nivel 3 está compuesto por expertos especializados en tecnología, desarrolladores, ingenieros de sistemas o incluso proveedores externos. Este nivel se encarga de:

- Investigar y resolver incidentes que requieran conocimientos profundos y especializados.
- Desarrollar parches o soluciones temporales para problemas críticos.
- Realizar modificaciones en el software, hardware o la infraestructura.
- Desarrollo y actualización de bases de datos

Para el caso de los incidentes atendidos por otros canales, cada director definirá la forma de atención y los profesionales que requiera.

De acuerdo con sus funciones las divisiones de la UTDI atienden los incidentes de la siguiente manera:

- División de Seguridad y protección de datos: Los incidentes relacionados con la información y protección de datos se atienden a través del procedimiento de incidentes de seguridad
- División de Infraestructura Hardware: Incidentes relacionados con equipos de cómputo, redes WAN, Centros de datos a cargo de la división y software de seguridad.
- División de Infraestructura Software: Incidentes de software y sistemas de información
- División de Servicios tecnológicos: incidentes relacionados con redes LAN, servicios nube pública o privada.

9. LIDER DEL PROCEDIMIENTO:

CARGO	DEPENDENCIA
Director Unidad	Unidad de Transformación Digital e Informática

10. RESPONSABLES DEL PROCEDIMIENTO:

CARGO	DEPENDENCIA
Director Administrativo	División de Servicios Tecnológicos División de Infraestructura de Software División de Seguridad y Protección de Datos División de Infraestructura de Hardware, Comunicaciones y Centros de Datos

11. PROVEEDORES E INSUMOS:

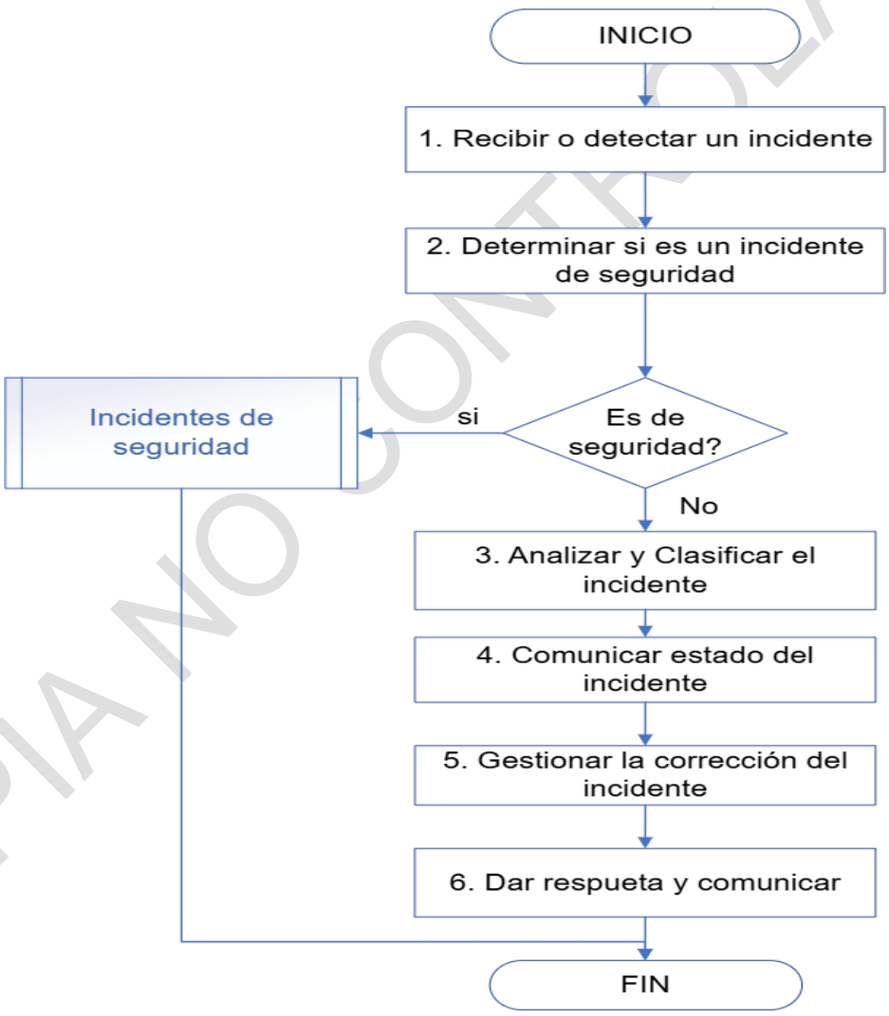
PROVEEDORES	ENTRADA / INSUMOS
Dependencias Consejo Superior / Direcciones Seccionales de Administración Judicial / funcionarios y Servidores Judiciales de los Despachos Judiciales del país.	Planeación estratégica / Plan Sectorial de Desarrollo / PET / Planes de Inversión / Plan Operativo. Direccionamiento Estratégico, Sistema de Gestión de Calidad y del Medio Ambiente, Manual de Contratación y de Supervisión de la Entidad. Reportes de incidentes
Divisiones / Áreas de la Unidad de Transformación Digital e informática	Información para atención de incidentes Actualizaciones a los sistemas de información
División de Seguridad y Protección de Datos	Reportes internos de incidentes y análisis de amenazas
Contratista Servicio Mesa de Ayuda	Informes de soporte técnico y servicios asociados.

12. CONTROLES DEL PROCEDIMIENTO:

TIPO DE CONTROL	DESCRIPCIÓN
Herramientas oficiales de comunicación	Canales de comunicación oficial efectivos tanto internos como externos. Seguimiento a los casos generados en la herramienta. Reporte general de los estados de los incidentes.
Indicadores	Definición y seguimiento de indicadores relacionados con la gestión de incidentes a través de la herramienta de gestión de mesa de ayuda, que permitan medir la eficacia y eficiencia del proceso.
Acuerdos de Niveles de Servicio	Un Acuerdo de Nivel de Servicio o ANS (Service Level Agreement o SLA), definidos en la herramienta de gestión de la mesa de ayuda.
Seguimiento de actividades de Ejecución de la gestión de incidentes.	Informes de seguimiento de gestión de incidentes que se atiendes a través de la herramienta de gestión de la mesa de ayuda

13. DESCRIPCIÓN DEL PROCEDIMIENTO (Ciclo PHVA)

FLUJOGRAMA



DESCRIPCIÓN

Etapa	Actividad	Descripción	Producto	Responsable
P (1)	Recibir o detectar incidentes	Se recibe del usuario la solicitud del incidente mediante los canales establecidos por la entidad (correo electrónico institucional, herramienta de gestión) o se detecta algún incidente mediante • Caídas de servidores • Informes de monitoreo • Otros funcionamientos fuera de lo normal de los servicios	• Registro de los incidentes presentados • Informes de servicios	Profesional Universitario Designado
H (2)	Analizar y Clasificar el incidente	El incidente se clasifica teniendo en cuenta lo definido en las políticas de operación. El profesional designado realiza un análisis preliminar para entender la naturaleza del incidente y su alcance. Se identifican las posibles causas del incidente, si existen otros reportes similares y se evalúan los sistemas afectados. Esto puede incluir la revisión de registros de auditoría, análisis de tráfico de red, y la verificación de la integridad del sistema. Se asigna el incidente a los técnicos y/o especialistas según se requiera.	Herramienta de gestión o correo electrónico.	Profesional Universitario Designado
H (3)	Determinar si es un incidente de seguridad	Se analiza el tipo de incidente de la siguiente manera: Es un incidente de seguridad?: Si, Escalar el incidente al profesional de seguridad para su gestión e inicia la activación del procedimiento de Incidentes de seguridad. No, continua el procedimiento en la actividad 3.	• Correo electrónico • Herramienta de gestión • Procedimiento incidentes de seguridad	Profesional Universitario Designado
H (4)	Comunicar estado del incidente	Se informa a los afectados sobre la situación y se les proporciona una actualización sobre el estado del incidente. Cuando el incidente lo amerite, se realizará un comité de crisis PMU. De igual forma, dependiendo del tipo de incidente, se declarará la indisponibilidad de los servicios afectados.	Correo comunicando el estado del incidente	Profesional Universitario Designado
H (5)	Gestionar la corrección del incidente	Se implementan acciones para contener el incidente y evitar que se extienda o cause más daño. Esto puede incluir	Acciones para la solución del incidente	Profesional Universitario Designado

Etapa	Actividad	Descripción	Producto	Responsable
		el aislamiento de sistemas comprometidos, la revocación de accesos y el despliegue de parches o actualizaciones. Se verifica que las medidas adoptadas han detenido la progresión del incidente. Se asegura de que todas las funciones del sistema estén operativas y de que no haya persistencia de vulnerabilidades o problemas.		
H (6)	Resolver y comunicar	Se registra el proceso, incluyendo el diagnóstico, la respuesta, las acciones tomadas y las lecciones aprendidas Se genera un informe final que incluye un análisis detallado del incidente, el impacto, las medidas tomadas y recomendaciones para evitar futuros incidentes. El incidente se cierra formalmente una vez que todas las actividades de resolución y recuperación hayan sido completadas y documentadas.	Informe de incidente	Profesional Universitario Designado Directores Administrativos UTDI
V (7)	Verificar	Revisar que el procedimiento de gestión de incidentes se haya realizado conforme a lo está establecido.	Informes y correos	Directores Administrativos UTDI Profesional Universitario designado
A (8)	Acciones de Mejora	Conforme al proceso de autoevaluación realizado se formulan y ejecutan los planes de acción y mejoramiento	Acciones correctivas, preventivas y de mejoramiento	Directores Administrativos UTDI

14. ANEXOS (Formatos, Guías, Instructivos, Planes)

N/A