# INSTITUTO DISTRITAL DE DEPORTES Y RECREACIÓN -IDER

## CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

| ITEM | PROCESOS | ACTIVIDADES | TAREAS | Fecha de inicio | Fecha final | Responsable | Indicadores de resultados | SEGUIMIENTO 1er TRIMESTRE (ENE - MAR) | | SEGUIMIENTO 2DO TRIMESTRE (ABR - JUN) | | SEGUIMIENTO 3ER TRIMESTRE (JUL - SEP) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Resultados de avance 1 | Observación | % de AVANCE 2 | Observación | % de AVANCE 3 | Observación |
| 1 | Gestión de TI | Actuallización de los planes de Gestión de TI de la entidad, de acuerdo al decreto 612 de 2018. | Actuallizar plan de PTRSPI de laGestión de TI de la entidad. | 2021/01/14 | 2021/06/30 | Sistemas | * PTRSPI Actualizado | 100% | Actualizado el PTRSPI, y publicado en la pagina web institucional | 100% | Publicación ejecución a 30 junio 2021 | 100% | Publicación ejecución a 30 Septiembre 2021 |
| 2 | Gestión de TI | Sencibilización | Realizar campañas de sencibilización de los Riesgos de ciberseguridad y privacidad de la información | 2021/01/15 | 2021/06/30 | Sistemas | Evidencia de la socialización | 80% | Se realizo sencibilizacion en sitio sobre el uso de los equipos tecnologicos, la adecuada conexion a los estabilizadores, el adecuado encendido y apagado de los equipos, y distribucion de la informacion en almacenada en las carpetas y discos duros. | 80% | Se esta realizando una estrategia de sencibilizacion en temas de ciber seguridad | 80% | Se esta realizado campaña de sencibilizacion en temas de ciber seguridad. |
| 3 | Gestión de TI | Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación. | Identidicación, Analisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación. | 2021/02/01 | 2021/06/30 | Sistemas | Mapa de Riesgo | 100% | Se reporta el mapa de riesgo y planes de tratamiento en el PTRSPI pag 33 | 100% | Se realizo la identificacion, analisisi y evaluacion de los riesgos de seguridad digital en el componente de riesgo del plan de anticorrupcion | 100% | Se realizo la identificacion de nuevos riesgos de seguridad digital. |
| 4 | Gestión de TI | Publicación | Realimentación, Revisión y verificación de los riesgos identificados. | 2021/02/15 | 2021/06/30 | Sistemas -Planeación | Mapa de Riesgo (Ajustado) | 100% | Mapa de riesgo agustado | 100% | Mapa de riesgo agustado | 100% | Se realizo la identificacion, analisis y evaluacion de los riesgos de seguridad digital en el componente de riesgo del plan de anticorrupcion. |
| 5 | Gestión de TI | | Publicación del Mapa de riesgo | 2021/03/01 | 2021/06/30 | Sistemas -Jurídica | Link del Mapa de riesgo en la web | 100% | http://www.ider.gov.co/images/2020/OKPLAN-TRATAMDERIESGOS-DE-SEGUR-Y-PRIVAC-DE-LA-INFOR-IDER.pdf | 100% | http://ider.gov.co/index.php/centro-de-descarga/category/9-transparencia?download=499:seguimiento-plan-anticorrupcion-y-atencion-al-ciudadano-a-junio-2021 | 100% | http://ider.gov.co/index.php/centro-de-descarga/category/9-transparencia?download=541:seguimiento-plan-anticorrupcion-y-atencion-al-ciudadano-a-septiembre-2022 |

| ITEM | PROCESOS | ACTIVIDADES | TAREAS | Fecha de inicio | Fecha final | Responsable | Indicadores de resultados | SEGUIMIENTO 1er TRIMESTRE (ENE - MAR) | | SEGUIMIENTO 2DO TRIMESTRE (ABR - JUN) | | SEGUIMIENTO 3ER TRIMESTRE (JUL - SEP) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Resultados de avance 1 | Observación | % de AVANCE 2 | Observación | % de AVANCE 3 | Observación |
| 6 | Gestión de TI | reconoser como mitigar los riesgos a traves de poiticas de seguridad para el control en el acceso de contenido a la red y equipos de computos | Implementar politicas de seguridad para mitigar los riesgos al acceder a las redes Wi-Fi, Internet, equipos de computos, servidores y aplicaciones de gestion de informacion | 2021/03/01 | 2021/06/30 | Sistemas | Politicas implementadas y documentadas en el Firewall , con reglas de filtrados y contenidos no deseados, liniamientos y procedimientos para el correcto control de acceso a la red y equipos | 100% | Se actualizaron las siguientes politicas de seguridad:<br>a) El registro de los equipos a la red Wi-fi con password<br>c) las restricciones para la instalación de software;<br>d) los requisitos para las versiones y licencia del software de los equipos,<br>e) los controles de acceso para acceder a internet;<br>g) Roles y contraseñas para cuentas de usuarios administradores y usuarios de escritorios<br>h) protección contra software malicioso;<br>i) Control en el acceso por enlaces remotos,<br>j) copias de respaldo base de datos<br>k) uso de servicios y aplicaciones web.<br>k) Los equipos portátiles personales que ingresen al Instituto deben<br>Revisado por el equipo de sistemas y debeb presentar las lisencias del S.O. y de los programas instalados. | 100% | Politicas implementadas y documentadas en el Firewall , con reglas de filtrados y contenidos no deseados, liniamientos y procedimientos para el correcto control de acceso a la red y equipos | 100% | Monitoreo de reglas de filtrados y contenidos no deseados, del uso de los recursos en la red. |
| | | | | | | | | **97%** | | **97%** | | **97%** | |
| | | | | | | | | **24%** | | **24%** | | **24%** | |