Escuela Tecnológica Instituto Técnico Central Establecimiento Público de Educación Superior	PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: GSI-PC-05
		VERSIÓN: 3
		VIGENCIA: SEPTIEMBRE 2023
	PROCESO: GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	DOCUMENTO CONTROLADO

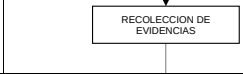
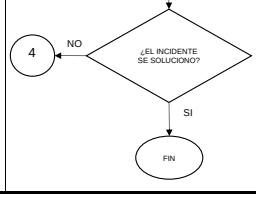
1. OBJETIVO	Definir acciones para identificar, analizar, clasificar, valorar y dar respuestas pertinentes en busca de la solución de los incidentes de Seguridad de la Información que se presenten.
2. ALCANCE	Inicia desde la detección de un incidente de Seguridad de la Información hasta que se da cierre en la herramienta de gestión de servicios de TI (Aplicativo Mesa de Ayuda).
3. RESPONSABLE	**Servidores Públicos, Proveedores y demás partes interesadas:** Administrativos, Contratistas, Docentes y Estudiantes del Instituto de Bachillerato Técnico Industrial (IBTI) y de Programas de Educación Superior (PES). **Profesional de Gestión Informática y Comunicaciones:** encargado de gestionar los servicios de TI. **Gestor de Mesa de Servicios:** responsable de administrar la aplicación de la mesa de ayuda (GLPI). **Equipo Técnico de Soporte:** responsable de dar el soporte a los incidentes reportados en el primer nivel según lo escale la mesa de servicios. **Profesional de Seguridad de la Información:** responsable de dar respuesta a los incidentes de Seguridad de la Información según lo escale la mesa de servicios.

4. DEFINICIÓN DE TÉRMINOS

TÉRMINO	DEFINICIÓN
ACTIVO DE INFORMACIÓN	Son todos los datos, sistemas o servicios que generan valor a la ETITC.
ATAQUE INFORMÁTICO	Es un procedimiento técnico que tiene como objetivo tener acceso a un sistema de información de forma no autorizada o ejecutar malware en el mismo.
AMENAZA CIBERNÉTICA	Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854, pág. 87).
ATAQUE CIBERNÉTICO	Acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (CONPES 3854, pág. 87).
BASE DE DATOS	Es un conjunto de datos almacenados sistemáticamente y que son consultados mediante un sistema de información
CERT (COMPUTER EMERGENCY RESPONSE TEAM)	Equipo de respuesta a emergencias cibernéticas.
CCOC	Comando Conjunto Cibernético se desempeña como unidad élite en aspectos relacionados con la ciberseguridad y ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales, desarrollando operaciones militares en el ciberespacio para defender la soberanía, la independencia, la integridad territorial y el orden constitucional, contribuyendo a generar un ambiente de paz, seguridad y defensa nacional.
CIBERATAQUE	Es cualquier tipo de actividad ofensiva realizada por personal malintencionado que comprometen los sistemas de información como la infraestructura, redes de datos y bases de datos que están alojadas en servidores institucionales. Generalmente estas actividades maliciosas son originadas desde fuentes anónimas y direcciones que no pueden ser rastreadas.
CIBERCRÍMEN (DELITO CIBERNÉTICO)	Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).
CIBERESPACIO	Red independiente de infraestructuras de tecnología de información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (Decreto 338 de 2022, pág. 5).
CIBERSEGURIDAD	Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio. (CONPES 3854, pág. 87).
CÓDIGO MALICIOSO	Es un script o código que fue escrito para generar vulnerabilidades en un sistema de información.
COLCERT	Grupo de respuesta a emergencias cibernéticas de Colombia.
CSIRT PONAL	Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional de Colombia
CSIRT DEFENSA	Equipo de respuesta a incidentes de seguridad digital Ministerio de Defensa.
CSIRT EDUCACIÓN	Equipo de respuesta ante incidentes de seguridad informática y ciberseguridad – Ministerio de Educación
DATOS PERSONALES	Son los datos o información que se relacionan con las personas y que los hace identificables.
DENEGACIÓN DEL SERVICIO	Es una técnica que tiene como objetivo detener la operación de algún sistema de información
ENTORNO DIGITAL	Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).
ENTORNO DIGITAL ABIERTO	Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).
IBTI	Instituto de Bachillerato Técnico Industrial
EVENTO DE SEGURIDAD	Es una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. (Norma ISO 27035)
INCIDENTE DIGITAL	Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
INCIDENTE	Interrupción no planificada de un servicio de TI o reducción de la calidad de un servicio de TI (ITIL v3)
INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Cualquier incidente que se presente y que afecte la confidencialidad, integridad o disponibilidad de los activos de información de la ETITC. (Accesos a los sistemas de información, intrusiones, uso no autorizado, divulgación no autorizada, falsificación o destrucción no autorizada de la información o infección de variantes malware como ransomware y/o secuestro de información).
KAWAK	Aplicativo para Sistemas de Gestión de Calidad
MALWARE	Software malicioso que tiene como objetivo infiltrarse en algún sistema de información sin autorización y de esta forma dañar o perjudicar al propietario de la misma.
MESA DE AYUDA (GLPI)	Aplicación institucional en donde se registran todos los incidentes y servicios de tecnología
PES	Programas de Educación Superior
RESILIENCIA	Capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).
RIESGO DE SEGURIDAD DIGITAL	Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que pueden afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.
SEGURIDAD DE LA INFORMACIÓN	Preservación de la autenticidad, confidencialidad, integridad y disponibilidad de la información, en cualquier medio de almacenamiento: impreso o digital, y la aplicación de procesos de resiliencia operativa.
VULNERABILIDAD	Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

5. CONDICIONES GENERALES Y/O POLITICAS DE OPERACIÓN	Partes interesadas pertinentes al Modelo de Seguridad y Privacidad de la Información y al SGSI de la ETITC y sus necesidades: https://www.etitc.edu.co/archives/partesinteresadasmsp.pdf
	19.1 “Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información”.

6. DESARROLLO DEL PROCEDIMIENTO

No.	DIAGRAMA	ACTIVIDAD- DESCRIPCIÓN	RESPONSABLE	REGISTRO
1		**REGISTRO DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN** Servidores Públicos, Proveedores y demás partes interesadas deben reportar un incidente de seguridad, que identifique o reconozca cualquier actividad y/o situación que ponga en riesgo la confidencialidad, integridad o disponibilidad de los activos de información de la ETITC, a través del correo institucional a la Mesa de Servicios (mesadeayuda@itc.edu.co). Dando cumplimiento a de acuerdo al manual de políticas de SGSI de la ETITC, numeral 19.1 "Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información"	Servidores Públicos, Proveedores y demás partes interesadas.	Correo Institucional a mesadeayuda@itc.edu.co
2		**IDENTIFICACION Y CATEGORIZACIÓN DEL INCIDENTE** El Gestor de Mesa de Servicios se encarga de analizar e identificar el incidente con el fin de priorizar, categorizar como incidente de seguridad digital y asignarlo al Profesional de Seguridad de la Información	Gestor de Mesa de Servicios	Creación de Ticket en el aplicativo de Mesa de Ayuda (GLPI)
3		**INFORMAR AL USUARIO** Se informa a los Servidores Públicos, Proveedores y demás partes interesadas como propietarios o custodios de la información asociado al incidente para que no sea manipulado el activo de información relacionado por él o por más personas de su área y otras recomendaciones**.**	Profesional de Seguridad de la Información	Correo electrónico
4		**ANÁLISIS DEL INCIDENTE DE SEGURIDAD** Ejecutar las actividades de análisis pertinentes en busca de la solución del incidente de seguridad. En caso que el análisis determine que requiere contacto con las autoridades se continua con el paso 5, de lo contrario continúe con el paso 6.	Profesional de Seguridad de la Información	Registro en el aplicativo Mesa de Ayuda (GLPI) y KAWAK (Gestión de Riesgos y Oportunidades)
5		**CONTACTO CON LAS AUTORIDADES** Contactar a las entidades externas oficiales que dan soporte a incidentes de seguridad de la información tales como la COLCERT, CSIRT PONAL, CSIRT DEFENSA, CSIRT EDUCACION, FISCALIA y DIJIN de acuerdo al procedimiento GIC-PC-13 Contacto con las autoridades.	Profesional de Gestión Informática y Telecomunicaciones Profesional de Seguridad de la Información	Correo electrónico
6		**RECOLECCIÓN DE EVIDENCIAS** Se identifica, recolecta y documenta todas las evidencias asociadas al incidente de seguridad según el procedimiento: GSI-PC-01 Identificación, Recolección, Adquisición y Preservación de Evidencias.	Profesional de Gestión Informática y Telecomunicaciones Profesional de Seguridad de la Información	Evidencia física o digital identificada y recolectada
7		**TRATAMIENTO DEL INCIDENTE** El profesional de Seguridad de la Información en conjunto con el área de Informática y Telecomunicaciones, desarrollaran las actividades necesarias para dar tratamiento al incidente de seguridad, documentando en el aplicativo de Mesa de Ayuda (GLPI), las actividades realizadas diligenciando el formato GSI-FO-06 Reporte de eventos e incidentes de seguridad de la información.	Equipo Técnico de Soporte Profesional de Gestión Informática y Telecomunicaciones Profesional de Seguridad de la Información	Histórico en el aplicativo de Mesa de Ayuda (GLPI)
8		**APRENDIZAJE ASOCIADO AL INCIDENTE** Se documenta todo el conocimiento adquirido asociado a la identificación, análisis y respuesta del incidente de seguridad con el fin de reducir la posibilidad y el impacto en futuros incidentes diligenciando el formato GSI-FO-07 Lecciones aprendidas.	Equipo Técnico de Soporte Profesional de Gestión Informática y Telecomunicaciones Profesional de Seguridad de la Información	Histórico en el aplicativo de Mesa de Ayuda (GLPI), por parte del responsable a dar gestión
9		**CERRAR INCIDENTE** Si el incidente se solucionó finaliza el procedimiento y se procede a cerrarlo de acuerdo al procedimiento GIC-PC-08 Gestión de Servicios TI. Si el incidente no se solucionó se devuelve a la actividad 4.	Gestor de Mesa de Ayuda	Histórico en el aplicativo de Mesa de Ayuda (GLPI), por parte del responsable a dar gestión

7. ANEXOS	GSI-PC-01 PROCEDIMIENTO PARA LA IDENTIFICACIÓN, RECOLECCIÓN, ADQUISICIÓN Y PRESERVACIÓN DE EVIDENCIAS DIGITALES.
	GSI-FO-06 REPORTE DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
	GSI-FO-07 LECCIONES APRENDIDAS
	GIC-PC-08 GESTIÓN DE SERVICIOS DE TI.
	GIC-PC-13 PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES.

8. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
16/10/2019	1	Adopción del procedimiento
1/08/2022	2	Redacción del documento Actualización de la sección términos y definiciones Inclusión de grupos CSIRT bajo el decreto 338 del 08 de marzo de 2022, el Gobierno Nacional dictó los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital. Inclusión de términos CERT, CSIRT Ponal, CSIRT Defensa, CSIRT Educación. Ajustes correspondientes al manual de políticas de SGSI de la ETITC, numeral 19.1 "Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información".
20/09/2023	3	Actualización del numeral 4. Definición de términos. Se ajusta numeral 6. Desarrollo del Procedimiento, registro paso 1 en Responsables. Actualización del paso 7. Tratamiento del incidente se diligencia el documento GSI-FO-06 Reporte de eventos e incidentes de seguridad de la información. Actualización del paso 8. Aprendizaje asociado al incidente se diligencia el documento GSI-FO-07 Lecciones aprendidas.

ELABORÓ	REVISÓ	APROBÓ
SANDRA JOHANA GUERRERO GÓMEZ	**ANAY PINTO**	**DORA AMANDA MESA CAMACHO**
Líder del Proceso de Gestión Seguridad de la información	Administrador de la Documentación	Representante de la Dirección

CLASIFICACIÓN DE CONFIDENCIALIDAD	IPB	CLASIFICACIÓN DE INTEGRIDAD	A	CLASIFICACIÓN DE CONFIDENCIALIDAD	1