

1. OBJETIVO

Definir las actividades que permiten cumplir con la responsabilidad de contactar a las autoridades pertinentes, cuando la violación de seguridad de la información no pueda ser tratada internamente por la ETITC, debido a la gravedad de los hechos.

2. ALCANCE

Inicia con la elaboración y/o actualización del mapa de riesgos y finaliza con la documentación del caso.

3. RESPONSABILIDADES

CUSTODIOS DE LA INFORMACIÓN:

- Efectuar un control diario del estado de las instalaciones físicas de las oficinas.
- Efectuar diariamente tareas de monitoreo hacia las actividades de funcionarios, contratistas, docentes.
- Colaborar con la definición del tipo de violación de seguridad.
- En caso de no estar presente el Propietario de la Información, informa al área interna competente para el tratamiento inicial del caso y adicional a la Alta Dirección.

SUPERVISOR DE EMPRESA DE SEGURIDAD PERIMETRAL:

Debe identificar el tipo de desastre materializado. Debe informar, inmediatamente al área de Seguridad de la Información, sobre la materialización del desastre y los daños preliminares identificados.

PROFESIONAL DE INFORMÁTICA Y TELECOMUNICACIONES:

Debe identificar el tipo de desastre materializado. Debe informar, inmediatamente al área de Seguridad de la Información, sobre la materialización del desastre y los daños preliminares identificados.

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
-----------------------------	-----	-----------------------	---	---------------------------	---



Escuela Tecnológica
Instituto Técnico Central

PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES

CÓDIGO: GSI-PC-06
VERSIÓN: 1
VIGENCIA: 2024-07-01
PÁGINA: 2 de 9

EMPRESA DE SEGURIDAD PERIMETRAL CONTRATADA:

Debe implementar las técnicas de análisis e investigación para identificar el origen de la violación de seguridad. Informar a la Alta Dirección sobre los resultados del análisis del caso.

PROFESIONAL DE SEGURIDAD DE LA INFORMACIÓN:

Efectuar entrevistas en las áreas y aplicar la metodología de análisis de riesgos. Colaborar con la definición del tipo de violación de seguridad. Debe implementar técnicas de análisis e investigación para identificar el origen de la violación de seguridad. Informar a la Alta Dirección sobre los resultados del análisis del caso.

SERVIDORES PÚBLICOS:

- Permanecer atentos ante cualquier situación anómala, en cuanto al estado de los equipos, integridad de la información, contraseñas de acceso, etc.
- Colaborar con la definición del tipo de violación de seguridad.
- En caso de no estar presente el Propietario de la Información o el Custodio de la Información, informar al área interna competente para el tratamiento inicial del caso y adicional a la Alta Dirección.


AUTORIDAD EXTERNA:

Estudiar el caso y elaborar un informe donde se evidencie el tratamiento dado a la violación de seguridad y a las acciones tomadas para su sanción.

CONTROL INTERNO DISCIPLINARIO:

Estudiar el caso y elaborar un informe donde se evidencie el tratamiento dado a la violación de seguridad y a las acciones tomadas para su sanción.

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
-----------------------------	-----	-----------------------	---	---------------------------	---

 <p>Escuela Tecnológica Instituto Técnico Central</p>	<p>PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES</p>	<p>CÓDIGO: GSI-PC-06 VERSIÓN: 1 VIGENCIA: 2024-07-01 PÁGINA: 3 de 9</p>
--	--	--

ALTA DIRECCIÓN:

Decide de acuerdo a la gravedad de los hechos, contactar con las autoridades externas, policía, Centro Cibernético Policial, entre otras entidades competentes.

4. DEFINICIÓN DE TÉRMINOS

AUTORIDAD: Grupo de personas o entidades encargadas de resolver una violación de seguridad de la información identificada en la ETITC. A su vez están responsabilidades a dictar medidas de corrección ante las mismas.

ALTA DIRECCIÓN: Hace referencia al Rector de la ETITC, encargado de tomar decisiones definitivas con respecto a las violaciones de seguridad identificadas.

CUSTODIO DE LA INFORMACIÓN: Este rol fue definido para todos los líderes de áreas de la ETITC.

PROPIETARIO DE LA INFORMACIÓN: Este rol fue definido para todos los líderes de procesos de la ETITC.

SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos, que permiten resguardar y proteger la información, preservando, con esto, la confidencialidad, la disponibilidad, integridad y la autenticación segura como principios esenciales para garantizar la continuidad del servicio.

SERVIDOR PÚBLICO: Persona vinculada a la entidad mediante cualquier modalidad: carrera, provisional, ocasional, libre nombramiento y remoción, supernumerario y contratista.

VIOLACIÓN DE SEGURIDAD: Es toda acción que vaya en contra de las políticas de seguridad y privacidad de la información, marcos jurídicos y normativos vigentes, que conlleven al daño o sustracción de medios informáticos e información digital y/o física sin autorización del propietario de la misma. La violación de seguridad puede ser:

- **Física:** Robo de equipos, rotura de puertas, ventanas, candados, pérdida de documentación, ingreso de personal no autorizado a áreas, etc.

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
------------------------------------	-----	------------------------------	---	----------------------------------	---

 <p>Escuela Tecnológica Instituto Técnico Central</p>	PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES	CÓDIGO: GSI-PC-06 VERSIÓN: 1 VIGENCIA: 2024-07-01 PÁGINA: 4 de 9
--	---	---

- **Lógica:** Robo de contraseñas, ingresos a sistemas de información no autorizado, modificación de información no autorizada, ausencia de información en los sistemas, penetración a la LAN institucional no autorizada, etc.

5. REQUISITOS Y CONDICIONES GENERALES

Acuerdo 018 del 2021 “Por el cual se actualiza la Política de Administración del Riesgo de la Escuela Tecnológica Instituto Técnico Central”.

6. DESCRIPCIÓN DEL PROCEDIMIENTO

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
<p>1. ELABORAR Y/O ACTUALIZAR MAPA DE RIESGOS DE VIOLACIONES DE SEGURIDAD.</p> <p>El Profesional de Seguridad de la Información efectúa entrevistas en las áreas y aplica la metodología de análisis de riesgos.</p>	<p>Profesional de Seguridad de la Información.</p>	<p>N/A</p>	<p>Cronograma de Trabajo.</p> <p>Encuestas de Seguridad.</p> <p>GSI-FO-06 Reporte de eventos e incidentes de seguridad de la información.</p>	<p>GDC-FO-09 Mapa y Plan de Tratamiento de Riesgos.</p>
<p>2. REALIZAR CONTROL DIARIO.</p> <p>Para identificar si se han presentado violaciones de seguridad, los Propietarios de la Información, de conjunto con los Custodios de la Información, efectúan un control diario sobre el estado de las instalaciones físicas de las oficinas y un</p>	<p>Propietarios/Custodios de la Información.</p> <p>Servicios públicos, contratistas y partes interesadas.</p>	<p>N/A</p>	<p>N/A</p>	<p>N/A</p>

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
------------------------------------	-----	------------------------------	---	----------------------------------	---

Documento controlado por el Sistema de Gestión de la Calidad

Asegúrese que corresponde a la última versión consultando el microsítio de calidad de la Escuela Tecnológica Instituto Técnico Central (ETITC)



Escuela Tecnológica
Instituto Técnico Central

PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES

CÓDIGO: GSI-PC-06
VERSIÓN: 1
VIGENCIA: 2024-07-01
PÁGINA: 5 de 9

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
<p>monitoreo hacia las actividades de servidores públicos.</p> <p>Los servidores públicos se mantienen atentos ante cualquier situación anómala, en cuanto al estado de los equipos, integridad de la información, contraseñas de acceso, etc.</p>				
<p>3. IDENTIFICAR VIOLACIONES.</p> <p>Una vez realizado el control diario, si se identifican violaciones de seguridad se debe identificar el tipo de violación, de lo contrario finaliza.</p>	<p>Propietarios/Custodios de la Información.</p> <p>Servicios públicos, contratistas y partes interesadas.</p>	N/A	N/A	N/A
<p>4. DEFINIR E INFORMAR TIPO DE VIOLACIÓN.</p> <p>Se verifica si la violación es de tipo Física y/o Lógica.</p> <p>Para el tratamiento inicial del caso se debe informar verbalmente por cualquier vía (personal o telefónica) al área de Seguridad de la Información y/o Informática y Telecomunicaciones, si la violación es de tipo lógica y/o a la Empresa de Seguridad Perimetral, si la violación es de tipo Física. En ambos casos se debe informar a la Alta Dirección.</p>	<p>Propietarios/Custodios de la Información.</p> <p>Supervisor de Empresa de Seguridad Perimetral.</p> <p>Profesional de Seguridad de la Información.</p> <p>Servicios públicos, contratistas y partes interesadas.</p>	N/A	N/A	N/A

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
-----------------------------	-----	-----------------------	---	---------------------------	---



Escuela Tecnológica
Instituto Técnico Central

PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES

CÓDIGO: GSI-PC-06
VERSIÓN: 1
VIGENCIA: 2024-07-01
PÁGINA: 6 de 9

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
<p>Nota: Si la violación física implica el robo de algún recurso informático (computador, servidor, medios de almacenamiento, etc) y/o documentos en físico, debe notificarse también al área de Seguridad de la Información.</p>				
<p>5. ANÁLISIS DE CASO.</p> <p>El área correspondiente (Seguridad de la Información o la Empresa de Seguridad Perimetral contratada), implementa técnicas de análisis e investigación, para identificar el origen de la violación de seguridad.</p>	<p>Supervisor de Empresa de Seguridad Perimetral.</p> <p>Empresa de Seguridad Perimetral contratada.</p> <p>Profesional de Seguridad de la Información.</p>	N/A	N/A	N/A
<p>6.COMUNICAR RESULTADOS.</p> <p>Las áreas correspondientes (Seguridad de la Información, Informática y Telecomunicaciones o la Empresa de Seguridad Perimetral contratada), debe informar a la Alta Dirección sobre los resultados del análisis del caso.</p>	<p>Supervisor de Empresa de Seguridad Perimetral.</p> <p>Empresa de Seguridad Perimetral contratada.</p> <p>Profesional de Seguridad de la Información.</p> <p>Profesional de Informática y Telecomunicaciones</p>	N/A	N/A	N/A
<p>7. TOMA DE DECISIÓN.</p> <p>La Alta Dirección, de acuerdo a la gravedad de los hechos decide si se contacta con las</p>	<p>Alta Dirección.</p>	N/A	N/A	N/A

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
------------------------------------	-----	------------------------------	---	----------------------------------	---



Escuela Tecnológica
Instituto Técnico Central

PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES

CÓDIGO: GSI-PC-06
VERSIÓN: 1
VIGENCIA: 2024-07-01
PÁGINA: 7 de 9

DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	CONTROL	DOCUMENTO DE REFERENCIA	REGISTRO RESULTANTE
autoridades externas, Policía Nacional, Centro Cibernético Policial y/o Grupo CSIRT Gobierno, entre otras entidades competentes y/o la oficina de Control Interno Disciplinario de la ETITC.				
8. DOCUMENTAR EL CASO. La autoridad externa o Control Interno Disciplinario de la ETITC, debe elaborar un informe dirigido a la Alta Dirección, en el cual se evidencie el tratamiento dado al caso de violación de seguridad y las acciones tomadas para su sanción.	Autoridad Externa. Control Interno Disciplinario.	N/A	N/A	Informe de Tratamiento al Caso.

7.ANEXOS:

GSI-FO-06 Reporte de eventos e incidentes de seguridad de la información.
GDC-FO-09 Mapa y Plan de Tratamiento de Riesgos.

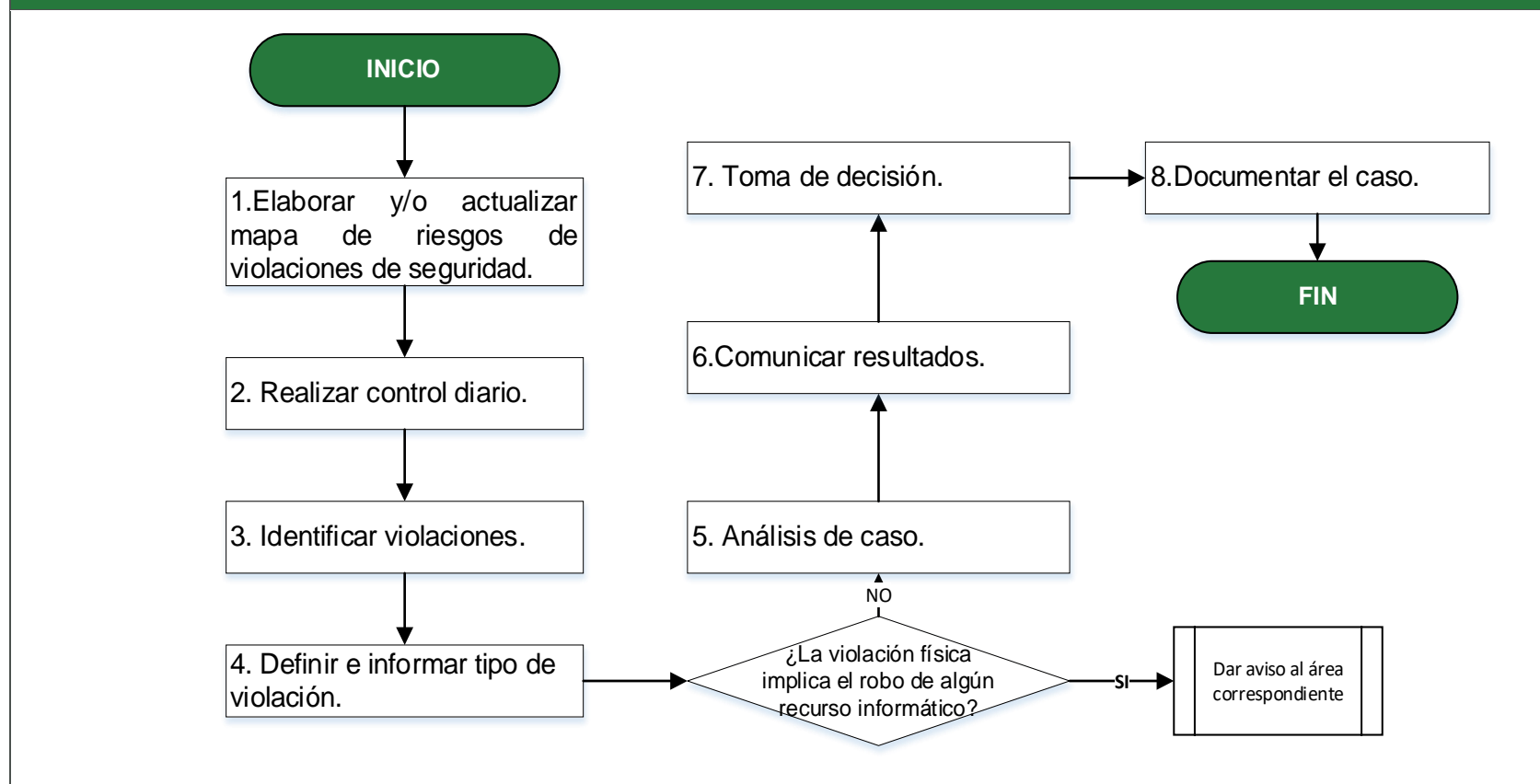
CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
-----------------------------	-----	-----------------------	---	---------------------------	---

Documento controlado por el Sistema de Gestión de la Calidad

Asegúrese que corresponde a la última versión consultando el microsítio de calidad de la Escuela Tecnológica Instituto Técnico Central (ETITC)



8. DIAGRAMA DE FLUJO



 <p>Escuela Tecnológica Instituto Técnico Central</p>	<p>PROCEDIMIENTO CONTACTO CON LAS AUTORIDADES</p>	<p>CÓDIGO: GSI-PC-06 VERSIÓN: 1 VIGENCIA: 2024-07-01 PÁGINA: 9 de 9</p>
---	--	--

9.SISTEMAS DE INFORMACIÓN			
SISTEMA DE INFORMACIÓN	DESCRIPCIÓN	FRECUENCIA	UBICACIÓN
N/A	N/A	N/A	N/A

10. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
2024-07-01	1	Adopción del procedimiento.

ELABORÓ	REVISÓ	APROBÓ
<p>SANDRA GUERRERO G. Líder del Proceso de Seguridad de la Información</p>	<p>ANAY PINTO VALENCIA Administrador de la Documentación</p>	<p>JORGE HERRERA ORTIZ Representante de la Dirección</p>

CLASIF. DE CONFIDENCIALIDAD	IPR	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1
------------------------------------	-----	------------------------------	---	----------------------------------	---