**PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

# Justificación

Con el desarrollo naciente de nuevas tecnologías y herramientas tecnológicas en un mercado cada vez más competitivo año a año, nos ha permitido la automatización de muchos procesos tal que agiliza y mejora los servicios convirtiendo estas herramientas en una característica transcendental para sostener la continuidad del negocio en los mejores niveles de disponibilidad, confiabilidad, rendimiento y funcionalidad.

Los procedimientos, manuales y otros documentos que actualmente son parte del proceso de I&T del INCI, si bien mitigan en buena parte un caso de riesgo, es necesario identificar otras soluciones válidas en la atención de un riesgo a la planta Informática institucional.

En caso de presentarse un desastre informático en la interrupción de cualquiera de los servicios informáticos en uno o varios de sus componentes ya sea de tipo eléctrico (red eléctrica regulada o no regulada), hardware (servidores, Firewall, equipos CORE, de Borde o piso, PC, portátiles entre otros), software, aplicativos o herramientas (S.O, bases de Datos, Orfeo, Web SAFI, VMWare, Antivirus, Pagina INCI, INCI Radio, Biblioteca Virtual), comunicaciones o servicios (conectividad servicio Internet, hosting), entre otros; conllevaría a impactos negativos de alta significancia, factores que ocasionarían posibles pérdidas por el cese de actividades misionales y de apoyo, esto es en la continuidad del negocio.

Teniendo una identificación de Riesgos para la Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno Digital, esto permitirá cubrir costos innecesarios en materiales de los activos de la entidad en caso de una calamidad, y servirán para recuperar el negocio en lo más preciado que es su información, evitando su pérdida.

# Objetivo General

* Identificar las situaciones de riesgo que pueden afectar la infraestructura informática, las acciones que minimizan la materialización de dichos imprevistos y poder responder por la continuidad de operación de la plataforma tecnológica Institucional.

# Objetivos Específicos

* Valorar las posibles situaciones que generan los riesgos
* Identificar las acciones que actualmente mitigan la presencia de los riesgos valorados
* Definir la continuidad o nuevas acciones para retomar el curso normal de operación en caso de presentarse los riesgos valorados.
* Brindar respuesta rápida y oportuna para dar continuidad a las operaciones que componen la infraestructura tecnológica.
* Procurar que la restauración de los servicios informáticos y tecnológicos sean o presenten un impacto mínimo de costo / pérdida para la entidad, esperando un beneficio alto para el INCI.

# Identificación, valoración y control de Riesgos

De acuerdo a lo planteado en la Guía de Administración de Riesgos y Diseño de Controles en Entidades Públicas, versión 6 de del 2021 por la Función Pública, los lineamientos para riesgos de seguridad de la información son

1. Identificación de los activos de seguridad de la información: o es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:

-Aplicaciones de la organización

-Servicios web

-Redes

-Información física o digital

-Tecnologías de información TI

-Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital

1. Identificación del riesgo: se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

 Pérdida de la confidencialidad

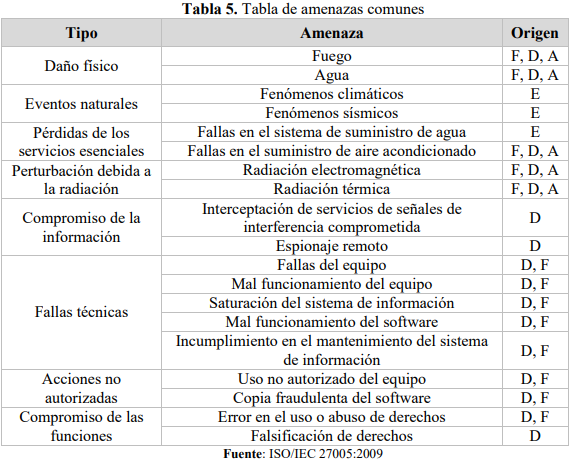
 Pérdida de la integridad

 Pérdida de la disponibilidad

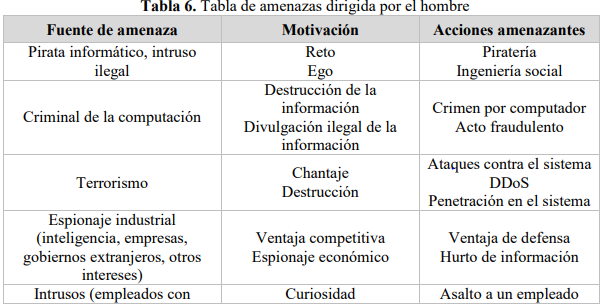
## Identificación de Amenazas

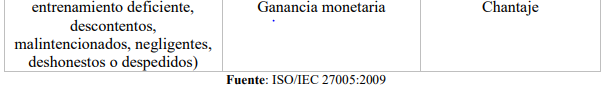
De acuerdo al documento de MinTIC Anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos:

* Deliberadas (D), Fortuito (F) o Ambientales (A).



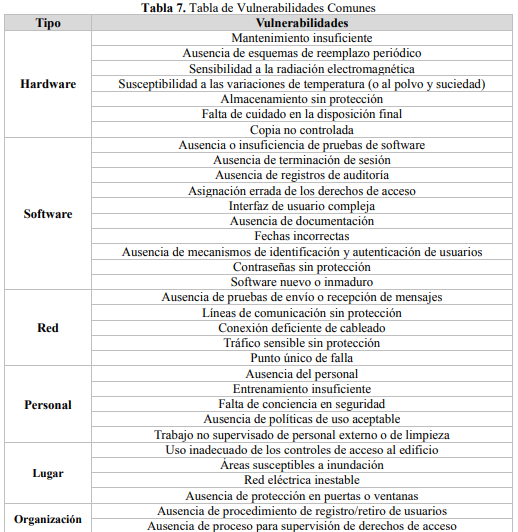
* Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros

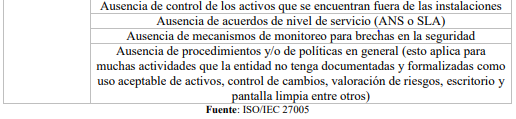




## Identificación de Vulnerabilidades

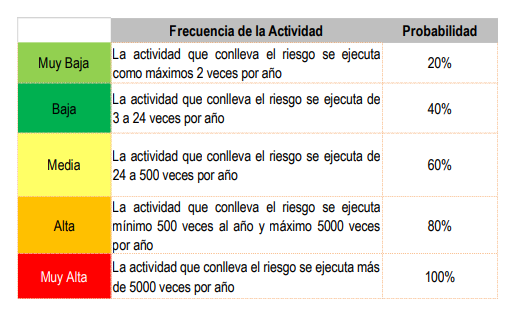
Se puede identificar vulnerabilidades (debilidades) en las siguientes áreas:



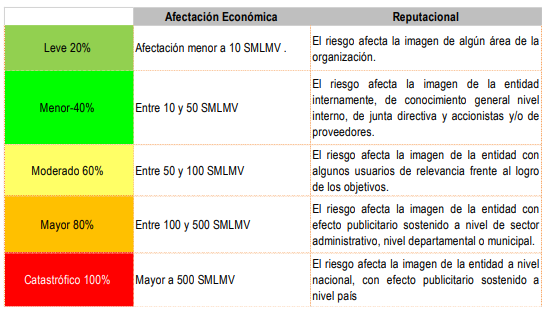


1. Valoración del riesgo: Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía. En este sentido, se debe considerar para este análisis las siguientes tablas:

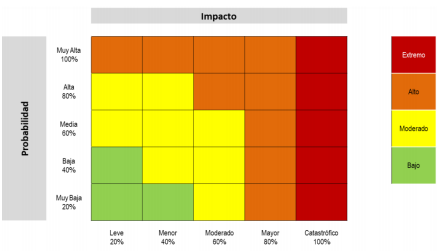
## Probabilidad



## Impacto



## Matriz de Calor (Riesgo inherente)



1. **Controles asociados a la seguridad de la información:** Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos, dicha información está compuesta por 114 controles de seguridad agrupados en 14 secciones:

A.5: Políticas de Seguridad de la Información: hace referencia a los controles sobre cómo escribir y revisar políticas de seguridad.

A.6: Organización de la Seguridad de la información: los controles se encargan de establecer responsables. Al mismo tiempo también se centra en dispositivos móviles y situaciones como la de teletrabajo.

A.7: Seguridad de los Recursos Humanos: controles para las situaciones previas y posteriores referentes a la contratación y finalización de contrato de personal.

A.8: Gestión de Recursos: establecidos para realizar inventario, clasificación de información y manejo de los medios de almacenamiento.

A.9: Control de Acceso: control del acceso tanto a la información como a aplicaciones u otro medio que contenga información.

A.10: Criptografía: controles para gestionar encriptación de información.

A.11: Seguridad física y ambiental: controles para garantizar factores externos, seguridad de equipo y medios que puedan comprometer la seguridad.

A.12: Seguridad Operacional: controles relacionados con gestión de la protección de malware o vulnerabilidades.

A.13: Seguridad de las comunicaciones: Control sobre la seguridad de las redes, transmisión de información, mensajería…

A.14: Adquisición, desarrollo y mantenimiento de Sistemas: controles que establecen los requisitos de seguridad en desarrollo y soporte.

A.15: Relaciones con los proveedores: incluye lo necesario a la hora de realizar contratos y seguimiento a proveedores.

A.16: Gestión de Incidentes en Seguridad de la Información: sirven para reportar eventos las debilidades, así como procedimientos de respuesta.

A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio: referidos a la planificación de continuidad de negocio.

A.18: Cumplimiento: control relacionado a la hora de identificar regulaciones relacionadas con seguridad de la información y hacer que se cumplan.

# 1. IDENTIFICACIÓN DE ACTIVOS INCI

Para el caso que aplica al INCI, se identifican el Hardware, Software y Equipos de Comunicaciones.

| **TIPO DE ACTIVO** |
| --- |
| SERVICIO DE INTERNET, SERVIDORES, SWITCH CORE Y DE BORDE, ROUTER, REDES LAN, Wi-Fi. |
| EQUIPOS SERVIDORES INSTITUCIONALES |
| EQUIPOS ELECTRÓNICOS Y HARDWARE. |
| UPS (Sistemas de Poder In-interrumpido) y RED ELECTRICA REGULADA. |
| TELEFONÍA IP |
| RED DE DATOS |
| LIBROS DIGITALES |
| PÁGINA WEB INSTITUCIONAL |
| INFORMACIÓN INSTITUCIONAL |
| HARDWARE Y SOFTWARE |
| SEGURIDAD PARA EL INGRESO, MANEJO Y DISPOSICIÓN DE INFORMACIÓN EN EQUIPOS ASIGNADOS |
| INFRAESTRUCTURA INFORMATICA |
| EQUIPOS DE SEGURIDAD PERIMETRAL FIREWALL |
|  |

# 2. VULNERABILIDADES Y AMENAZAS INCI

| **VULNERABILIDADES** | **AMENAZAS** |
| --- | --- |
| 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. |
| * Falta de mantenimiento preventivo y correctivo a los Sistemas de : * Equipos Servidores * Sistema eléctrico regulado – UPS * Red LAN. * Servidores que componen la Planta Informática. * Desconocimiento de los Ingenieros * Por des configuración en equipos. * Ausencia de un sistema de Back up o copias de respaldo. * Falta tercerizar algunos servicios en la NUBE * Soportes poco idóneos. * Ausencia de Políticas de Seguridad Informática para los Servidores. * Desarrollos inadecuados de aplicativos o implementaciones mal realizadas. * Falta de documentación técnica. | Daños físicos o lógicos en los servidores institucionales.   * Caída de la red LAN * Fallo en el Fluido eléctrico regulado por UPS´s * Propagación de virus o programas basura como SPAM * 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. * Caidas de otros servicios de importancia institucional por fallos internos como Inci RADIO, Biblioteca Virtual. |
| * 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. | * 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 |
| * Por falta de mantenimiento preventivo y correctivo a la Planta de UPS´s actuales 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. | * 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. |
| * 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 vigente que es un software de servidor de comunicaciones unificadas que reúne PBX IP, entre otras. y sus funcionalidades. | * Caída del Servidor 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) |
| * Ausencia de una política de Red de Datos. * Falta de Certificación de la Red de datos institucional. * Deficiente Maquillaje o identificación de puntos de red. * Deficiente Organización de puntos de datos en los Centros de Datos principal e Imprenta. * Deficiente Mantenimiento a los dispositivos de redes como Switch. * Deficiente Reorganización del cableado de datos * Deficiente Redistribución de puntos | * Corto en Puntos de Datos. * Congelamiento de la red por daños o malas conexiones en esta. * 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. |
| * Deficiente Sistema de Copias de respaldo 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 | * 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. |
| * 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 | * Falta de Copias de respaldo de la Pagina Web del INCI y 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 |
| * 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. |
| * Falta de políticas en el uso de Software * 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. |
| * 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 | * 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. |
| 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 espacios físicos diferentes en la entidad, en razón a esto, se dificulta controlar el acceso de personas que puedan alterar el normal funcionamiento de los sistemas informáticos, incluyendo aquellos que se encuentran en espacios físicos que son transitados por cualquier persona o funcionario diferentes a los ingenieros o técnicos de la Oficina Asesora Planeación. |
| Presencia de cortos en las tomas eléctricas, por ende recalentamiento en equipos, 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.  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) |
| * 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 |
| * 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. |

# 3. VALORACION DEL RIESGO INCI

| **RIESGO** | **ACTIVO** | **AMENAZAS** | **TIPO** | **PROBABILIDAD** | **IMPACTO** | **RIESGO RESIDUAL** | **OPCION TRATAMIENTO** | **CONTROL** | **SOPORTE** | **RESPONSABLE** | **TIEMPO** | **INDICADOR** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ataques a la plataforma informática | SERVICIO DE INTERNET, SERVIDORES, SWITCH CORE Y DE BORDE, ROUTER, REDES LAN, Wi-Fi. | Accesos no autorizados por parte de “delincuentes informáticos” u otros con pretensiones de causar daños potenciales a la Red informática y a los datos allí contenidos, mediante ataques a los sistemas que componen la Plataforma Informática. | * 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 | MUY BAJA | MENOR | BAJO | REDUCIR | Política De Seguridad definida,  Servicio de conectividad activo  Servicio Manteni-  Miento equipos seguridad perimetral | Política De Seguridad vigente  Contratos de servicios conectividad y Manteni\*  Miento equipos seguridad perimetral | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Pérdida de información en los Servidores | EQUIPOS SERVIDORES INSTITUCIONALES | Daños físicos o lógicos en los servidores institucionales.   * Caída de la red LAN * Fallo en el Fluido eléctrico regulado por UPS * Propagación de virus o programas basura como SPAM * 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. * Caídas de otros servicios de importancia institucional por fallos internos como INCI Radio, Biblioteca Virtual. | * Falta de mantenimiento preventivo y correctivo a los Sistemas de : * Equipos Servidores * Sistema eléctrico regulado – UPS * Red LAN. * Servidores que componen la Planta Informática. * Desconocimiento de los Ingenieros * Desconfiguración en equipos. * Ausencia de un sistema de Back up o copias de respaldo. * Falta tercerizar algunos servicios en la NUBE * Soportes poco idóneos. * Ausencia de Políticas de Seguridad Informática para los Servidores. * Desarrollos inadecuados de aplicativos o implementaciones mal realizadas. * Falta de documentación técnica. | MEDIA | MODERADO | MOD3ERADO | REDUCIR | Servicio de apoyo en Manteni-  Miento Pag Web, aplicaciones institucionales  documental,  Incidentes en cortes de servicios | Contratos de servicios apoyo.  Registro de incidentes | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Fallas funcionamiento de equipos electrónicos y hardware. | EQUIPOS ELECTRÓNICOS Y HARDWARE. | * 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 | * 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. | MEDIA | MODERADO | MOD3ERADO | REDUCIR | Política De Seguridad definida,  Servicio de  Manteni-  Miento equipos  Incidentes cortes energía regulada | Política De Seguridad vigente  Contratos de servicios Manteni\*  Miento equipos  Reporte Incidentes | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Falla funcionamiento UPS y Red Eléctrica Regulada | UPS (Sistemas de Poder In-interrumpido) y RED ELECTRICA REGULADA. | * 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. | * Por falta de mantenimiento preventivo y correctivo a la Planta de UPS´s actuales 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. | BAJO | MAYOR | ALTO | REDICIR | Servicios de manteni-  Miento UPS  Línea a tierra (GND) en servicio  Certificación red regulada definida | Contrato Manteni-  Miento equipos  Línea a tierra funcionando  Certificación Vigente | I&T | Primer Cuatrimestre | * No. Actividades ejecutadas / No. Actividades programadas |
| Falla del servicio telefónico | TELEFONÍA IP. | Se puede dar por:   * Caída del Servidor 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) | 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. | MEDIA | MODERADO | MODERADO | REDUCIR | Servicio manteni-  Miento equipo telefonía  Incidentes servicio telefónico | Contrato Manteni-  Miento telefonía  Registro incidentes | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Fallos de la Red de Datos por una mala instalación y/o cortos presentados en esta | RED DE DATOS  . | Se puede dar por:   * Corto en Puntos de Datos. * Congelamiento de la red por daños o malas conexiones en esta. * 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. | 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 | MEDIA | MAYOR | ALTO | REDUCIR | Certificación red regulada definida  Red LAN en servicio | Certificación vigente  Red LAN funcionando | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Perdida de los archivos que contienen los libros digitales | LIBROS DIGITALES | * 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 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 | MEDIA | * MAYOR | * ALTO | * REDUCUR | Servicio de repositorio y copias de seguridad  Servicio manteni-  Miento aplicativos institución | Contratos repositorio y copias de seguridad  Contrato manteni-  Miento aplicativos institución | * I&T | * Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Indebida manipulación de los archivos fuentes y bases de datos de la página WEB | PÁGINA WEB INSTITUCIONAL | * Falta de Copias de respaldo de la Pagina Web del INCI y 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 | * 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 | MEDIA | * MAYOR | * ALTO | * REDUCIR | Servicio de hosting  Servicio de manteni-  miento pag web | Contratos servicio hosting y de  manteni-  miento pag web | * I&T | * Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Sustracción no autorizada de Datos e información institucional | INFORMACIÓN INSTITUCIONAL | -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. | * 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. | BAJO | MODERADO | MODERADO | REDUCIR | Servicio de manteni-  miento y soporte equipos seguridad  Mecanismos de ciberseguridad | Contrato manteni-  miento  firewall  Mensajes centros ciberneticos | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Daños en equipos y/o el software por el ataque de virus informáticos | HARDWARE Y SOFTWARE | Propagación de programas o rutinas dañinas que afecten los sistemas informáticos. | * Falta de políticas en el uso de Software * Ausencia de un programa antivirus en los equipos * Deficiente administración del Antivirus * Actualizaciones no realizadas * Desactivación del antivirus | BAJO | MENOR | MODERADO | REDUCIR | Servicio de antivirus  Política de seguridad de la información definida | Contrato antivirus  Política de seguridad de la información vigente | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Fallas del manejo de claves de acceso y manejo de equipos | SEGURIDAD PARA EL INGRESO, MANEJO Y DISPOSICIÓN DE INFORMACIÓN EN EQUIPOS ASIGNADOS | * 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. | * 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 | * BAJO | * MAYOR | * ALTO | REDUCIR | Servicio Manteni-  miento  Directorio activo  Servicio copias seguridad máquinas virtuales | Contrato manteni-  miento  Directorio activo  Formato copias seguridad máquinas virtuales | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Sabotaje o vandalismo a la infraestructura informática | INFRAESTRUCTURA INFORMATICA | El Centro de Datos se encuentra dispuesto en dos espacios físicos diferentes en la entidad, en razón a esto, se dificulta controlar el acceso de personas que puedan alterar el normal funcionamiento de los sistemas informáticos, 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. | 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. | * BAJO | * MAYOR | * ALTO | REDUCIR | Centro datos seguridad ingreso | Centro de datos con claves de acceso | I&T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |
| Desastres naturales / Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática | INFRAESTRUCTURA INFORMATICA  . | 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) | El INCI, no está exento de que se pueden presentar cortos en las tomas eléctricas, por ende recalentamiento en equipos, 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.  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 | MEDIA | MAYOR | ALTO | REDUCIR | Copias de seguridad máquinas virtuales  Planes de riesgos y desastres | Formato copias de seguridad  Plan SGSST | I6T | Primer Cuatrimestre | No. Actividades ejecutadas / No. Actividades programadas |