***SEGUNDO CUATRIMESTRE SEGUIMIENTO PLAN TRATAMIENTO DE RIESGOS DE SEGURIDADY PRIVACIDAD DE LA INFORMACIÓN***

| **TIPO DE ACTIVO** | **VULNERABILIDADES** | **AMENAZAS** | **SEGUNDO CUATRIMESTRE 2021** |
| --- | --- | --- | --- |
| SERVICIO DE INTERNET, SERVIDORES, SWITCH CORE, DE BORDE, AP, ROUTER , REDES LAN, Wi-Fi.  Ataques a la plataforma informática. | Los ataques pueden ser internos o externos por:   * Deficiencia o falta de una Política de Seguridad Informática institucional definida correctamente para el uso los Sistemas Informáticos del INCI * Herramientas de Seguridad Perimetral poco eficaces en hardware y software en la construcción e implantación de Políticas eficaces en el INCI | Accesos no autorizados por parte de “delincuentes informáticos” u otros con pretensiones de causar daños potenciales a la Red informática del INCI y datos contenidos en estos, mediante ataques a los sistemas que componen la Plataforma Informática. | Se da aplicación a la Política de seguridad de la información Resolución No.20161010000683 del 16/03/2016.  Se ejecuta el contrato de conectividad No.052/21, con la empresa IFX NETWORKS.  Se verifica diariamente el buen funcionamiento de la RED LAN, servidores con diferentes servicios, switches, también en eventos de cortes inesperados de energía eléctrica no regulada en la zona (ubicación del INCI), también regulada y UPS.  Se ejecuta el contrato No. 061/21 Wilmar Medina para mantenimiento y soporte de equipos SWITCH CORE, DE BORDE, AP, ROUTER REDES LAN, Wi-Fi |
| EQUIPOS SERVIDORES INSTITUCIONALES  Pérdida de información en los Servidores | * Falta de mantenimiento preventivo y correctivo a los Sistemas de : * Equipos Servidores * Sistema eléctrico regulado – UPS´s * Red LAN. * Servidores que componen la Planta Informática. * Desconocimiento de los Ingenieros * Por des configuración en equipos. * Ausencia de un sistema de Backup´s o copias de respaldo. * Falta Tercerizar algunos servicios de importancia en la NUBE * Soportes poco idóneos. * Ausencia de Políticas de Seguridad Informática para los Servidores. * Desarrollos inadecuados de aplicativos o implementaciones mal realizadas. * Falta o ausencia de documentación técnica. | Daños físicos y/o lógicos en los servidores institucionales.   * Caída de la red LAN * Fallo en el Fluido eléctrico regulado por UPS´s * Propagación de virus y/o programas basura como SPAM, entre otros. * Daños en aplicativos y/o Base de Datos. * Daños físicos en discos duros (HDD) * Alteración de los desarrollos de los aplicativos * Caídas del servicio de Internet o Conectividad. * Caídas o cortes de otros servicios de importancia institucional por fallos internos como INCI Radio, Biblioteca Virtual. | Se ejecutan los contratos 036 Ing. David Bello (aplicaciones APP biblioteca, INCI Radio, INCI Digital y e- learning), 038 Ing. Pablo Villate (página web INCI).  Se revisa permanente el funcionamiento de servidores, especialmente por restricción movilidad causada en la emergencia sanitaria. Además, por las eventualidades de corte inesperado de energía eléctrica en la zona.  Se reciben y aplican las Políticas, lineamientos y mecanismos de ciber seguridad y prevención de ataques cibernéticos brindados por COLCERT, CSIRT, CCIT, Centro cibernético Policial. |
| EQUIPOS ELECTRÓNICOS Y HARDWARE.  Falla de equipos electrónicos y hardware. | * Ausencia de Políticas claras y definidas en el uso correcto de equipos electrónicos y de Hardware. * Planes de Mantenimiento preventivo y correctivo anuales a la Planta Informática del INCI. * Uso adecuado de la red eléctrica regulada certificada en el 100% del INCI tanto de la sede Administrativa como la Imprenta, que cumpla con normas vigentes para la protección entre otros de equipos electrónicos. | Estas se pueden dar por:   * Cumplimiento de “vida útil” de un equipo de cómputo. * Uso continuo de equipo electrónico * Falta de Mantenimientos Preventivos y Correctivos * Mal uso de la red eléctrica regulada. * Ineficiente cantidad de UPS y calidad de estas. * Mal uso por parte de los responsables de los equipos | Se aplica la Política de seguridad de la información Resolución No.20161010000683 del 16/03/2016.  Se ejecutan los contratos 051/21 All Technological y 056/21 Wbeimar Miranda para el mantenimiento hardware (equipos de cómputo e impresoras)  Se verifica el uso eficiente de la red eléctrica regulada mediante conexión efectiva de los equipos de cómputo y periféricos oficiales asignados a usuarios. |
| UPS (Sistemas de Poder In-interrumpido) y RED ELECTRICA REGULADA. | * Por falta de mantenimiento preventivo y correctivo a la Planta de UPS´s actuales (Baterias, tarjetas) y el sistema de tomas eléctricas de los puestos de trabajo. * Políticas no existentes o poco claras en su uso de la Red Eléctrica Regulada y sus aditivos que la componen. * Inestabilidad de la UPS´s por sobrecarga. * Latencias de energía eléctrica constante en subidas y bajadas en picos de voltaje. * Deficientes conexiones en tomas eléctricas reguladas. | Se puede dar por:   * Deficiencia de UPS´s para mantener estable los servicios de misión crítica por un tiempo razonable en los equipos. * Sistema de UPS poco confiables en su funcionalidad. * Conexiones inadecuadas en tomas eléctricas de puestos de trabajo * Malas conexiones de las UPS * Niveles de carga eléctrica mayores a los soportados por la Red Eléctrica Regulada o las UPS asignadas. * Ausencia de Línea a Tierra (GND) * Calidad del cableado eléctrico ineficiente o poco confiable. | Se verifica el funcionamiento de las UPS´s, se realiza detección cuando se presentan fallas y se intervienen para su solución.    Se cuenta con la línea a tierra (GND) instalada y certificada para el INCI en el edificio Administrativo en el sótano, funcionando adecuadamente.    Se cuenta con la línea a tierra instalada para el INCI en la zona de la Imprenta y funciona adecuadamente.  Se cuenta con la “certificación vigente de la red eléctrica regulada”, que se adapta a los protocolos de tipo de cable, tomacorrientes, marquillaje e identificación para su correcto funcionamiento. |
| TELEFONÍA IP.  Caídas del servicio telefónico IP | Por falta de:   * Soporte o ventanas al servicio de ETB (fibra Óptica y equipos especiales para Conexión **IP** denominada **Trunk** SIP o Enlace Troncal para conectarla con la Red Telefónica) * Mantenimiento a los equipos del servicio. * Soporte de implementación y actualización a la herramienta **Issabel** que es un software de servidor de comunicaciones unificadas que reúne **PBX** IP, entre otras. y sus funcionalidades. | Se puede dar por:   * Caída del Servidor de Telefonia Ip, tanto físicamente como lógicamente. * Fallo en la Fibra Óptica del proveedor ETB o en los equipos Router del operador. * Desconexiones de Red en los teléfonos IP. * Fallos en Red LAN. * Bloqueos al sistema de Telefonía Ip, por factores de Red LAN o caídas de otros servicios como el AD (Directorio Activo) | Se tiene un equipo que actúa como un Servidor de contingencia para este servicio y se hacen pruebas de manera controlada.  Se realizan pruebas y se verifica la funcionalidad de la línea telefónica PBX 3846666, así como el paso de comunicaciones a la red de extensiones autorizadas y asignadas a los servidores públicos.  Se encuentra en perfeccionamiento el proceso contractual para el soporte de Telefonía IP del INCI. |
| RED DE DATOS  Fallos de la Red de Datos por una mala instalación y/o cortos presentados en esta. | Por falta de:   * Ausencia de una política de Red de Datos. * Certificación de la Red de datos institucional. * Maquillaje o identificación de puntos de red. * Organización correcta de puntos de datos en los Centros de Datos principal e Imprenta. * Mantenimiento a los dispositivos de redes como Switch. * Reorganización del cableado de datos * Redistribución de puntos | Se puede dar por:   * Corto en Puntos de Datos. * Congelamiento de la red por daños o malas conexiones en la RED LAN. * Dispositivos Switch en mal estado. * Cables de datos en mal estado. * Deficiente distribución de puntos por pisos. * Passcord o Crossover hechos manualmente o no certificados. * Manipulación inadecuada de los cables. | Se cuenta con certificación vigente de la red de datos de la sede Principal y la Imprenta, que se adapta a los protocolos del tipo de cable CAT 6A o más, puntos de conexión, marquillaje de estos e identificación para su correcto funcionamiento.  Se presentó intervención en la red, producto de modernización locativa, se procedió a revisar el tipo de cable instalado, los puntos ajustados, el marquillaje correcto y su efectivo funcionamiento |
| LIBROS DIGITALES  Perdida de los archivos que contienen los libros digitales | * Ausencia de Políticas claras y definidas en el uso correcto para los Libros Digitales. * Se puede dar por no tener un Sistema de Copias de respaldo efectivo de todos los repositorios de los Libros Digitales del INCI y/o en tenencia por otros medios o convenios existentes. * Tercerear con empresas outsourcing * No actualizar las copias con los últimos libros. * Información errada en las Bases de Datos. | * Perdida de datos por falta de Backup o respaldo de los Libros Existentes. * Caída de servidor o Storage (almacenamiento), donde reposan actualmente los Libros Digitales del INCI. * Daño en disco Duro donde se almacenan los libros digitales. * Daños lógicos en los Repositorios (carpetas) que contienen los Libros Digitales | Se revisa con el proveedor de hosting el repositorio suficiente para incluir los libros, de acuerdo al servicio que brinda IFX Networks, contrato 035/21.  Se ejecuta contrato 036/21 Ing. David Bello para apoyar el mantenimiento de las aplicaciones biblioteca, INCI Radio, INCI Digital y e-learning.  Se continua la verificación con los servidores públicos del Grupo de trabajo Centro Cultural, encargados de la Biblioteca Virtual para Ciegos, del funcionamiento, copias de seguridad o respaldo y acceso a los usuarios inscritos |
| PÁGINA WEB INSTITUCIONAL  Manipulación indebida de los archivos fuentes y bases de datos de la página WEB | * Políticas claras en el uso de la Pagina WEB * Pérdida de Control en el manejo de la página WEB. * Accesos no autorizados * Manipulación de los datos * Se puede dar por no tener un Sistema de Copias de respaldo efectivo | * Falta de Copias de respaldo de la Pagina Web del INCI , sus bases de datos, contenidos. * Garantías sobre las empresas prestadoras del servicio      * No habría control total de los archivos fuentes y las bases de datos | Se continúan realizando las copias de respaldo de acuerdo a las obligaciones del contrato 035/21 con IFX Networks,.  Se ejecuta el contrato 038/21 con el Ing. Pablo Villate para el apoyo y mantenimiento de la página web del INCI.  Se continúan las actividades de la actualización de contenidos web - transparencia por parte de la Of. Planeación- y demás sitios por parte del Proceso de Comunicaciones. |
| INFORMACIÓN INSTITUCIONAL  Sustracción no autorizada de Datos e información institucional | Puede ocurrir por:   * Falta de lineamientos en cuanto a responsabilidades del manejo de la información. * Controles poco eficientes en accesos no autorizados * Exceso de confianza en el manejo de las responsabilidades. | Se puede dar por:  -Personal no autorizado que tiene acceso no autorizado a los sistemas informáticos, equipos de cómputo, servidores, archivos importantes, lo que convierte la Plataforma Tecnológica en algo muy sensible a pérdidas, alteración, daño o robos de información. | Se continua realizando la aplicación y socialización por correo electrónico de lineamientos y mecanismos de ciber seguridad y prevención de ataques cibernéticos recibidos desde los entes oficiales COLCERT, CSIRT, CCIT, Centro cibernético Policial, dirigidos a la reducción de probables ataques informáticos, por hackers.  Se perfeccionó contrato 073/21 con Star Solutions para actualizar el aplicativo antivirus requerido para reducir la probabilidad de ingreso de virus informático (vía correo electrónico, descargas archivos o instalación de USB).  Se continúa el manejo eficiente de herramientas de seguridad perimetral Firewall y Políticas definidas para su uso. Servicio del Directorio Activo con Políticas definidas para su uso. Herramienta Antivirus vigente y con Políticas Definidas. |
| HARDWARE Y SOFTWARE  Daños en equipos y/o el software por el ataque de virus informáticos | Puede ocurrir por:   * Falta de políticas en el uso de Software y Hardware * Ausencia de un programa antivirus en los equipos * Deficiente administración del Antivirus * Actualizaciones no realizadas * Desactivación del antivirus | Propagación de programas o rutinas dañinas que afecten los sistemas informáticos. | Se activó la herramienta antivirus bitdefender, hasta la vigencia 2022 con la empresa Star Solutions contrato No. 073/21, la cual se instaló oportunamente en todos los equipos de cómputo del instituto y con Políticas definidas para su uso.  Se encuentra vigente la Política de seguridad de la información Resolución No.20161010000683 del 16/03/2016 y se informa de su aplicación, particularmente con la actual forma de trabajo en casa, para el uso de equipos de cómputo institucionales asignados, conexión remota con el correo electrónico, el aplicativo Orfeo, WEBSAFI entre otros. |
| SEGURIDAD PARA EL INGRESO, MANEJO Y DISPOSICIÓN DE INFORMACIÓN EN EQUIPOS ASIGNADOS  Fallas del manejo de claves de acceso y manejo de equipos | * Comprensión de las Políticas de seguridad Informática institucional. * Malversación o pérdida de información institucional causada por préstamo de las claves de acceso. * Dificultad para consultar, manejar y disponer de la información por perdida de las claves de acceso. * Retrasos en la gestión institucional por los reprocesos de reasignación y definición de nuevas claves de acceso para disponer de la información | Se puede dar por:   * Ausencias temporales de los servidores (vacaciones, licencias, enfermedad, accidente, encargos de puestos de trabajo, retiro temporal por sanción disciplinaria). * Ausencias definitivas de los servidores (finalización de la vinculación laboral, renuncias, abandono del cargo, traslado definitivo de puesto) * Deficiencias en el manejo de las claves de acceso por olvido, manipulación o intentos fallidos. | Se realiza de forma presencial o remota, a través del Directorio Activo (AD), la asignación de usuarios y claves de ingreso a la red institucional en los equipos de cómputo asignado, existen Políticas definidas, administradores, grupos especiales de ingreso a Internet, sistemas de DHCP con rangos definidos, agentes FSSO, igualmente en ocasiones de desactivación por intentos fallidos, vencimiento, necesidad de ingreso de otros servidores debidamente autorizados (por desvinculación, licencias, permisos del titular y necesidad de consulta de información importante o urgente.  Se cuenta con dos (2) servidores con Máquinas Virtuales (MV) de AD replicadas, uno respalda al otro en caso de fallo y a diario se están revisando en su funcionamiento, actualizaciones y otras que se requieran para tenerlos funcionales institucionalmente.  Se continúa realizando copia de seguridad de estas dos máquinas virtuales cada mes.  Se ejecuta contrato 058/21 soporte del Directorio Activo con MCE Net Solutions. |
| INFRAESTRUCTURA INFORMATICA  Sabotaje / vandalismo | Deficiencias en el control de ingreso no autorizados a los Centros de Datos y/o equipos de red, ubicados en diferentes sitios a este y que carecen de seguridad, lo que pueden ser manipulables por cualquiera. | El Centro de Datos se encuentra dispuesto en dos (2) espacios físicos diferentes en la entidad, cada uno con herramientas y servicios definidos, en razón a esto, se dificulta controlar el acceso de personas no autorizadas que puedan alterar el normal funcionamiento de los sistemas informáticos del INCI, incluyendo aquellos que se encuentran en espacios físicos que son transitados por cualquier persona o funcionario diferentes a los ingenieros o técnicos de la OAP. | Se controla el ingreso a los centros de datos solo a los Ingenieros de Sistemas, adscritos a la Oficina Asesora de Planeación y vinculados a la planta de empleos del INCI. Si es necesario que contratistas o personas diferentes requieran ingresar siempre se efectúa con el acompañamiento de los Ingenieros autorizados. |
| INFRAESTRUCTURA INFORMATICA  Desastres naturales / Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática. | - El Inci, no está exento de que se pueden presentar cortos en las tomas eléctricas, por ende recalentamiento en equipos, y/o hechos más graves como conflagraciones que afecten los equipos y redes informáticos.  -Los equipos de cómputo, la red eléctrica regulada, la red LAN (canaletas) puede sufrir daños, causados por inundaciones al presentarse rupturas en la tubería del agua o casos por malas e inadecuadas instalaciones por personal idoneo.  - La presencia de los movimientos telúricos es alta e impredecible, lo que provocaría que en el INCI se presente catástrofe en la infraestructura física, de acuerdo a estudio realizado por la Universidad Nacional donde la edificación principal no cumple con normas de sismo resistencia, afectando por ende la infraestructura informática. | Incendios, inundaciones, movimientos telúricos que afecten la infraestructura informática provocando daños en la misma (perdida de información, daños  en equipos que generen parálisis en la gestión institucional) | Se cuenta con el sistema de seguridad interna liderado por el Grupo de Gestión Humana y de la Información, quienes están encargados del SGSST, y llevan a cabo jornadas de prevención a desastres.  Se continúa aplicación de la Política de seguridad de la información Resolución No. 20161010000683 del 16/03/2016.  Se realizan copias de seguridad de los servidores donde se aloja la información institucional en repositorios en la nube, para enfrentar posibles pérdidas de información |
| EQUIPOS DE SEGURIDAD PERIMETRAL FIREWALL | * Comprensión de Políticas claras de seguridad. * Vencimiento de la licencia. * Copias no existentes. * Daños por falta de mantenimiento oportuno. * Ausencia de un programa antivirus especial para estos equipos * Deficiente administración * Actualizaciones no realizadas * Ingresos no autorizados | Bloqueos en el servicio de Internet.  Entradas bloqueadas por VPN para empresas de servicios como WEBSAFI, ORFEO, redes y otras herramientas de importancia.  Daño por ingresos de personal no autorizado.  Copias de seguridad no actualizadas | Se cuenta con: políticas definidas y objetos para estos, licencias anuales especialmente para los Firewall Fortinet Fortigate 100D, copias mensuales de estos en su configuración en caso de daño.  Se cuenta con dos (2) firewall licenciados, uno MASTER y otro ESCLAVO, en alta disponibilidad y redundancia.  Diariamente se ingresa a estos para revisar su estado y actividad de funcionamiento.  Se continua con el diagnostico de cada máquina Firewall acerca de su actividad y se hacen pruebas de desconexión en puertos especiales, se toma las medidas de tiempo en recuperar los servicios en caso de fallo en alguno de los dos.  Se ejecuta con la empresa Core IP el contrato No. 054/21 del Licenciamiento, activación y puesta en marcha para los Firewall por un año hasta el 2022.  Se ejecuta con la empresa MCE Solutions el contrato No. 055/21, de Soporte Firewall de dispositivos de seguridad perimetral. |
| SERVIDOR VMware y Máquinas Virtuales. | * Por falta de mantenimiento preventivo y correctivo a la Plataforma VMware y sus Máquinas Virtuales. * Políticas no existentes o poco claras en su uso. * Inestabilidad por falta de actualizaciones. * Licencias no actualizadas y vigentes tanto en Servidor VMware como Máquinas Virtuales. * Ingreso de personal no autorizado para el manejo de esta Plataforma. | Bloqueos de servicios existentes en las Máquinas virtuales.  Daños por ingresos no autorizados.  Sistema VMware y operativos Server sin soporte técnico. | Se continúa mensualmente realizando copias de las Máquinas Virtuales, se elabora formato de soporte.  Se continúa a diario realizando revisión por el VMware para verificar el estado de las máquinas virtuales.  Se ejecuta el contrato No. 060/21 Insertel SAS, para el mantenimiento de la Plataforma VMware y Máquinas Virtuales (MV). |