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

Propietarios 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.
- Definir el tipo de violación de seguridad.
- Informar al área interna competente para el tratamiento inicial del caso y adicional a la Alta Dirección.

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.

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.

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, informa al área interna competente para el tratamiento inicial del caso y adicional a la Alta Dirección.

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

Área de Informática y Comunicaciones: Implementa 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.
Empresa de Seguridad Perimetral contratada: 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.

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.

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.

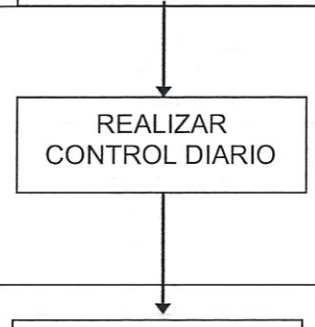
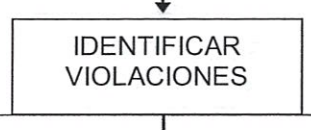
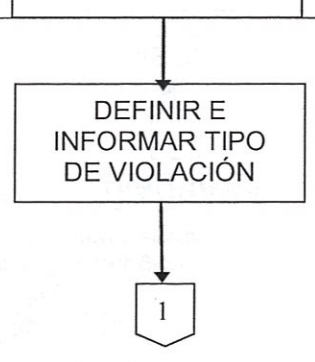
SEGURIDAD DE LA INFORMACIÓN: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos, que permiten resguardar y proteger la información, preservando, con esto, la confidencialidad, la disponibilidad y la integridad de la información.

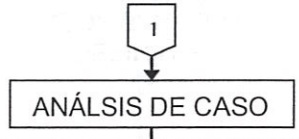
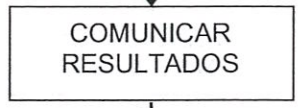
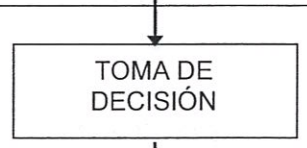
SERVIDOR PÚBLICO: Persona vinculada a la entidad mediante cualquier modalidad: carrera, provisional, ocasional, libre nombramiento y remoción, supernumerario y contratista.

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.
- 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. DESCRIPCIÓN DEL PROCEDIMIENTO

No.	DIAGRAMA	ACTIVIDAD - DESCRIPCIÓN	RESPONSABLE	REGISTRO
1		**ELABORAR Y/O ACTUALIZAR MAPA DE RIESGOS DE VIOLACIONES DE SEGURIDAD** El Profesional de Seguridad de la Información efectúa entrevistas en las áreas y aplica la metodología de análisis de riesgos.	Profesional de Seguridad de la Información. .	Cronograma de Trabajo. Encuestas de Seguridad. Mapa de Riesgos.
2		**REALIZAR CONTROL DIARIO** 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 monitoreo hacia las actividades de servidores públicos. 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.	Propietarios/Custodios de la Información. Servicios públicos	NA
3		**IDENTIFICAR VIOLACIONES** Una vez realizado el control diario, si se identifican violaciones de seguridad se debe identificar el tipo de violación, de lo contrario finaliza.	Propietarios/Custodios de la Información. Servidores públicos	NA
4		**DEFINIR E INFORMAR TIPO DE VIOLACIÓN** Se verifica si la violación es de tipo Física y/o Lógica. Para el tratamiento inicial del caso se debe informar verbalmente por cualquier vía (personal o telefónica) al área de Informática y Comunicaciones, si la violación es de tipo lógica y/o a la Compañía de Seguridad Perimetral, si la violación es de tipo Física. En ambos casos se debe informar la Alta Dirección. **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 Informática y Comunicaciones.	Propietarios/Custodios de la Información. Profesional de Seguridad de la Información. Servidores públicos	NA

No.	DIAGRAMA	ACTIVIDAD - DESCRIPCIÓN	RESPONSABLE	REGISTRO
5		**ANÁLISIS DE CASO** El área correspondiente (Informática y Comunicaciones o la Empresa de Seguridad Perimetral contratada), implementa técnicas de análisis e investigación, para identificar el origen de la violación de seguridad.	Área de Informática y Comunicaciones. Empresa de Seguridad Perimetral contratada.	NA
6		**COMUNICAR RESULTADOS** El área correspondiente (Informática y Comunicaciones o la Empresa de Seguridad Perimetral contratada), debe informar a la Alta Dirección sobre los resultados del análisis del caso.	Área de Informática y Comunicaciones. Empresa de Seguridad Perimetral contratada.	NA
7		**TOMA DE DECISIÓN** La Alta Dirección, de acuerdo a la gravedad de los hechos decide si se contacta con las autoridades externas, policía, Centro Cibernético Policial, entre otras entidades competentes y/o la oficina de Control Interno Disciplinario de la ETITC.	Alta Dirección.	NA
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.	Informe de Tratamiento al Caso.

6. ANEXOS

NA

7. CONTROL DE CAMBIOS

FECHA	VERSION	CAMBIOS
11-11-2016	1	Adopción del procedimiento
17-09-2018	2	Actualización del procedimiento por inclusión del etiquetado de la información.

ELABORÓ	REVISÓ	APROBÓ
DAVID LEONARDO TORRES RODRÍGUEZ Líder del Proceso de Informática y Comunicaciones	**YANETH JIMENA PIMIENTO CORTES** Administrador de la Documentación	**DORA AMANDA MESA CAMACHO** Representante de la Dirección