1. **NOMBRE DEL PROCEDIMIENTO**: Gestión de Incidentes
2. **RESPONSABLE**: Jefe recursos informáticos y educativos (Líder de Gestión de Incidentes)
3. **OBJETIVO**: Establecer los lineamientos para la prevención, detección y corrección de eventos e incidentes que comprometan la seguridad de la información o puedan afectar la continuidad de las operaciones de la Universidad Tecnológica de Pereira.
4. **RESULTADOS ESPERADOS**: Apoyar las diferentes dependencias académicas para el desempeño de sus funciones.
5. **LÍMITES**

Punto inicial: Realizar actividades para la prevención de incidentes.

Punto final: Registrar las lecciones aprendidas

FORMATOS O IMPRESOS

- Formato de Acciones correctivas
- Matriz de Riesgos de los Activos de Información
- Informes mensuales de Gestión de Incidentes

6. **DESCRIPCIÓN ESPECÍFICA**

No	Actividad	Ejecutante
1	**Realizar actividades para la prevención de incidentes.** Para la prevención de incidentes es necesario realizar una serie de actividades por parte de los funcionarios responsables de los activos de información de la entidad: • Análisis Periódico de Riesgos. • Auditorías periódicas. • Administración de Actualizaciones Informáticas. • Fortalecimiento de seguridad de los Equipos de cómputo. • Seguridad en la Red. • Prevención de Código Malicioso. • Concientización y Capacitación a los usuarios de la entidad.	Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI). Jefes unidades organizacionales
2	**Detectar y reportar eventos, incidentes y debilidades de seguridad de la información.** En la medida que un funcionario, contratista, estudiante, proveedor u otra parte interesada note que se está presentando un ataque a los activos de información de	Colaboradores UTP Contratistas

	la entidad, que alguna persona está violando las políticas de seguridad de la información o en general, conoce de riesgos asociados a la información, debe proceder a reportar esta situación como un evento o incidente de seguridad a través de alguno de los siguientes medios: • Correo electrónico o telefónicamente a la mesa de ayuda. • Correo: soporte@utp.edu.co • Teléfono: 3137273 Es responsabilidad del especialista de Service Desk abrir el ticket.	Estudiantes Proveedores Otras Partes Interesadas
3	**Clasificar los eventos, incidentes y debilidades de seguridad de la información reportados.** Consiste en catalogar como evento o incidente el reporte recibido. Si el reporte es categorizado como evento, sólo se mantendrá registro del mismo para posterior análisis e informes. Sin embargo, si el reporte es categorizado como incidente, este debe ser clasificado teniendo en cuenta las categorías y subcategorías, enumeradas a continuación: ***1. Acceso no autorizado (físico y lógico)*** • Robo de información física o digital. • Alteración de la información. • Intentos recurrentes y no recurrentes de acceso no autorizado • Robo de contraseñas. • Robo de información web mediante Cross-Site-Scripting o SQL Injection. • Divulgación no autorizada de información personal. • Intrusión física a las instalaciones • Modificación o eliminación no autorizada de datos. • Modificación, instalación o eliminación no autorizada de software. • Intento fallido de conexión VPN de clientes • Robo o pérdida de un recurso informático • Pérdida o eliminación no autorizada de backups de la información. • Robo de backups de la información • Consultas no autorizadas mediante Telnet • Intento de acceso no autorizado en Base de Datos • Acceso no autorizado a carpetas privadas de servidores	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).

	• Creación de usuarios administrativos sin autorización. • Robo, pérdida o destrucción no autorizada de manuales de funcionamiento de servidores internos. • Robo de cookies. • Otro no contemplado ***2. Código malicioso*** • Virus informáticos • Troyanos • Gusanos informáticos ***3. Denegación de servicios*** • Tiempos de respuesta muy bajos sin razones aparentes. • Servicio(s) interno(s) inaccesibles sin razones aparentes • Servicio(s) externo(s) inaccesibles sin razones aparentes • Interrupción prolongada en un sistema o servicio de red • Caída de Base de Datos • Caída del servicio de internet • Otro no contemplado ***4. Escaneo, pruebas o intentos de obtención de información de la red*** • Sniffers (software utilizado para capturar información que viaja por la red) • Detección de Vulnerabilidades • Ataques Man in the Middle • Cracking de passwords • Email bombing • Intento de conexiones arbitrarias a través del mismo puerto • Intento de escalar privilegios de usuarios • Instalación de Keyloggers (capturadores de caracteres introducidos por teclado) • Intento de seguimiento de conexiones mediante consultas “ping” • Otro no contemplado ***5. Mal uso de los activos de información***	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).

	• Mal uso y/o Abuso de servicios informáticos internos o externos • Violación de las normas de acceso a Internet • Mal uso y/o Abuso del correo electrónico de la Entidad • Violación de las Políticas, Normas y Procedimientos de Seguridad de la información aprobados en la entidad. • Modificación no autorizada de un sitio o página web • Destrucción o alteración física de los componentes de la red ***6. Ingeniería Social*** • Abuso de la ingenuidad o confianza de un usuario. Hubo intento de obtener información o se obtuvo y fue utilizada para tener acceso autorizado a la información de los computadores. Esta actividad puede o ha sido realizada a través de mensajes de correo, llamadas telefónicas personales, entre otros.	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).
4	**Evaluación de Incidentes de seguridad de la información.** El proceso de evaluación de incidentes de seguridad de la información comprende: **1. Establecimiento del nivel de prioridad** Es frecuente que existan múltiples incidentes concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de los mismos. El nivel de prioridad se basa esencialmente en dos parámetros: • Impacto: Determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio, número de usuarios y/o activos de información afectados, y la importancia de los mismos para la entidad. • Urgencia: Depende del tiempo máximo de demora que acepte el cliente para la resolución del incidente y/o el nivel de servicio. En la siguiente tabla (Tabla1) se establece el diagrama de prioridades al diagrama de prioridades en función de la urgencia y el impacto del incidente.	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).

PRIORIDAD		IMPACTO			
Crítica / Media / Alta / Baja		Bajo	Medio	Alto	Crítico
URGENCIA		1	2	3	4
Crítica	4	4	8	12	16
Alta	3	3	6	9	12
Media	2	2	4	6	8
Baja	1	1	2	3	4

Tabla 1. Diagrama de prioridades

Además, se debe asignar el tiempo de respuesta del incidente de acuerdo con el nivel de prioridad, así:

- Crítico: 0 - 3 horas
- Alto: 4 - 8 horas
- Medio: 9 - 16 horas
- Bajo: 17 - 40 Horas

2. Asignación de recursos

Se debe registrar la asignación del ticket al personal del proceso correspondiente que realizó la solicitud, teniendo en cuenta los niveles de escalamiento, los tiempos máximos en cada nivel y el responsable de la Resolución de Incidentes por Categoría (Tabla 2)

Estado	Rol Responsable
Acceso No Autorizado (Físico o Lógico)	
Robo de información física o digital.	Jefes unidades organizacionales
Alteración de la información física.	Jefes unidades organizacionales
Alteración de información digital.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI
Intentos recurrentes y no recurrentes de acceso no autorizado	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI
Robo de contraseñas.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI
Robo de información web mediante Cross-Site-Scripting o SQL Injection	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI

Técnico I (CRIE, GTI-SI),

Profesional I (CRIE, GTI-SI),

Profesional II (CRIE, GTI-SI).

	Divulgación no autorizada de información personal.	Física y digital: jefes de unidades organizacionales	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).
	Intrusión física a las instalaciones	Ejecutivo 26 Gestión de Servicios Institucionales	
	Modificación o eliminación no autorizada de datos.	Jefes de unidades organizacionales	
	Modificación, instalación o eliminación no autorizada de software.	Jefes de unidades organizacionales	
	Intento fallido de conexión VPN de clientes	Ejecutivo 26 CRIE	
	Robo o pérdida de un recurso informático	Jefes de unidades organizacionales	
	Pérdida o eliminación no autorizada de backups de la información de servidores.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Robo de backups de la información	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Consultas no autorizadas mediante Telnet	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Intento de acceso no autorizado en Base de Datos	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Acceso no autorizado a carpetas privadas de servidores	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Creación de usuarios administrativos sin autorización.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Robo, pérdida o destrucción no autorizada de manuales de funcionamiento de servidores internos.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Robo de cookies.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Otro no contemplado	Ejecutivo 26 CRIE	
	Código Malicioso		
	Virus informáticos	Ejecutivo 26 GTI-SI	
	Troyanos	Ejecutivo 26 GTI-SI	
	Gusanos informáticos	Ejecutivo 26 GTI-SI	
	Denegación de Servicios		
	Tiempos de respuesta muy bajos sin razones aparentes.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Servicio(s) interno(s) inaccesibles sin razones aparentes	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Servicio(s) externo(s) inaccesibles sin razones aparentes	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Interrupción prolongada en un sistema o servicio de red	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Caída de Base de Datos	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
	Caída del servicio de internet	Ejecutivo 26 CRIE	
	Otro no contemplado	Ejecutivo 26 CRIE y	

	Ejecutivo 26 GTI-SI	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).
Escaneo, Pruebas o Intentos de Obtención de Información de la Red		
Sniffers (software utilizado para capturar información que viaja por la red)	Ejecutivo 26 CRIE	
Detección de Vulnerabilidades	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Ataques Man in the Middle.	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Cracking de passwords	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Email bombing	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Email Spamming	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Intento de conexiones arbitrarias a través del mismo puerto	Ejecutivo 26 CRIE	
Intento de escalar privilegios de usuarios	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Instalación de Keyloggers (capturadores de caracteres introducidos por teclado)	Ejecutivo 26 GTI-SI	
Intento de seguimiento de conexiones mediante consultas “ping”	Ejecutivo 26 CRIE	
Otro no contemplado	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Mal Uso de los Activos de Información		
Mal uso y/o Abuso de servicios informáticos internos o externos	Ejecutivo 26 CRIE y Ejecutivo 26 GTI-SI	
Violación de las normas de acceso a Internet	Ejecutivo 26 CRIE	
Mal uso y/o Abuso del correo electrónico de la Organización	Jefes de unidades organizacionales	
Violación de las Políticas, Normas y Procedimientos de Seguridad de la información aprobados en UTP	Ejecutivo 26 CRIE	
Modificación no autorizada de un sitio o página web	Ejecutivo 26 CRIE	
Destrucción o alteración física de los componentes de la red	Ejecutivo 26 CRIE	
Ingeniería Social		
Abuso de la ingenuidad o confianza de un usuario. Hubo intento de obtener información o se obtuvo y fue utilizada para tener acceso autorizado a la información de los computadores. Esta actividad puede o ha sido realizada a través de mensajes de correo, llamadas telefónicas personales, entre otros.	Ejecutivo 26 CRIE	

Tabla 2. Responsables de la Resolución de Incidentes por Categoría

Inicialmente, el ticket será asignado al Especialista de Service Desk (Nivel 1). En caso de que el Especialista de Service Desk no pueda solucionar el incidente

mediante asesoría remota o exceda el tiempo máximo asignado al nivel 1, este debe asignar el ticket a un especialista de siguiente nivel (Nivel 2). En caso tal de que el especialista considere que no está en capacidad de dar solución al incidente o se exceda el tiempo máximo asignado al nivel 2, el ticket debe ser escalado a un tercero (Nivel 3).

Niveles de Escalamiento

Es frecuente que los especialistas consideren que no están en capacidad de resolver en primera instancia un incidente y para ello deberán recurrir a un tercero. A este proceso se le denomina escalado o escalamiento. El proceso de escalamiento se describe en la Figura 1.

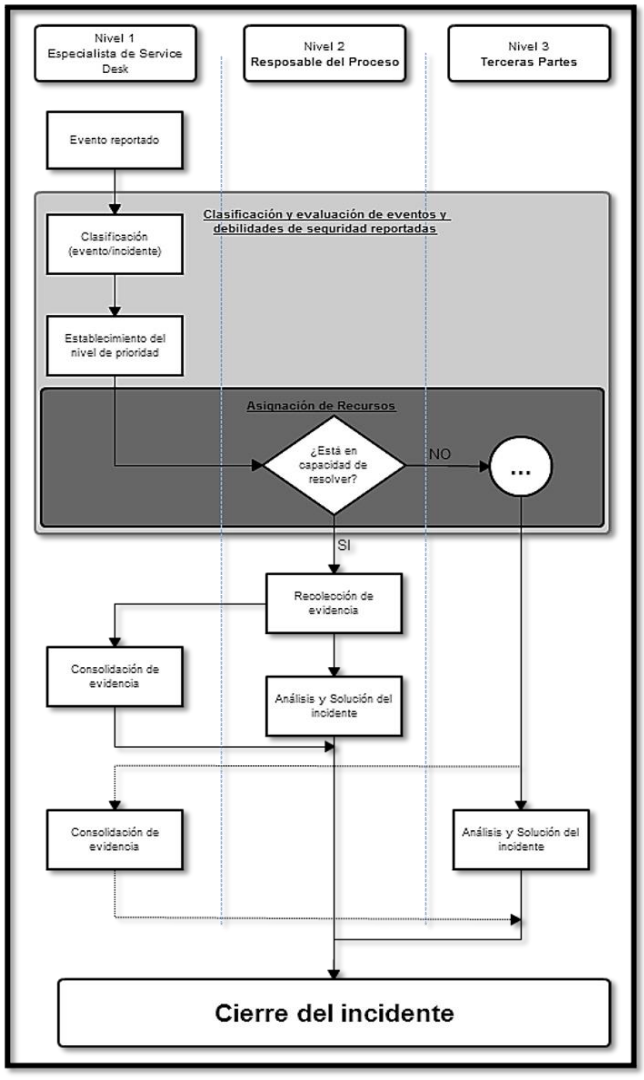

Figura 1. Niveles de Escalamiento

Técnico I (CRIE, GTI-SI),

Profesional I (CRIE, GTI-SI),

Profesional II (CRIE, GTI-SI).

	<u>Tiempos Máximos en Cada Nivel de Escalamiento</u> **Nivel 1** 10% del tiempo establecido para la resolución del incidente de acuerdo con su prioridad. **Nivel 2** 40% del tiempo establecido para la resolución del incidente de acuerdo con su prioridad. **Nivel 3** 50% del tiempo establecido para la resolución del incidente de acuerdo con su prioridad.	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).
5	**Recolectar la evidencia.** Para la recolección de evidencia es necesario tener en cuenta lo siguientes criterios, según aplique: • **Información basada en la red:** Logs de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación. • **Live data collection:** Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. • **Forensic duplication:** Backups, archivos copiados recientemente, etc. • **Otra información:** Testimonio de la persona que reporta el evento o incidente. Para el manejo de la evidencia se contactarán a las autoridades correspondientes en caso de ser necesario.	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).
6	**Consolidar la evidencia.** La evidencia debe ser registrada y consolidada a través del software de la mesa de ayuda.	Técnico I (CRIE, GTI-SI), Profesional I (RIE, GTI-SI), Profesional II (RIE, GTI-SI).
7	**Analizar y solucionar el incidente.** En primera instancia se examina el incidente con ayuda de la base de datos de conocimiento para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado. En caso contrario, se define e implementa una solución encaminada a resolver el incidente y a garantizar la	Técnico I (CRIE, GTI-SI),

	Seguridad de la Información. En segundo lugar, se debe decidir si se va a plantear o no una acción correctiva para dar respuesta al incidente siguiendo el procedimiento de Acciones Correctivas de la universidad, iniciar la ejecución de la misma y notificar por correo electrónico al Ejecutivo 26 CRIE, así como alimentar la base de datos de conocimiento. En caso de incidentes críticos se reportará dentro de las 24 horas siguientes a su detección al CSIRT-Gobierno. Por último, si el incidente involucra pérdida o fuga de datos personales, se debe informar a la superintendencia de industria y comercio.	Profesional I (RIE, GTI-SI), Profesional II (RIE, GTI-SI).
8	**Verificar el cumplimiento de la acción correctiva.** Se debe verificar y hacer seguimiento a la implementación de la solución y cierre del ticket en el tiempo acordado.	Ejecutivo 26 CRIE
9	**Dar cierre al ticket.** El Especialista de Service Desk tiene la responsabilidad de cerrar el ticket. Lo anterior con el fin de evitar que los tickets sean cerrados sin el cumplimiento del requerimiento.	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (CRIE, GTI-SI).
10	**Presentar informe a la Dirección.** Semestralmente, el Líder de Gestión de Incidentes de la Información debe presentar un informe consolidado de la Gestión de Incidentes de Seguridad de la Información ante el Grupo de Seguridad de la Información.	Ejecutivo 26 CRIE
11	**Registrar las lecciones aprendidas.** Se buscará definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la universidad. Entre las actividades que se realizan para este efecto están: • Mantener la documentación de los eventos e incidentes de Seguridad de la Información. • Alimentar la Base de Conocimiento. • Integrar los eventos e incidentes a la Matriz de Riesgos de los Activos. • Realizar planes de capacitación a los funcionarios y colaboradores de la entidad en temas concernientes a eventos e incidentes de Seguridad de la Información. • Analizar los hechos y tomar decisiones. Implementar controles preventivos.	Técnico I (CRIE, GTI-SI), Profesional I (CRIE, GTI-SI), Profesional II (RIE, GTI-SI).

Elaborado Por:	Revisado Por:	Aprobado Por:
Personal UTP	Profesional IV Gestión del Sistema Integral de Calidad	Ejecutivo 26 Jefe Recursos Informáticos y Educativos

**********Fin del documento**********