UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS	**FORMATO: ACTA DE REUNIÓN**	Código: GI-FR-010	SIGUD
	Macroproceso: Direccionamiento Estratégico	Versión: 03	
	Proceso: Gestión Integrada	Fecha de Aprobación: 21/03/2017	

ACTA No. 007		
Proceso: Gestión de los Sistemas de la Información y las Telecomunicaciones		
Unidad Académica y/o Administrativa: Oficina Asesora de Tecnologías e Información		**Hora de Inicio:** 7:00 a.m.
Motivo y/o Evento: Comité de Transformación Digital		**Hora de finalización:** 8:00 a.m.
Lugar: Teams (virtual)		**Fecha:** 12 de septiembre de 2023
Participantes	**Nombre**	**Cargo**
	Alejandro Paolo Daza	Jefe Oficina Asesora de Tecnologías e Información
	Andrés Julián Moreno	Representante Laboratorios
	Carlos Montenegro	Coordinador RITA - PlanesTIC
	Elvis Gaona	Coordinador Doctorado en Ingeniería
	Giovanny Mauricio Tarazona	Rector Universidad Distrital
	Jheshua Larrota Alférez	CPS Coordinación TI Oficina de Extensión
	Julián Guerrero	CPS Red de Datos
	Martha Valdés	Líder Programa Red UDNET
	Nelson Orozco	Asesor Rectoría
	Santiago López	CPS Red UDNET
	Viviana Álvarez	CPS Oficina Asesora de Tecnologías e Información
Elaboró: Viviana Álvarez	**Visto Bueno del Acta:**	

OBJETIVOS:

- Revisión estado de la Resolución de reorganización del Comité de Transformación Digital
- Presentación de informe sobre el evento de seguridad del 30 de julio de 2023

ORDEN DEL DÍA:

1. Revisión del estado de la Resolución de reorganización del Comité de Transformación Digital
2. Presentación de informe sobre el evento de seguridad del 30 de julio de 2023
3. Varios

DESARROLLO:

1. **Revisión del estado de la Resolución de reorganización del Comité de Transformación Digital**

Se abre la reunión con la intervención del Ingeniero Nelson Orozco, que indica que la resolución en mención y pasó la revisión por la Oficina Asesora Jurídica, donde se le hicieron unas observaciones de forma al documento. También se incluyó a un delegado de Planestic por parte de Rectoría, por lo que solamente está pendiente la recogida de las antefirmas para la rúbrica del Rector.

Por otro lado, se menciona que en el documento del comité se hace énfasis en la importancia de definir un modelo financiero y la estructura de los componentes relacionados a TI. Teniendo en cuenta lo anterior, se afianza la responsabilidad para identificar y registrar el modelo financiero, que pueda generar sostenibilidad financiera para el PETI.

Dentro de las responsabilidades que se deben tener en cuenta en el momento que se apruebe la resolución del Comité, se destaca el control estratégico de las tecnologías, evitar dispersión de TI y generar escenarios de economía a escala, optimizando el uso de las tecnologías. También indica que los riesgos de no trabajar en estos aspectos, genera escenarios de inseguridad, falta de control de componentes de TI y falta de soporte, atención a equipos finales, infraestructura tecnológica y de sistemas de información.

2. **Presentación de informe sobre el evento de seguridad del 30 de julio de 2023**

Se abre el siguiente punto de la reunión con la proyección y presentación del informe relacionado al evento de seguridad por parte del Ingeniero Alejandro Daza. A continuación, se presenta la información relacionada:

- **Origen de la amenaza:** La afectación se dio por el ransomware trigona, el cual está orientado a sistemas operativos Windows. Se detectó por primera vez en la sede de Bosa con ataque de fuerza bruta a credenciales de inicio de sesión y que se propaga a través de conexión a internet. El ataque cifró archivos con extensión .locked
  Se puso en conocimiento al proveedor infocomunicaciones SAS del incidente y el proveedor dio una serie de recomendaciones para enfrentar el ataque, entre esas, no realizar ningún tipo de pago al atacante.
- **Contención de la amenaza:** Se realizó la desconexión de los equipos de la red y se bajaron los servicios de conectividad para evitar la propagación del ransomware. Luego se analizó un equipo para enviar el reporte a Karspersky.

- **Detección de la amenaza:** Con la herramienta Karspersky Virus Removal Tool se realizó el escaneo de los equipos y se verificó la instalación del antivirus más actualizada. Además, se realizó la verificación y desconexión de recursos no autorizados. Se validó que no se hayan creado nuevos usuarios y se limitó el uso de credenciales privilegiadas.
- **Mitigación de la amenaza:** Se realizó la actualización y parcheo de todos los equipos por las personas del área de TI y se realizó la Implementación de cuatro consolas de administración, en las que se agregaron licencias KEDRO. También se realizó la definición de políticas de acceso web y dispositivos extraíbles, segmentación de la red y WiFi.
- **Recuperación de información y servicios:** Para este fin se realizó:
    - El formateo de equipos afectados y restablecimiento de backups de servidores
    - El despliegue de DNS (directorio activo) y DHCP
    - La habilitación del servicio de internet
    - El restablecimiento de los backups de carpetas compartidas, de las páginas bajo el dominio udistrital y de la conexión por VPN (con control de acceso por grupos)
    - La habilitación del servicio de telefonía
    - Se realizó el envío de circulares el 30 de julio de 2023 y de protocolo de restablecimiento de servicios de conectividad en sedes, desde la Rectoría y la OATI.

Queda pendiente el informe por parte del CSIRT.

Cuando se finaliza la presentación del informe por parte del Ingeniero Alejandro Daza, el Rector interviene y señala que éste se debe complementar para su presentación al Consejo Superior Universitario con los siguientes ítems:

- Realizar el timeline del incidente, describiendo el modo, tiempo y lugar de las acciones que se realizaron e indicar el porcentaje de servicios reestablecidos.
- Indicar los costos asociados al evento de seguridad relacionados a la infraestructura física (equipos, discos duros, entre otros) y de operación.
- ¿Cuál es el protocolo para afrontar un nuevo ataque? Que se debe hacer y qué inversiones de deben realizar. Qué soporte adicional se deben solicitar para mitigar un ataque de esa naturaleza.

Po otro lado, resalta la importancia de tener una política de seguridad, un tercero de confianza y los servicios centrales en la nube.

El profesor Daza acota que se va a trabajar con el equipo sobre los ítems descritos. A su vez, señala que es importante comenzar a trabajar en el proyecto de implementación de seguridad de la información, donde se identifiquen las vulnerabilidades. También indica que se ha avanzado en el análisis de brecha y determinación de riesgos.

Por otro lado, resalta la importancia de realizar la contratación de un oficial de seguridad, no solo de las áreas de TI, sino para que dé lineamientos de seguridad a nivel institucional, que puedan apoyar la capacidad de decisión de la institución.

El profesor Tarazona menciona la importancia de trabajar en la política de seguridad de la información. La importancia de la definición de este plan se denota con una serie de ejemplos de incidentes que han sucedido por no contar con estas directrices, como el acceso y entrega de información no autorizada.

Con el fin de realizar la correcta definición e implementación del plan, se resalta:

- Tener un solo enfoque que oriente la decisión de inversión, identificando los recursos y generando la posibilidad de gestionar los recursos de cara al presupuesto del 2024 y 2025, en un ejercicio de planeación.
- Tener claridad en las necesidades de equipos, reconversión tecnológica.
- Mejorar y habilitar la conectividad de las sedes de la Universidad, con condiciones de seguridad.

El Ingeniero Orozco menciona que es fundamental generar una integración de todo tipo que esté alineada al PETI y, sobre todo, tener claros los escenarios de riesgo para la Universidad para mitigar los incidentes de seguridad y poder optimizar los recursos informáticos.

Mencionó que se debe trabajar en torno a la arquitectura institucional, sobre todo a lo relacionado con el inventario de activos de información, pues es prioritario que la Universidad determine la clasificación de la información que tiene en su custodia, el sistema que maneja esa información y donde reposa ésta, además de saber cuál es el aseguramiento de la data y de los aplicativos que la manejan. Al respecto, señala que ya se tiene ruta clara de modelo de seguridad y privacidad de la información, y que ya se cuenta con recursos de PFC y estos recursos deben estructurarse y comprometerse.

Por último, señala los proyectos que se deben tener en el radar del Comité de Transformación Digital, divididos en los que se estructuraron en el Comité y los que no:

Proyectos no estructurados en el comité:

- Sistema de Gestión Documental Electrónica (SGDA)
- Proyecto de Gestión documental
- MIPG: sistema de información que permita manejar el sistema integrado de planeación y gestión.

Proyectos estructurados en el comité:

- Modelo de seguridad y privacidad de la información
- Sistema de Gestión Académica: al respecto, señala que se tienen los recursos para la ejecución del proyecto (por una parte, 500 millones y el saldo será tramitado con excedentes presupuestales)

- Proyecto de identificación de integrantes de la comunidad universitaria: Este proyecto busca identificar a los miembros de la Universidad y generar una dinámica más flexible en programas de Bienestar, entre otros.

Teniendo en cuenta el poco tiempo, se señala la importancia de estructurar los estudios previos requeridos para los proyectos.

3. Varios

El Ingeniero Jheshua resalta el trabajo del equipo realizado en la mitigación del evento de seguridad y menciona que por parte de la Oficina de Extensión se ha venido trabajando en la recuperación de la información, resolviendo temas de conectividad. También propone:

- Continuar con el plan de políticas de seguridad de la información que se ha venido adelantando en la Oficina de Extensión, que ya tiene cierto nivel de madurez.
- Trabajar en el proyecto de caracterización de activos de información: Con automatización y el uso de Inteligencia Artificial se están identificando qué conforman los activos de información y cómo están categorizados.

Al respecto, el profesor Daza menciona que es importante no dejar ese trabajo de lado, pero que es importante trabajar con el equipo de seguridad de la OATI y de la Red de datos para que no sea un trabajo suelto.

Por otro lado, el profesor Montenegro precisa que se debe actualizar la organización del Comité, pues el aparece como la persona que preside el espacio. Al respecto, el ingeniero Orozco indica que esta actualización se realizará a través de un acto administrativo, una vez se firme la resolución de reorganización del comité.

Por último, el profesor Gaona resalta la importancia de establecer la hoja de ruta para la mitigación de ataques, teniendo en cuenta la contingencia presentada en días anteriores.

Encargado	Compromiso	Fecha
Alejandro Paolo Daza - Jefe OATI	Entregar del informe ejecutivo que incluya el timeline de recuperación del servicio, el estado actual y los costos asociados.	26 de septiembre de 2023
Alejandro Paolo Daza - Jefe OATI	Informe del avance de la implementación del ERP con la prospectiva de inversión y desarrollo de éste.	26 de septiembre de 2023

Firma

Alejandro Paolo Daza Corredor
Secretaría Técnica Comité de Transformación Digital