



REPORTE DE INCIDENTES 2 SEMESTRE 2022



**SEGUNDO SEMESTRE
AÑO 2022**





1. OBJETIVO

Dar a conocer los resultados de los incidentes presentados durante el segundo semestre 2022.

2. ALCANCE

El presente informe muestra los resultados obtenidos en el análisis de desempeño de la seguridad de la información en la Universidad.

3. ANÁLISIS DE RESULTADOS

a. Indicadores del Sistema de Gestión De Seguridad De La Información SGSI – ISO 27001:2013

Los indicadores definidos para el Sistema de Gestión de Seguridad de la Información SGSI, se encuentran en el PLAN DE GESTION DE SERVICIOS DE TI Y SEGURIDAD DE LA INFORMACION A-RI-L03, donde se puede evidenciar la relación con los objetivos, meta y frecuencia de medición.

Los resultados de la medición realizada hasta diciembre de 2022, se observan a continuación:

INDICADORES SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

Fecha de Corte: diciembre 2022.

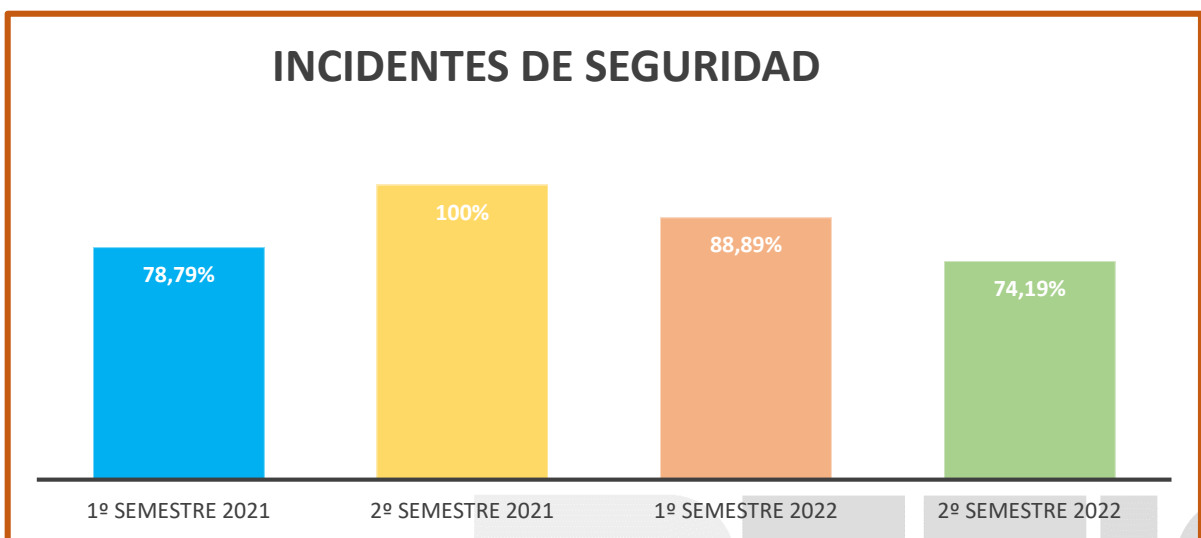
No	Nombre del indicador	Frecuencia	Meta	1º Semestre 2021	2º Semestre 2021	1º Semestre 2022	2º Semestre 2022
3	Tratamiento de incidentes de seguridad de la información	Semestral	90%	78,79%	100%	88,89%	74,19

En la tabla anterior se evidencia el comportamiento del indicador Tratamiento de incidentes de seguridad de la información. En el primer semestre del 2021, quedaron pendientes unas



incidencias de seguridad que estaban siendo atendidas, por tal razón es la disminución en el cumplimiento de la meta.

Para el año 2022, en el primer trimestre se presentaron 27 incidentes de seguridad, de los cuales se dio respuesta en los tiempos establecidos a 23 de ellos, en el segundo trimestre se presentaron 9 incidentes de seguridad a los cuales se les atendió en los tiempos establecidos dando como resultado para el primer semestre 2022 un cumplimiento del 88%. a pesar de que faltaron 2 puntos porcentuales para cumplir la meta la dirección de tecnologías hace lo posible para cumplir con los tiempos para dar respuesta a los incidentes de seguridad que se presenten, para el segundo semestre de 2022 se presentó de la siguiente manera: el tercer trimestre del 2022 llegaron 21 correos electrónicos al correo de soporte.seguridad@uptc.edu.co, a los cuales se les dio respuesta oportuna a 15 y 6 de ellos se ignoraron debido a que no estaba relacionados con seguridad de la información. para el cuatro trimestre del 2022 se dio respuesta oportuna a 8 correos electrónicos y se ignoraron 2 puesto que no estaban relacionados con seguridad de la información, por tal motivo durante el semestre se ignoraron 8 correos y lo cual refleja un desfase en el cumplimiento de la meta a pesar de no contar con una mesa de servicio. Se está trabajando en la implementación de la mesa de servicio institucional la cual ya se encuentra en pruebas





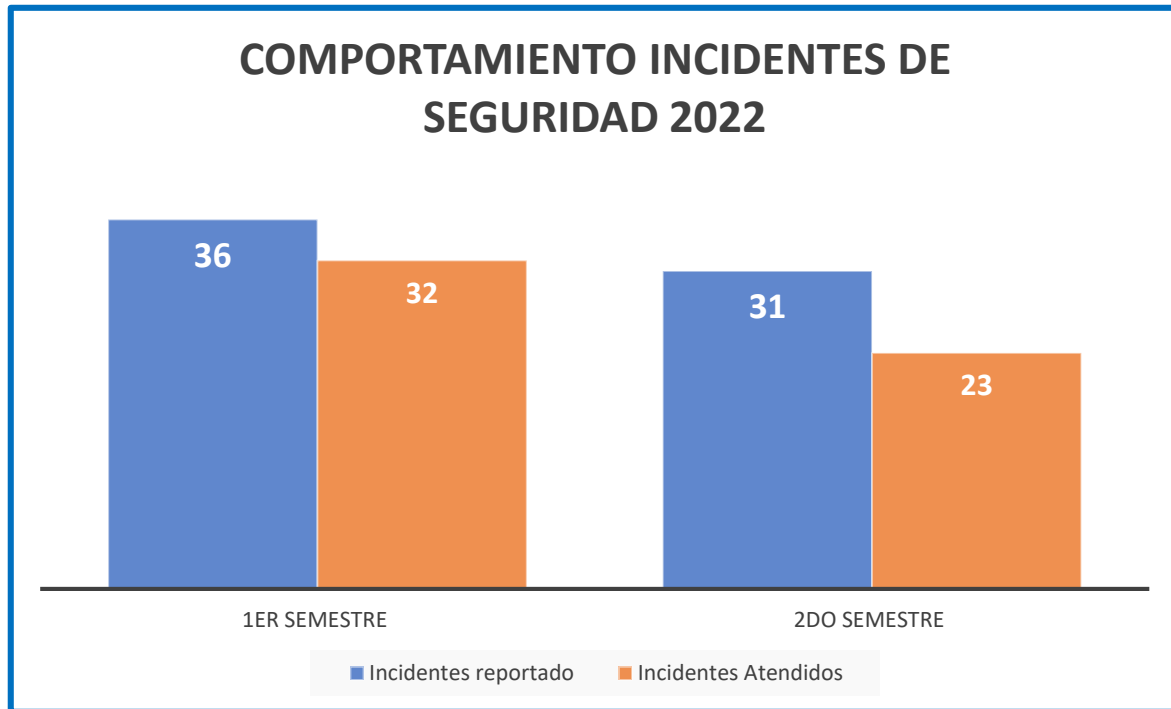
La Dirección de las Tecnologías y Sistemas de la información y de las Comunicaciones, ha realizado varias actividades al interior de la universidad, para disminuir el impacto cuando se presentan amenazas a la seguridad de la información, las medidas tomadas este año fueron las siguientes:

- ✓ Envío de correo masivo a la comunidad universitaria, alertando sobre correos maliciosos.
- ✓ Generación de campaña seguridad de la información a través de la página institucional.
- ✓ Envío de correo masivo con consejos sobre seguridad de la información.
- ✓ Publicación de campañas de seguridad de la información en redes sociales.
- ✓ Capacitaciones a las diferentes dependencias sobre el buen uso de la infraestructura tecnológica para reconocer ataques y evitar incidentes de seguridad.
- ✓ Implementación de nuevas herramientas para la identificación, descripción y control contra software ilegal
- ✓ Mantenimiento correctivo en ordenadores sospechosos de tener software malicioso.

Incidentes de seguridad

En investigaciones sobre seguridad durante el año se han atendido las incidencias reportadas a través de los correos electrónicos a la dirección soporte.seguridad@uptc.edu.co.

Para el primer semestre del año se obtuvieron los siguientes resultados:



Para el año 2022, en el primer trimestre se presentaron 27 incidentes de seguridad, de los cuales se dio respuesta en los tiempos establecidos a 23 de ellos, en el segundo trimestre se presentaron 9 incidentes de seguridad a los cuales se les atendió en los tiempos establecidos dando como resultado para el primer semestre 2022 un cumplimiento del 88%. a pesar de que faltaron 2 puntos porcentuales para cumplir la meta la dirección de tecnologías hace lo posible para cumplir con los tiempos para dar respuesta a los incidentes de seguridad que se presenten, para el segundo semestre de 2022 se presentó de la siguiente manera: el tercer trimestre del 2022 llegaron 21 correos electrónicos al correo de soporte.seguridad@uptc.edu.co, a los cuales se les dio respuesta oportuna a 15 y 6 de ellos se ignoraron debido a que no estaba relacionados con seguridad de la información. para el cuarto trimestre del 2022 se dio respuesta oportuna a 8 correos electrónicos y se ignoraron 2 puesto que no estaban relacionados con seguridad de la información, por tal motivo durante el semestre se ignoraron 8 correos y lo cual refleja un desfase en el cumplimiento de la meta a pesar de no contar con una mesa de servicio. Se está trabajando en la implementación de la mesa de servicio institucional la cual ya se encuentra en pruebas.