**SEGURIDAD Y PRIVACIDAD DE LA INFORMACION**

**Gestión de Riesgos - INCI**

***Antecedentes***

El INCI ha venido adelantando continuamente la **MODERNIZACION y RENOVACION** de su plataforma tecnológica en todos los casos y durante años, mejorando de manera eficaz, eficiente y efectiva los procesos de la Entidad y como estrategia de apoyo al continuo desarrollo e implementación a su sistema Informático y de información en cumplimiento de su misión institucional.

En razón a lo anterior, se debe reducir al máximo los riesgos y siniestros informáticos que se presenten en el INCI, como también reducir la posibilidad de ocurrencia.

En los últimos años, el INCI ha registrado incidentes informáticos, que si bien se ha mejorado las herramientas informáticas, hay casos fortuitos como la suspensión del fluido eléctrico de la red no regulada, saturación de servidores y/o fallos en estos, fallos en el sistema de correo electrónico, perdida de las bases de estos en cualquiera de las aplicaciones existentes, daños en partes electrónicas y/o de hardware, equipos de comunicaciones, defectos en desarrollos y/o aplicativos , e instalaciones de aplicativos que han quedado fuera de servicio (falta del código), garantías u obsolescencia en la Plataforma Informática y daños en servidores , entre otros.

Teniendo en cuenta que el instituto Nacional para Ciegos “INCI” es una entidad de orden Nacional, donde se adoptara el Modelo de Seguridad y Privacidad de la información en el marco de la Estrategia de Gobierno en Línea, haciendo necesario poner en marcha un Plan de Seguridad de la Información donde se deben “identificar” aquellos riesgos, que colocan inestable los Servicios Tecnológicos institucionales y la continuidad de estos, se debe orientar los pasos a seguir en caso de presentarse un incidente de estos, que permitirá recuperar la funcionalidad de la plataforma tecnológica, garantizando la continuidad de las operaciones de la Entidad en el cumplimiento misional.

***Objetivo General***

* Gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad)
* Vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información
* 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.

***Justificación***

Con el desarrollo naciente de nuevas tecnologías y herramientas tecnológicas en un mercado cada vez más competitivo año a año, lo que nos ha hecho más dependientes de estas en la calidad, servicios, manejo y la continuidad del negocio, convirtiendo estas herramientas en una forma transcendental de **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 parte un caso de riesgo, estos sólo son de aplicabilidad momentánea y no atienden de forma específica una solución válida 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…), 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; conllevando a un impacto financiero, detrimento a la imagen institucional y otros factores que ocasionarían posibles pérdidas, dando en el cese de actividades misionales, 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 en Línea**, 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 la pérdida de esta.

***Identificación de Riesgos***

De acuerdo a lo planteado en la guía, la identificación del riesgo se hace con base en causas identificadas para los procesos, dichas causas pueden ser internas o externas, según lo que haya identificado la Entidad a través del Contexto estratégico.

En este momento es importante establecer cuáles son los activos críticos para asociarlos a los procesos correspondientes y de allí generar el listado de procesos críticos. Inventariar los activos de información sensible, revisar los procesos según la clasificación del MECI y del modelo de gestión, con éste punto se revisa la pertinencia del alcance planteado para el MSPI.

En esta etapa es especialmente importante la participación del personal designado para la implementación del MSPI, dentro de la mesa interdisciplinaria en la cual se revisan los procesos, tomando parte en la identificación de los riesgos de seguridad, para los procesos identificados como críticos dentro del planteamiento del MSPI.

Para este capítulo, la guía inicia con la definición de algunos términos que son necesarios dentro del empleo de ésta metodología, estos términos son comúnmente empleados en las Entidades ara efectos de la aplicación del sistema de Calidad o el MECI, y se listarán a continuación:

 Proceso.

 Objetivo del Proceso.

 Identificación de Activos.

 Riesgo.

 Causas (Amenazas y Vulnerabilidades).

 Descripción del Riesgo.

 Efectos de la materialización del Riesgo.

Como acto seguido se debe realizar la clasificación de los riesgos, Para nuestro caso institucional se hará la identificación de “**Riesgos de Tecnología**”, teniendo en cuenta los pilares de la seguridad de la información:

 Disponibilidad

 Confidencialidad

 Integridad

**ANÁLISIS DE RIESGOS**

A continuación se presentan una serie de etapas propuestas para la Generación del análisis de riesgos de las Entidades, basadas la norma ISO27005 (La norma ISO 27005 contiene **diferentes recomendaciones y directrices** generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información).

* **IDENTIFICACIÓN DEL RIESGO**

El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

* **IDENTIFICACIÓN DE LOS ACTIVOS**

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. ***Para realizar esta identificación es necesario revisar la guía de gestión de activos adjunta al MSPI*.**

**- IDENTIFICACIÓN DE LAS AMENAZAS**

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas)

Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

A continuación se describen una serie de amenazas comunes.

D= Deliberadas

A= Accidentales

E= Ambientales

***Para los riesgos tecnológicos que se identificaran, se tendrá en cuenta las posibles amenazas comunes y las amenazas humanas que apliquen al INCI.***

**Fuentes de amenazas comunes**

|  |  |  |
| --- | --- | --- |
| TIPO | AMENAZA | ORIGEN |
| PERDIDA DE LOS SERVICIOS ESENCIALES | Fallas en el sistema de suministro de aire acondicionado | DA |
| Perdida de suministro de energía | A |
| Falla en equipo de telecomunicaciones | DA |
| Compromiso de la información | Hurto de equipo | A |
| Manipulación con hardware | A |
| Manipulación con software | A |
| Fallas técnicas | Fallas del equipo | AE |
| Mal funcionamiento del equipo | A |
| Saturación del sistema de información | A |
| Mal funcionamiento del software | A |
| Incumplimiento en el mantenimiento del sistema de información | DA |
| Fallos en servicios Internet, Hosting…) | A |
| Acciones no autorizadas | Uso no autorizado del equipo | DA |
| Uso de software falso o copiado | DA |
| Corrupción de los datos | DA |
| Procesamiento ilegal de datos | DA |
| Copia fraudulenta del software | DA |

**Fuentes de amenazas humanas**

|  |  |  |
| --- | --- | --- |
| **FUENTE DE AMENAZA** | **MOTIVACION** | **ACCIONES AMENAZANTES** |
| Pirata informático, intruso ilegal | Reto  Ego  Rebelión  Estatus  Dinero | • Piratería  • Ingeniería Social  • Intrusión, accesos forzados al sistema  • Acceso no autorizado |
| Criminal de la computación | Destrucción de la información  Divulgación ilegal de la información  Ganancia monetaria  Alteración no autorizada de los datos | • Crimen por computador  • Acto fraudulento  • Soborno de la información  • Suplantación de identidad  • Intrusión en el sistema |
| Terrorismo | Chantaje  Destrucción  Explotación | • Penetración en el sistema  • Manipulación en el sistema |
| Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos) | Curiosidad  Ego  Inteligencia  Ganancia monetaria  Venganza  Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación ) | Asalto a un empleado  Chantaje  Observar información reservada  Uso inadecuado del computador  Fraude y hurto  Soborno de información  Ingreso de datos falsos o corruptos  Interceptación  Código malicioso  Venta de información personal  Errores en el sistema  Intrusión al sistema  Sabotaje del sistema  Acceso no autorizado al sistema. |

**IDENTIFICACIÓN DE CONTROLES EXISTENTES**

Algunos controles que se tienen, para evitar riesgos o amenazas a la PLATAFORMA TECNOLOGICA del INCI son:

* Resolución No.20161010000683 del 16-03-2016 documento POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
* Socialización de la POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.
* Auditorías internas, para control y cumplimiento de licenciamiento institucional, uso del Internet , en cumplimiento de la Política de seguridad y privacidad de la información.
* Herramientas de control de software en los equipos.
* Presentación de informe anual de DERECHOS DE AUTOR de licenciamiento institucional.

**IDENTIFICACIÓN DE LAS VULNERABILIDADES**

Para el caso que nos aplica al INCI, se identificara vulnerabilidades en el área “Hardware, software y equipos de comunicaciones”.

**NOTA:** La sola presencia de una vulnerabilidad no causa daños por sí misma, dado que es necesario que exista una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

*Vulnerabilidades identificadas en el proceso de Informática & Tecnología y métodos para la valoración de la misma.*

| **TIPO DE ACTIVO** | **VULNERABILIDADES** | **AMENAZAS** |
| --- | --- | --- |
| SERVICIO DE INTERNET, SERVIDORES, SWITCH CORE Y DE BORDE, 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. |
| 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 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. |
| 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 |
| UPS (Sistemas de Poder In-interrumpido) y RED ELECTRICA REGULADA. | * 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. | 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. |
| 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 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) |
| 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 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. |
| LIBROS DIGITALES  Perdida de los archivos 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 | * 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 |
| 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 | * 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 |
| 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. |
| 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 * 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. |
| 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. |
| 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 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. |
| 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, 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) |

**Pasos para análisis del Riesgo**

Impacto:

* + Activo (¿qué se trata de proteger?)
  + Amenaza (¿que se teme que suceda?)

Probabilidad:

* + Vulnerabilidad (¿cómo se puede ocurrir la amenaza?)
  + Mitigación (¿cómo se reduce actualmente el riesgo?)

**Siguiendo el “Estándar AS/NZS 4360 de Análisis de Riesgos de la Metodología del Ministerio de Comunicaciones (Gobierno Digital - MINTIC)**

1. Establecer el contexto : Administración de riesgos
2. Identificar Riesgos: Los expuestos en este documento son de Tipo Tecnológico.
3. Analizar Riesgos
   * Aplicar las medidas cualitativas de Impacto
   * Aplicar las medidas cualitativas de probabilidad

4. Evaluar Riesgos:

* + Comparar contra criterios
  + Establecer prioridades de riesgo
  + Tratar Riesgos : Aplicar los pasos dados en el estándar AS/NZS 4360

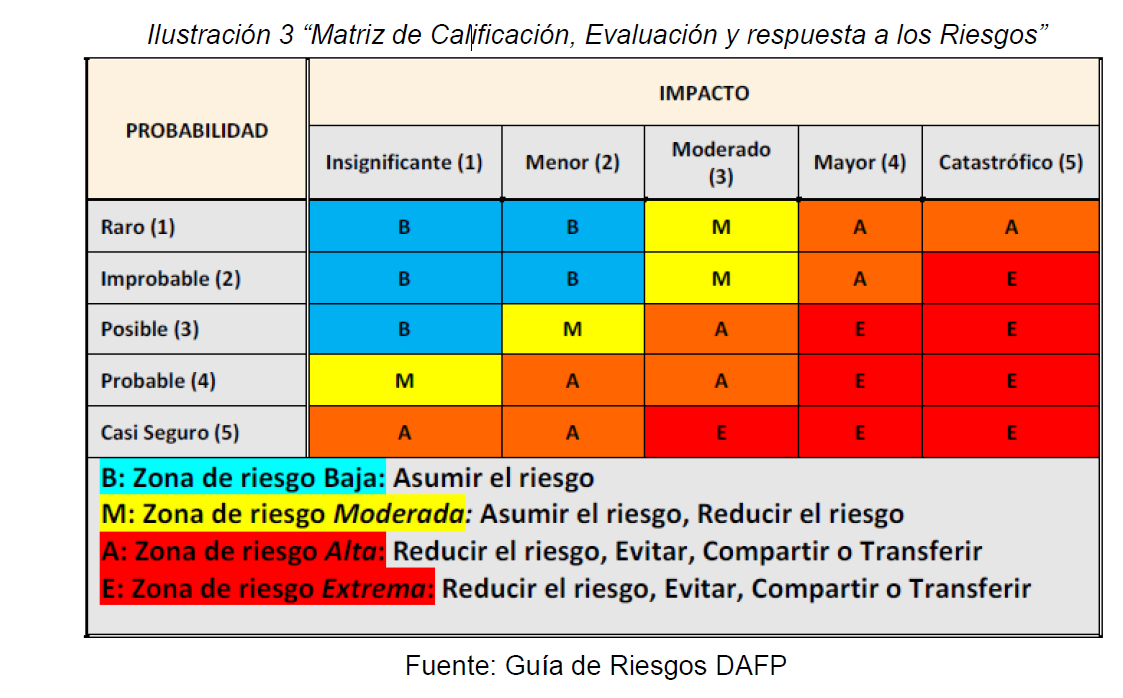
1. Matriz de Análisis de Riesgo Cualitativo
2. Aplicación de la Matriz de Análisis de Riesgo Cualitativo

**Identificación y Análisis de Riesgos Informáticos**

| **TIPO DE ACTIVO** | **PROBABILIDAD / VULNERABILIDADES** | **IMPACTO / AMENAZAS** |
| --- | --- | --- |
| SERVICIO DE INTERNET, SERVIDORES, SWITCH CORE Y DE BORDE, 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. |
| 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 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. |
| 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 |
| UPS (Sistemas de Poder In-interrumpido) y RED ELECTRICA REGULADA. | * 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. | 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. |
| 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 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) |
| 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 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. |
| LIBROS DIGITALES  Perdida de los archivos 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 | * 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 |
| 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 | * 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 |
| 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. |
| 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 * 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. |
| 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. |
| 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 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. |
| 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, 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) |

**EVALUACIÓN DE RIESGO**

Esta se hace de manera cualitativa generando una comparación en la cual se Presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada “Matriz de Calificación, Evaluación y respuesta a los Riesgos”, con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:



Teniendo en cuenta los pasos mencionados anteriormente, y las herramientas entregadas por la guía, se presenta a continuación el análisis de uno de los riesgos de Seguridad de la Información identificados anteriormente:

**Matriz de análisis de riesgo cualitativo**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Probabilidad** | **Impacto** | | | | |
| Insignificante  1 | Menores  2 | Moderados  3 | Mayores  4 | Catastróficas  5 |
| A (casi certeza) | A | A | E | E | E |
| B (probable) | M | A | A | E | E |
| C (moderado) | B | M | A | E | E |
| D ( improbable) | B | B | M | A | E |
| E (raro) | B | B | M | A | A |

**B:** Bajo **M:** Moderado **A:** Alto **E:** Extremo

**Aplicación Matriz y calificación de los riesgos**

| **Riesgo** | **Probabilidad** | **Impacto** | **Calificación** |
| --- | --- | --- | --- |
| **Servicio de Internet, Servidores, Switch, Router, redes LAN , Wi-Fi.**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia BAJA | D | 2 | **B** |
| **Pérdida de información en los Servidores**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia MODERADA | C | 2 | **M** |
| **Falla de equipos electrónicos y Hardware**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia MODERADO | C | 2 | **M** |
| **Fallas en el suministro de Energía Eléctrica Regulada o UPS´s (Sistemas de Poder In-interrumpido)**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTA | B | 3 | **A** |
| **Caídas del Servicio Telefónico IP**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia MODERADO | C | 2 | **M** |
| **Fallos de la Red de Datos**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTA | C | 3 | **A** |
| **Libros Hablados Digitales**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTA | B | 3 | **A** |
| **Página WEB institucional**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTA | C | 3 | **A** |
| **Robo común de Datos e información institucional**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia MODERADO | B | 2 | **M** |
| **Equipos de virus informáticos**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia MODERADO | C | 2 | **M** |
| **Fallas de personal “clave” de Informática**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTO | B | 3 | **A** |
| **Sabotaje / vandalismo**  Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTO | B | 2 | **A** |
| **Conflagraciones, inundaciones, movimientos telúricos que afecten la infraestructura informática.** Evaluado el riesgo y lo que actualmente ha hecho el Inci para reducir este, es de ocurrencia ALTO | B | 3 | **A** |

|  |  |  |  |
| --- | --- | --- | --- |
| **VERSIÓN** | **FECHA** | **RELACIÓN DE LAS SECCIONES Ó PÁGINAS MODIFICADAS** | **NATURALEZA DEL CAMBIO** |
| 1 | 31/01/2019 | No aplica por ser versión inicial | Adopción del Plan de Riesgos |
| 2 | 08/01/2020 | Versión actualizada | Adopción del Plan de Riesgos |

|  |  |  |
| --- | --- | --- |
| **Elaborado por:** | **Revisado por:** | **Aprobado por:** |
| Firma  Nombre:  Helbert Castillo  Pro. Esp. OAP / INCI | Firma  Nombre  Ricardo Hernández  Jefe OAP | Firma  Nombre  Ricardo Hernández  Jefe OAp |

https://www.pmg-ssi.com/2017/05/iso-27001-plan-de-tratamiento-de-riesgos-de-seguridad-de-la-informacion/