Instituto Nacional de Metrología de Colombia

Proceso	**Coordinación de Sistemas de Información y Redes Secretaria General**
Tipo de documento	Plan
Nombre	**Plan Operativo de Seguridad de la información (POSI)INM 2020-2023**
Código	

(Documento aprobado por el Comité CIGD, Acta 01 de 2020)

CONTENIDO

Página

1. INTRODUCCIÓN 3
2. TÉRMINOS Y DEFINICIONES 4
3. NORMAS APLICABLES 6
4. DEFINICIÓN DE OBJETIVOS 7
4.1. General 7
4.2. Objetivos Específicos Del Plan 7
5. ALCANCE DEL PLAN OPERATIVO 8
6. MARCO TEÓRICO PARA LA DEFINICIÓN DE PLANES DE TRATAMIENTO 9
6.1. Establecimiento del Contexto Interno 9
6.2. Establecimiento del Contexto del Proceso 9
6.3. Identificar Amenazas o Eventos 10
6.4. Identificar Causas o Vulnerabilidades 11
7. METODOLOGÍA DEL PLAN OPERATIVO 13
7.1. Contexto 13
7.2. Situación Actual 14
7.3. Definición de las Variables para el Análisis 15
7.4. Definición de fases del POSI 17
7.5. Planes de Tratamiento para la Fase I 18
7.6. Planes de Tratamiento para la Fase II 19
7.7. Planes de Tratamiento para la Fase III 19

1. INTRODUCCIÓN

El Gobierno Nacional dentro de su política de aprovechamiento de las tecnologías de la información y las comunicaciones define el obligatorio cumplimiento de la Política de Gobierno Digital[1], en el marco del diagnóstico, planificación, implementación, gestión y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información – MSPI[2] desarrollado por el Ministerio TIC.

La protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

El INM ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2009 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como ISO 27002, ISO 27005, entre otras; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas las partes interesadas.

El **Plan Operativo de Seguridad de la información** (POSI) tiene como objetivo fundamental analizar y priorizar los planes de tratamiento de riesgo con el fin de implementar estos planes en un corto o mediano plazo y así cumplir con los objetivos y directrices de seguridad de la información en el INM. De esta manera el plan operativo se convierte en la herramienta necesaria para la implementación y el seguimiento de los controles resultado del análisis de riesgo.

Es un documento que expresa las intenciones de la Entidad en la implementación de iniciativas y acciones que promuevan el uso y la protección de las Tecnologías de la Información y las Comunicaciones – TIC como contribución al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional, El PESI y en general en todos los lineamientos orientados hacia el logro de la misión.

1 https://mintic.gov.co/portal/604/w3-article-74903.html?_noredirect=1

2 https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

2. TÉRMINOS Y DEFINICIONES

Activo: Cualquier cosa que tiene valor para la organización.

Activos de información: Es todo activo que contenga información, la cual posee un valor y es necesaria para realizar los procesos del negocio, servicio y soporte. Se pueden clasificar de la siguiente manera:

1. **Personas:** Incluyendo sus calificaciones, competencias y experiencia.
2. **Intangibles:** Ideas, conocimiento, conversaciones.
3. **Electrónicos:** Bases de datos, archivos, registros de auditoria, aplicaciones, herramientas de desarrollo y utilidades.
4. **Físicos:** Documentos impresos, manuscritos y hardware.
5. **Servicios:** Servicios computacionales y de comunicaciones.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Falla: Daño o afectación de un dispositivo por un periodo determinado. Las fallas las podemos clasificar dependiendo del tipo de evento que la ocasione en: fallas accidentales, intencionales o naturales.

Información: Entendemos por INFORMACIÓN cualquier manifestación (ya sea visual, auditiva, escrita, electrónica, óptica, magnética, táctil) de un conjunto de conocimientos. Por ejemplo:

1. Una noticia que escuchamos por la radio.
2. Una señal de tráfico que advierte un peligro.
3. Una fórmula que usamos en un problema.

Acción de tratamiento: Actividad planificada, temporal y única, diseñada y ejecutada para eliminar o reducir las causas de los riesgos o disminuir el impacto de una eventual materialización de estos.

Control: Actividad de monitoreo ejecutada sistemáticamente y definida en el marco de actividades establecidas en los procesos, determinada con el propósito de reducir la probabilidad o el impacto de la materialización de los riesgos, dando seguridad razonable el cumplimiento de los objetivos

Causas: Fallas, debilidades, condiciones, restricciones o circunstancias ciertas o potenciales, que pueden dar lugar al evento, pueden aumentar la exposición al riesgo o potenciar sus consecuencias.

Consecuencias: Efectos directos e indirectos sobre los recursos y objetivos del proceso si el riesgo se materializa.

Evento: Incidente u ocurrencia interna o externa al proceso, que se da en un lugar o espacio de tiempo particular, de forma súbita o accidental y que impacta el cumplimiento de los objetivos de un proceso.

Indicador de riesgo: Es una herramienta de medición que permite monitorear, de manera preventiva, el comportamiento de los riesgos. Indica cambios en el nivel o exposición a los mismos y permite la identificación de tendencias en el comportamiento de estos, generando alarmas tempranas que conducen a reforzar o enfocar la gestión para evitar su materialización.

Riesgo: Todo evento de ocurrencia incierta que de materializarse genera un impacto, positivo o negativo, en el logro o cumplimiento de los objetivos de los procesos o proyectos. Se puede medir en términos de la probabilidad de ocurrencia y el impacto de sus consecuencias.

Riesgo de Seguridad de la Información: Evento que afecta o amenaza la confidencialidad, integridad y disponibilidad de la información y puede impactar las funciones el logro de los objetivos organizacionales.

3. NORMAS APLICABLES

- NTC/ISO 27001:2013
- NTC/ISO 27005:2009
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL _ Habilitador Gobierno Digital -Seguridad – Decreto 1078 de 2015; Decreto 1008 de 2018.

4. DEFINICIÓN DE OBJETIVOS

4.1. General

Presentar el Plan Operativo de Seguridad de la Información, adoptado por el INM definiendo sus condiciones generales tales como: contexto, alcance, marco conceptual, metodología, análisis y resultados. El POSI busca definir una estrategia de Seguridad de la información liderada por la Coordinación de Sistemas de Información y Redes que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

4.2. Objetivos Específicos Del Plan

- Identificar los planes de tratamiento de riesgos para la mitigación de los riesgos identificados en el INM
- Formalizar y Socializar el POSI como instrumento de direccionamiento estratégico y planificación de la seguridad de la información.
- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Realizar seguimiento y control a la eficacia del plan de tratamiento de riesgos

5. ALCANCE DEL PLAN OPERATIVO

El análisis de riesgo se realizó sobre los activos de información identificados en las mesas de trabajo realizadas con los funcionarios del INM y valorados con criticidad alta. Este plan de focaliza en los riesgos altos para los cuales se definieron planes de tratamiento.

6. MARCO TEÓRICO PARA LA DEFINICIÓN DE PLANES DE TRATAMIENTO

Como parte del marco teórico del análisis de riesgo se determinan las características o aspectos esenciales del entorno en el cual opera la Entidad. Se pueden considerar factores como:

- Políticos
- Sociales y culturales
- Legales y reglamentarios
- Tecnológicos
- Financieros
- Económicos

6.1. Establecimiento del Contexto Interno

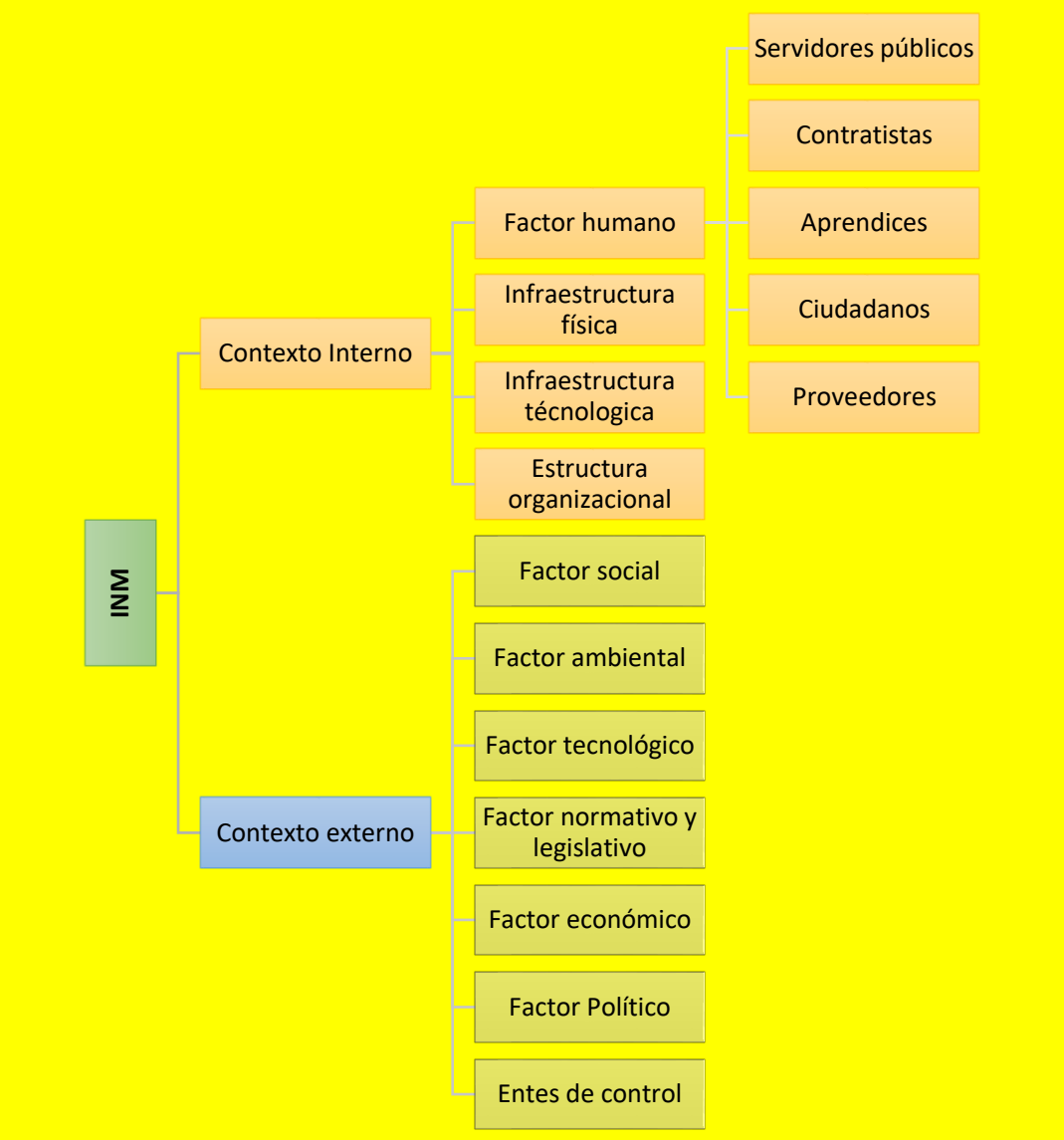
Se determinan las características o aspectos esenciales del ambiente en el cual la Entidad busca alcanzar sus objetivos. Se pueden considerar factores como:

- Estructura Organizacional
- Funciones y Responsabilidades
- Políticas, Objetivos y Estrategias implementadas
- Recursos y Conocimientos con que se cuenta (personas, procesos, sistemas, tecnología)
- Relaciones con las partes involucradas
- Cultura Organizacional

6.2. Establecimiento del Contexto del Proceso

Objetivos del proceso descritos de acuerdo con la metodología (¿Qué se quiere lograr?, ¿Cómo se hace? ¿Para qué?)

- Operatividad del proceso
- El alcance
- Procedimientos
- Roles y Responsabilidades
- Documentos que soportan el proceso
- Entradas y salidas
- Herramientas tecnológicas en las que se soporta el proceso
- Riesgos, medidas de mitigación existentes
- Interacciones con otros Procesos
- Resultados de auditorías internas y externas
- Resultados de autoevaluaciones y hallazgos de auditorías internas y externas



Gráfica: Contexto.

6.3. Identificar Amenazas o Eventos

Las amenazas pueden ser el resultado de actos deliberados o mal intencionados que afectan los activos de los procesos. Las organizaciones enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son específicas para el INM o son únicas consideradas desde el punto de vista de su impacto potencial.

Para la identificación de las amenazas a las que pueden enfrentarse los procesos críticos del negocio se realizan entrevistas con funcionarios del INM, que suministrarán información sobre cuáles son las amenazas con mayor impacto desde la perspectiva de continuidad del servicio o negocio, las que podrían llegar a afectar la continuidad de los procesos y, por consiguiente, podrían causar una pérdida financiera o afectación de la imagen de la Entidad.

6.4. Identificar Causas o Vulnerabilidades

En esta actividad se establece el conjunto de causas de posibles riesgos que posee cada activo crítico, que, en caso de ser explotadas por una o varias amenazas, afectarían la continuidad del proceso. Las vulnerabilidades, por su parte, son debilidades o ausencia de controles que un activo perteneciente a un proceso pueda tener.

Algunas de las causas de riesgos consideradas son:

1. Ausencia de políticas
2. Configuraciones no seguras
3. Errores de configuración
4. Errores de mantenimiento
5. Errores del administrador
6. Errores en código
7. Exposición a materiales peligrosos
8. Fallas de usuarios
9. Manuales de uso no documentados
10. Medidas de protección de acceso inadecuadas
11. Medidas de protección física inadecuadas
12. Procesos o procedimientos no documentados
13. Usuario desinformado
14. Tecnología inadecuada
15. Debilidad o inexistencia de controles

Por otra parte, para poder realizar una eficaz labor preventiva en relación con los riesgos de seguridad de la información es fundamental realizar una precisa identificación de todos y cada uno de los riesgos que existen y que en un momento dado pueden afectar la confidencialidad, la integridad y la disponibilidad de los activos de información del INM. Del análisis de riesgo se pueden obtener las causas que provocan estos riesgos, las causas que los originan, las vulnerabilidades existentes, los controles existentes y su efectividad, el riesgo inherente, y finalmente el riesgo residual, que con base en este último se definen los planes de tratamiento que mitigan estos riesgos, que por sus características sobre pasas el nivel de apetito al riesgo de la Entidad.

La finalidad de esta fase (plan de tratamiento) es descubrir, reconocer y registrar los riesgos. Este proceso incluye la identificación de las causas y el origen de los riesgos, los sucesos o situaciones que pueden tener un impacto en los objetivos de la organización.

El procedimiento para la gestión de riesgos contiene el reconocimiento de las causas y la procedencia del riesgo que puedan afectar a los objetivos.

El método de identificación del riesgo se basa en: mesas de trabajo con los dueños de cada activo, listas de verificación y revisiones de datos históricos sobre activos y riesgos.

Los pasos para la evaluación del riesgo serán:

- Identificación de los riesgos
  - Amenazas
  - Vulnerabilidades
- Análisis del riesgo
- Valoración del riesgo
- Riesgo inherente
- Riesgo residual
- Definición de los planes de tratamiento

Los riesgos que se deben mitigar y los que no, se determinan con base en la siguiente figura:

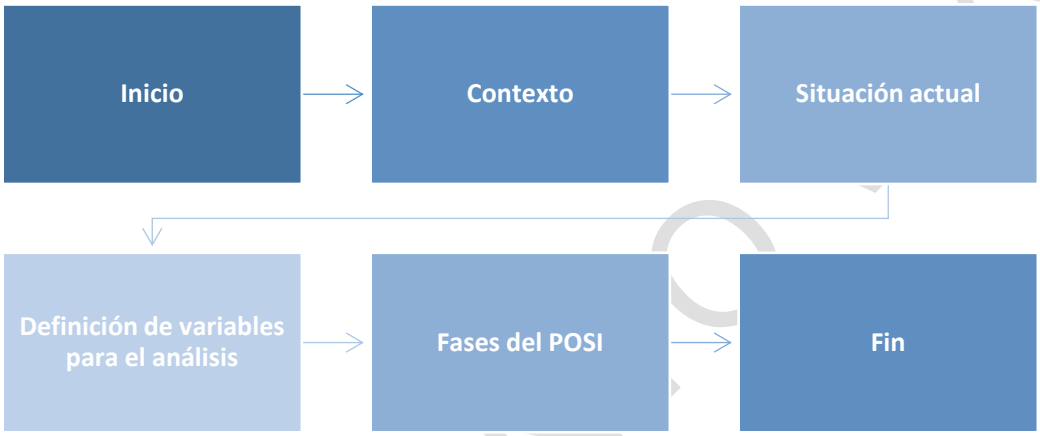
		Niveles de Riesgo				
Probabilidad	Casi seguro	Alto	Alto	Extremo	Extremo	Extremo
	Probable	Moderado	Alto	Alto	Extremo	Extremo
	Posible	Bajo	Moderado	Alto	Alto	Extremo
	Improbable	Bajo	Bajo	Moderado	Alto	Alto
	Rara vez	Bajo	Bajo	Bajo	Moderado	Alto
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		Impacto				

Gráfica: Mapa de riesgos.

Ahora bien, una vez con base en los riesgos críticos se determinan los planes operativos cuya metodología procedemos a exponer.

7. METODOLOGÍA DEL PLAN OPERATIVO

La metodología utilizada para el desarrollo del POSI, que contiene las etapas de contexto, situación actual, definición de variables para el análisis y la determinación de las fases de implementación del Plan Operativo, se muestran y se explican a continuación:



Gráfica: Metodología Utilizada por INM

7.1. Contexto

En esta fase inicial del desarrollo del POSI, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

1. **La misión**
2. **La visión**
3. **Historia y antecedentes**
4. **Estructura organizacional**
5. **Procesos**
6. **Cultura y valores**
7. **Legislación pertinente**

7.2. Situación Actual

Por situación actual se entiende el nivel de madurez que posee en este momento el INM con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina análisis GAP o análisis de brecha. Para poder realizar el POSI es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios.

Por situación actual se entiende también el nivel de madurez que posee en este momento el INM con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina análisis GAP o análisis de brecha. Para poder realizar el POSI es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios con el fin de estimar con mayor precisión las prioridades sobre su implementación.

Dominio ISO 27001	Objetivo de control
Política de seguridad.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14

Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad.	Objetivo de control A.16
Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Tabla: Dominios de la norma ISO 27001:2013.

A continuación, los resultados de la calificación del instrumento del MINTIC:

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**	10	100	**INICIAL**
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	15	100	**INICIAL**
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**	44	100	**EFECTIVO**
A.8	**GESTIÓN DE ACTIVOS**	10	100	**INICIAL**
A.9	**CONTROL DE ACCESO**	15	100	**INICIAL**
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**	63	100	**GESTIONADO**
A.12	**SEGURIDAD DE LAS OPERACIONES**	41	100	**EFECTIVO**
A.13	**SEGURIDAD DE LAS COMUNICACIONES**	44	100	**EFECTIVO**
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	21	100	**REPETIBLE**
A.15	**RELACIONES CON LOS PROVEEDORES**	0	100	**INEXISTENTE**
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**	11	100	**INICIAL**
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	10	100	**INICIAL**
A.18	**CUMPLIMIENTO**	30	100	**REPETIBLE**
PROMEDIO EVALUACIÓN DE CONTROLES		**29**	**100**	**REPETIBLE**

Tabla. Situación actual en materia de riesgos.

7.3. Definición de las Variables para el Análisis

Para la realización del análisis dentro del POSI es necesario definir una serie de variables que ayuden a la priorización de los planes de tratamiento. El POSI propone una estrategia para la implementación basada en la magnitud del riesgo residual (probabilidad e impacto residuales) que permite inferir el orden de implementación de cada uno de los dominios teniendo en cuenta

algunos aspectos asociados a cada uno de los controles. También es considerada la criticidad del activo y la efectividad de los controles.

Planes de tratamiento al riesgo:

Activo de información	Riesgo	Probabilidad residual	Impacto residual	Nivel de Riesgo Residual resultante	Riesgo residual	Plan de tratamiento.
Consecutivo de Resoluciones	Pérdida de disponibilidad por ausencia de espacio físico.	5	4	20	Extremo	Plan de Continuidad del Negocio, Respaldo de la información del Consecutivo de Resoluciones
Inventarios Documentales de Archivos Central	Pérdida de disponibilidad por acceso ineficiente.	4	3	12	Alto	Plan de Continuidad del Negocio, Respaldo de la información para los Inventarios Documentales de Archivos Central
Programa de Gestión Documental	Pérdida de disponibilidad por denegación de los servicios.	3	3	9	Alto	Plan de Continuidad del Negocio, Respaldo de la información, Programa Gestión Documental
Registro de Préstamo y Consulta de Documentos	Pérdida de información física debido a la alta rotación de personal.	3	4	12	Alto	Plan de Continuidad del Negocio, Respaldo de la información para el Registro de Préstamo y Consulta de Documentos
Informe del Congreso	Indisponibilidad de la información por ausencia de respaldos.	3	3	9	Alto	Plan de Continuidad del Negocio, Respaldo de la información del Informe del Congreso
Informe de Gestión Anual	Indisponibilidad de la información por ausencia de respaldos.	3	3	9	Alto	Plan de Continuidad del Negocio y Respaldo de la información del Informe de Gestión anual
Seguimiento de procesos contractuales	Pérdida de integridad por ausencia de control de cambios.	3	3	9	Alto	Procedimientos de operaciones y responsabilidades
Publicación de oferta en la página web y en Medios de Comunicación	Pérdida de integridad por modificación no autorizada de la información.	3	3	9	Alto	Control de Acceso a Publicación de oferta en la página web y en Medios de Comunicación
Formato Informe Mensual Presupuesto Ejecutado Consolidado	Pérdida de confidencialidad por robo de información.	3	4	12	Alto	Control de Acceso al Formato Informe Mensual Presupuesto Ejecutado Consolidado
Kactus	Pérdida de confidencialidad por robo de información,	3	4	12	Alto	Control de Acceso al Sistema de Información Kactus
Registro de las Necesidades de Mejora o Nuevos Desarrollos	Pérdida de confidencialidad por robo de información,	3	4	12	Alto	Control de Acceso del Registro de las Necesidades de Mejora o Nuevos Desarrollos
Especificación de Requerimientos	Pérdida de confidencialidad por robo de información,	3	4	12	Alto	Control de Acceso del Formato Especificación de Requerimientos
Catálogo de Sistemas de Información	Pérdida de confidencialidad por robo de información,	3	4	12	Alto	Control de Acceso al Catálogo de Sistemas de Información

Tabla. Planes de tratamiento.

7.4. Definición de fases del POSI

A continuación, se muestra de acuerdo con el riesgo residual las tres fases (fase 1, fase 2 y fase 3) en que deben ser implementados los planes de tratamiento al riesgo:

Activo de información	Riesgo	Riesgo residual	Plan de tratamiento al riesgo.	FASE DEL PLAN OPERATIVO
Consecutivo de Resoluciones	Pérdida de disponibilidad por ausencia de espacio físico.	20	Plan de Continuidad del Negocio, Respaldo de la información del Consecutivo de Resoluciones	1
Inventarios Documentales de Archivos Central	Pérdida de disponibilidad por acceso ineficiente.	12	Plan de Continuidad del Negocio, Respaldo de la información para los Inventarios	1
Registro de Préstamo y Consulta de Documentos	Pérdida de información física debido a la alta rotación de personal.	12	Plan de Continuidad del Negocio, Respaldo de la información para el Registro de Préstamo y Consulta de Documentos	1
Formato Informe Mensual Presupuesto Ejecutado Consolidado	Pérdida de confidencialidad por robo de información.	12	Control de Acceso al Formato Informe Mensual Presupuesto Ejecutado Consolidado	1
Kactus	Pérdida de confidencialidad por robo de información,	12	Control de Acceso al Sistema de Información Kactus	1
Registro de las Necesidades de Mejora o Nuevos Desarrollos	Pérdida de confidencialidad por robo de información,	12	Control de Acceso del Registro de las Necesidades de Mejora o Nuevos Desarrollos	1
Especificación de Requerimientos	Pérdida de confidencialidad por robo de información,	12	Control de Acceso del Formato Especificación de Requerimientos	1
Formato plantilla de pruebas funcional y/o técnica	Pérdida de confidencialidad por robo de información,	12	Control de Acceso del Formato plantilla de pruebas funcional y/o técnica	1
Catálogo de Sistemas de Información	Pérdida de confidencialidad por robo de información,	12	Control de Acceso al Catálogo de Sistemas de Información	1
Programa de Gestión Documental	Pérdida de disponibilidad por denegación de los servicios.	9	Plan de Continuidad del Negocio, Respaldo de la información, Programa Gestión Documental	2
Informe del Congreso	Indisponibilidad de la información por ausencia de respaldos.	9	Plan de Continuidad del Negocio, Respaldo de la información del Informe del Congreso	2

Informe de Gestión Anual	Indisponibilidad de la información por ausencia de respaldos.	9	Plan de Continuidad del Negocio y Respaldo de la información del Informe de Gestión anual	2
Seguimiento de procesos contractuales	Pérdida de integridad por ausencia de control de cambios.	9	Procedimientos de operaciones y responsabilidades	2

Tabla. Fases de implementación de los planes de tratamiento.

7.5. Planes de Tratamiento para la Fase I

A continuación, se presentan los planes de tratamiento que deben ser implementados en la fase I. Esta fase corresponde con los riesgos que tienen un mayor nivel de criticidad. En esta fase se debe dar importancia especial al diseño de planes de continuidad del negocio, los cuales deben contener las siguientes etapas:

- **Entendimiento del contexto**
- **Análisis de impacto al negocio o BIA.**
- **Definición de escenarios de riesgos.**
- **Análisis de estrategias de recuperación.**
- **Procedimientos.**
- **Gestión de crisis.**
- **Implementaciones.**

Por otro lado, se deben mejorar las medidas de control de acceso apoyados en sensibilizaciones orientadas al uso apropiado de las contraseñas.

Planes de tratamiento al riesgo en Fase I.	FASE DEL PLAN OPERATIVO	Control ISO 27001:2013.
Plan de Continuidad del Negocio, Respaldo de la información del Consecutivo de Resoluciones	1	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Plan de Continuidad del Negocio, Respaldo de la información para los Inventarios Documentales de Archivos Central	1	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Plan de Continuidad del Negocio, Respaldo de la información para el Registro de Préstamo y Consulta de Documentos	1	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Control de Acceso al Formato Informe Mensual Presupuesto Ejecutado Consolidado	1	A.9.1.1, A.9.1.2, A.9.2.1
Control de Acceso al Sistema de Información Kactus	1	A.9.1.1, A.9.1.2, A.9.2.1
Control de Acceso del Registro de las Necesidades de Mejora o Nuevos Desarrollos	1	A.9.1.1, A.9.1.2, A.9.2.1

Control de Acceso del Formato Especificación de Requerimientos	1	A.9.1.1, A.9.1.2, A.9.2.1
Control de Acceso del Formato plantilla de pruebas funcional y/o técnica	1	A.9.1.1, A.9.1.2, A.9.2.1
Control de Acceso al Catálogo de Sistemas de Información	1	A.9.1.1, A.9.1.2, A.9.2.1

Tabla. Fase I.

7.6. Planes de Tratamiento para la Fase II

En esta fase se debe dar énfasis en los planes de continuidad del negocio y de los planes de recuperación ante desastres. Los planes de contingencia también deben ser considerados con el fin de dar una respuesta rápida a cierto tipo de incidentes de seguridad de la información. A continuación, se presentan los planes de tratamiento que deben ser implementados en la fase II:

Planes de tratamiento al riesgo en Fase II.	FASE DEL PLAN OPERATIVO	Control ISO 27001:2013.
Plan de Continuidad del Negocio, Respaldo de la información, Programa Gestión Documental	2	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Plan de Continuidad del Negocio, Respaldo de la información del Informe del Congreso	2	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Plan de Continuidad del Negocio y Respaldo de la información del Informe de Gestión anual	2	A.17.1.1, A.17.1.2, A.17.1.3, A.17.2.1
Procedimientos de operaciones y responsabilidades	2	A.12.1.1
Control de Acceso a Publicación de oferta en la página web y en Medios de Comunicación	2	A.9.1.1, A.9.1.2, A.9.2.1

Tabla. Fase II.

7.7. Planes de Tratamiento para la Fase III

Finalmente, la plataforma INM debe ser provista de medidas de control de acceso que sean efectivas y eficientes con el fin de que no se vea afectado este sistema. A continuación, se presentan los planes de tratamiento que deben ser implementados en la fase III:

Planes de tratamiento al riesgo en Fase III.	FASE DEL PLAN OPERATIVO	Control ISO 27001:2013.
Control de Acceso a Plataforma INM	3	A.9.1.1, A.9.1.2, A.9.2.1

Tabla. Fase III.

ANEXO 1

En este anexo se presentan, para cada plan de tratamiento, las actividades que deben conducir a la implementación satisfactoria de estos planes:

PLAN DE TRATAMIENTO 1: Consecutivo de Resoluciones				
Nombre del Plan de Tratamiento	Plan de Continuidad del Negocio, Respaldo de la información del Consecutivo de Resoluciones			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Las condiciones ambientales deben apoyarse en el control A.11.1.4 con el fin de protegerse contra desastres naturales o accidentales. También el perímetro en donde se almacén información de la Entidad debe cumplir con el control A.11.1.1.	GESTIÓN DOCUMENTAL	1 año
	2	Colocar la Información en un servidor o servidor de archivos y realizar las copias adecuadas de seguridad en cintas magnéticas contando con el respectivo procedimiento. Para este fin se deben seguir los lineamientos del A.12.3.1 de la norma ISO 27001:2013.	SISTEMAS	1 año
	3	Las condiciones ambientales deben apoyarse en el control A.11.1.4 con el fin de protegerse contra desastres naturales o accidentales.	SISTEMAS	1 año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM			
Recursos necesarios para el plan Responsables del plan	Tecnológico: Servidor, Cintas Grupo Administración de Documentos			
Costos estimados				
$ 50.000.000 MCTE				

PLAN DE TRATAMIENTO 2: Inventarios Documentales de Archivos Central				
Nombre del Plan de Tratamiento	Plan de Continuidad del Negocio, Respaldo de la información para los Inventarios Documentales de Archivos Central			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Desarrollar un procedimiento para realizarla ejecución de las copias de respaldo y actualización de inventarios documentales que tenga en cuenta la criticidad del activo de información.	GESTIÓN DOCUMENTAL	1 año
	2	Guardar las copias (backups) de seguridad, en donde su repositorio sea seguro y confiable. Para este fin se deben seguir los lineamientos del A.12.3.1 de la norma ISO 27001:2013.	SISTEMAS	1 año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Servidor, Cintas			
Responsables del plan	Grupo Administración de Documentos			
Costos estimados	$ 20.000.000 MCTE			

PLAN DE TRATAMIENTO 3: Programa de Gestión Documental				
Nombre del Plan de Tratamiento	Plan de Continuidad del Negocio, Respaldo de la información, Programa Gestión Documental			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Desarrollar un procedimiento para verificar los riesgos que pueden ocasionar la perdida de información documental. La información documental debe encontrase en un sitio físico que cumpla con las condiciones ambientales requeridas y control de acceso a estas localidades.	GESTIÓN DOCUMENTAL	1 año
	2	Guardar las copias de seguridad en donde su repositorio sea seguro y confiable.	SISTEMAS	1 año
	3	Revisión de cómo se está aplicando el MIPG, la orientación publica y el Manual integrado de planeación y gestión (función pública) Decreto 1499 de 2017.	GESTIÓN DOCUMENTAL	1 año
Duración estimada del plan	1 año			
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM			
	Tecnológico: Servidor, Cintas			
Responsables del plan	Grupo Administración de Documentos			
Costos estimados	$ 20.000.000 MCTE			

PLAN DE TRATAMIENTO 4: Registro de Préstamo y Consulta de Documentos				
Nombre del Plan de Tratamiento	Plan de Continuidad del Negocio, Respaldo de la información para el Registro de Préstamo y Consulta de Documentos			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Procedimiento de verificación de controles que puede minimizar la pérdida de los documentos físicos. Estos documentos deben poseer las condiciones ambientales adecuadas según normas internacionales. Para este fin se deben seguir los lineamientos del A.12.3.1 de la norma ISO 27001:2013.	GESTIÓN DOCUMENTAL	1 año
	2	Guardar las copias de seguridad fuera de la Entidad, en donde su repositorio sea seguro y confiable. Para este fin se deben seguir los lineamientos del A.12.3.1 de la norma ISO 27001:2013.	SISTEMAS	1 año
	3	Se debe revisar y ajustar el Procedimiento de consulta y préstamo con el fin de mejorar y optimizar la protección de los activos de información cuando sea requerido de manera temporal por un funcionario o contratista.	GESTIÓN DOCUMENTAL	1 año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM			
	Tecnológico: Servidor, Cintas			
Responsables del plan	Grupo Administración de Documentos			
Costos estimados	$ 20.000.000 MCTE			

PLAN DE TRATAMIENTO 5: Informe del Congreso				
Nombre del Plan de Tratamiento	Plan de Continuidad del Negocio, Respaldo de la información del Informe del Congreso			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se debe mantener la información en un servidor replicado dentro o fuera de la Entidad. Este servidor debe poseer características de alta disponibilidad. Para ello se deben seguir los lineamientos de la norma ISO 27001:2013 específicamente en el control A.17.1.3.	SISTEMAS	1 año
	2	Guardar las copias de seguridad fuera de la Entidad, en donde su repositorio sea seguro y confiable. Se deben seguir los lineamientos de la norma ISO 27001:2013 en el control A.12.3.1.	SISTEMAS	1 año
	3	Se debe revisar el procedimiento a seguir del mantenimiento preventivo según lo requerido por el fabricante respectivo. Los procedimientos deben seguir los requisitos de la norma ISO 27001:2013 en el control A.12.1.2.	SISTEMAS	1 año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Servidor, Cintas			
Responsables del plan	Grupo de Gestión de la Información y evaluación de resultados			
Costos estimados	$ 15.000.000 MCTE			

PLAN DE TRATAMIENTO 6: Informe de Gestión Anual				
Nombre del Plan de Tratamiento	Plan de Continuidad del Negocio y Respaldo de la información del Informe de Gestión anual			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Tener la información en un servidor replicado con características de alta disponibilidad. Para lograr que el servidor tenga características de alta disponibilidad se deben seguir los lineamientos del control A.17.2.1.	SISTEMAS	1 año
	2	Guardar las copias de seguridad en donde su repositorio sea seguro y confiable. Se deben seguir los lineamientos de la norma ISO 27001:2013 en el control A.12.3.1.	SISTEMAS	1 año
	3	Mejorar el procedimiento de Verificación de la realización del mantenimiento preventivo según lo requerido por el fabricante. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1.	SISTEMAS	1 año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Servidor, Cintas			
Responsables del plan	Grupo de Gestión de la Información y evaluación de resultados			
Costos estimados	$ 15.000.000 MCTE			

PLAN DE TRATAMIENTO 10: Seguimiento de procesos contractuales				
Nombre del Plan de Tratamiento	Procedimientos de operaciones y responsabilidades			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Todo cambio desarrollado se debe controlar y documentar con el respectivo procedimiento de gestión de cambio y dejar evidencia de este y quien lo autorizó. Para implementar este procedimiento de gestión de cambio se deben seguir los lineamientos de la norma ISO 27001:2013 en lo especificado por el control A.12.1.2 (control de cambios) en donde se estipula que todo cambio que afecte a los activos de información debe ser controlado.	GESTIÓN CONTRACTUAL	1 año
	2	El control de cambios debe aplicarse a todos los documentos considerados como críticos en la matriz de activos de información. Se deben seguir los lineamientos de la norma ISO 27001:2013 en lo especificado por el control A.12.1.2 (control de cambios) en donde se estipula que todo cambio que afecte a los activos de información debe ser controlado.	GESTIÓN CONTRACTUAL	1 año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Pcs			
Responsables del plan	Grupo gestión contractual			

PLAN DE TRATAMIENTO 13: Publicación de oferta en la página web y en Medios de Comunicación				
Nombre del Plan de Tratamiento	Control de Acceso a Publicación de oferta en la página web y en Medios de Comunicación			
Proceso	GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deben aplicar los ítems expuestos en la Política de Control de Acceso y alinearlos a las Publicaciones de oferta en la página web y en Medios de Comunicación, de ser necesario se debe desarrollar procedimientos o guías para establecer el cumplimiento en el control de acceso a las publicaciones. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1.	SEC GRAL SISTEMAS	1 Año
	2	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SEC GRAL SISTEMAS	1 Año
	3	Se debe implementar un proceso formal de registro y de cancelación de registros de usuarios y de esta forma posibilitar los derechos de acceso. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1.	SEC GRAL SISTEMAS	1 Año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Pcs			
Responsables del plan	Director de Formación Profesional Integral.			

Riesgo 15: Formato Informe Mensual Presupuesto Ejecutado Consolidado.				
Nombre del Plan de Tratamiento	Control de Acceso al Formato Informe Mensual Presupuesto Ejecutado Consolidado			
Proceso	GESTIÓN DE LA INNOVACIÓN Y DE LA COMPETITIVIDAD			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deben aplicar los ítems expuestos en la Política de Control de Acceso y alinearlos a Formato Informe Mensual Presupuesto Ejecutado Consolidado, de ser necesario se debe desarrollar procedimientos o guías para establecer el cumplimiento en el control de acceso correspondiente.	SEC GRAL SISTEMAS	1 Año
	2	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que sean autorizados específicamente.	SEC GRAL SISTEMAS	1 Año
	3	Se debe implementar un proceso formal de registro y de cancelación de registros de usuarios y de esta forma posibilitar los derechos de acceso. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1.	SEC GRAL SISTEMAS	1 Año
Duración estimada del plan	1 año			
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Pcs			
Responsables del plan	Grupo de Formación Continua Especializada			

PLAN DE TRATAMIENTO 18: Sistema de Información Kactus				
Nombre del Plan de Tratamiento	Control de Acceso al Sistema de Información Kactus			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deben aplicar los ítems expuestos en la Política de Control de Acceso y alinearlos Sistema de Información de INM, de ser necesario se debe desarrollar procedimientos o guías para establecer el cumplimiento en el control de acceso correspondiente.	SISTEMAS	1 Año
	2	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que sean autorizados específicamente.	SISTEMAS	1 Año
	3	Se debe implementar un proceso formal de registro y de cancelación de registros de usuarios y de esta forma posibilitar los derechos de acceso. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1. Los procedimientos establecen el paso paso para realizar con seguridad y efectividad las actividades operativas del día a día.	SISTEMAS	1 Año
Duración estimada del plan	1 año			
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Pcs			
Responsables del plan	Oficina de sistemas			

PLAN DE TRATAMIENTO 19: Registro de las Necesidades de Mejora o Nuevos Desarrollos				
Nombre del Plan de Tratamiento	Control de Acceso del Registro de las Necesidades de Mejora o Nuevos Desarrollos			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deben aplicar los ítems expuestos en la Política de Control de Acceso y aplicarlos al Registro de las Necesidades de Mejora o Nuevos Desarrollos, de ser necesario se debe desarrollar procedimientos o guías para establecer el cumplimiento en el control de acceso correspondiente. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1. Los procedimientos establecen el paso paso para realizar con seguridad y efectividad las actividades operativas del día a día.	SISTEMAS	1 Año
	2	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que sean autorizados específicamente. Mantener la regla del menor privilegio.	SISTEMAS	1 Año
	3	Se debe implementar un proceso formal de registro y de cancelación de registros de usuarios y de esta forma posibilitar los derechos de acceso. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1. Los procedimientos establecen el paso paso para realizar con seguridad y efectividad las actividades operativas del día a día.	SISTEMAS	1 Año
Duración estimada del plan	1 año			
Recursos para el plan.	Tecnológico: Pcs			
Responsables del plan	Oficina de sistemas			

PLAN DE TRATAMIENTO 20: Formato Especificación de Requerimientos				
Nombre del Plan de Tratamiento	Control de Acceso del Formato Especificación de Requerimientos			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que sean autorizados específicamente.	SISTEMAS	1 Año

		Para establecer este control se debe contar con una política de control de acceso según lo estipulado por el control A.9.1.1.		
Recursos necesarios para el plan	Personas: funcionarios y contratistas Tecnológico: Pcs			
Responsables del plan	Oficina de sistemas			

PLAN DE TRATAMIENTO 21: Formato plantilla de pruebas funcional y/o técnica				
Nombre del Plan de Tratamiento	Control de Acceso del Formato plantilla de pruebas funcional y/o técnica			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deben aplicar los ítems expuestos en la Política de Control de Acceso y aplicarlos al Formato plantilla de pruebas funcional y/o técnica, de ser necesario se debe desarrollar procedimientos o guías para establecer el cumplimiento en el control de acceso correspondiente.	SISTEMAS	1 Año
	2	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que sean autorizados específicamente. Para establecer este control se debe contar con una política de control de acceso según lo estipulado por el control A.9.1.1. Es recomendable que el control de acceso se gestione de modo centralizado tanto para aplicaciones, servidores y equipos de red.	SISTEMAS	1 Año
	3	Se debe implementar un proceso formal de registro y de cancelación de registros de usuarios y de esta forma posibilitar los derechos de acceso. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1. Los procedimientos establecen el paso paso para realizar con seguridad y efectividad las actividades operativas del día a día.	SISTEMAS	1 Año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Pcs			
Responsables del plan	Oficina de sistemas			

PLAN DE TRATAMIENTO 22: Catálogo de Sistemas de Información				
Nombre del Plan de Tratamiento	Control de Acceso al Catálogo de Sistemas de Información			
Actividades a realizar	**Actividad**	**Descripción**	**Responsables**	**Duración**
	1	Se deberá revisar que solo se esté permitiendo el acceso a los usuarios a la red y a los servicios de red para los que sean autorizados específicamente. Para establecer este control se debe contar con una política de control de acceso según lo estipulado por el control A.9.1.1. Es recomendable que el control de acceso se gestione de modo centralizado tanto para aplicaciones, servidores y equipos de red.	SISTEMAS	1 Año
	2	proceso formal de registro y de cancelación de registros de usuarios y de esta forma posibilitar los derechos de acceso. Para la elaboración o mejora de los procedimientos existentes se deben adoptar los lineamientos del control A.12.1.1. Los procedimientos establecen el paso paso para realizar con seguridad y efectividad las actividades operativas del día a día.	SISTEMAS	1 Año
Recursos necesarios para el plan	Personas: funcionarios y contratistas del INM Tecnológico: Pcs			
Responsables del plan	Oficina de sistemas			

FASES POSI	2020	2021	2022
FASE I: Planes de Tratamiento			
FASE II: Planes de Continuidad de Negocio			
FASE III: Medidas de Control			