

“Realización de Fases de implementación del Modelo de Seguridad y Privacidad de la Información del Instituto Nacional de Salud conforme el proceso de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI del Instituto Nacional de Salud conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC y la Política de Gobierno Digital”.

**Bogotá D.C.,**

**CONTROL DE CAMBIOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VERSIÓN** | **FECHA DE APROBACIÓN** | | | **DESCRIPCIÓN** |
| **aaaa** | **mm** | **dd** |
| 00 | 2018 | 12 | 12 | Creación del Documento |
| 01 | 2019 | 12 | 28 | Se actualiza para el 2019 en varios temas que se piden por norma |
| 02 | 2020 | 12 | 15 | Se actualiza para el 2020 en varios temas que se piden por norma |

**TABLA DE CONTENIDO**

[1. OBJETIVO GENERAL 6](#_Toc528775190)

[1.1 OBJETIVOS ESPECÍFICOS 6](#_Toc528775191)

[2. GLOSARIO DE TÉRMINOS 6](#_Toc528775192)

[3. METODOLOGÍA DESARROLLADA 8](#_Toc528775193)

[3.1 EQUIPO DE TRABAJO CONSULTOR 8](#_Toc528775194)

[3.2 EQUIPO DE TRABAJO INSTITUTO NACIONAL DE SALUD 9](#_Toc528775195)

[3.3 ENTREVISTAS REALIZADAS 9](#_Toc528775196)

[3.4 ESCALA DE VALORACIÓN DEL NIVEL DE CUMPLIMIENTO DEL ISO/IEC 27001 10](#_Toc528775197)

[3.5 ESCALA DE VALORACION DEL NIVEL DE MADUREZ DEL SGSI 10](#_Toc528775198)

[4. RESULTADOS DEL ANÁLISIS DE BRECHAS 13](#_Toc528775199)

[4.1 NIVEL DE CUMPLIMIENTO DE CLAUSULAS (ISO/IEC 27001:2013) 13](#_Toc528775200)

[4.2 RESUMEN CUMPLIMIENTO (CLAUSULAS) 14](#_Toc528775201)

[4.3 ANÁLISIS DE MADUREZ DEL SGSI 15](#_Toc528775202)

[4.4 NIVEL DE IMPLEMENTACIÓN DE LOS REQURIMIENTOS DEL ANEXO A (ISO/IEC 27001:2015) 16](#_Toc528775203)

[4.5 RESUMEN IMPLEMENTACIÓN ANEXO A 17](#_Toc528775204)

[4.6 ANÁLISIS DE MADUREZ DEL ANEXO A 19](#_Toc528775205)

[5. CONCLUSIONES 21](#_Toc528775206)

[6. BIBLIOGRAFÍA 22](#_Toc528775207)

[7. ANEXOS 24](#_Toc528775208)

[ANEXO 1. DETALLE ANÁLISIS GAP CLAUSULAS MANDATORIAS ISO/IEC 27001:2013 24](#_Toc528775209)

[ANEXO 2. DETALLE ANÁLISIS DE GAP REQUERIMIENTOS ANEXO A - ISO/IEC 27001:2013 51](#_Toc528775210)

**ÍNDICE DE TABLAS**

[Tabla 1.Equipo de trabajo 8](#_Toc528828145)

[Tabla 2. Equipo de Trabajo Instituto Nacional de Salud 9](#_Toc528828146)

[Tabla 3. Entrevistas de Contextualización y Levantamiento de Información en INS. 10](#_Toc528828147)

[Tabla 4. Escala de Valoración del Cumplimiento 10](#_Toc528828148)

[Tabla 5. Escala de Valoración del Nivel de Madurez del MPSI de MINTIC 13](#_Toc528828149)

[Tabla 6. Detalle del Nivel de Madurez de Clausulas ISO/IEC 27001 Instituto Nacional de Salud 15](#_Toc528828150)

[Tabla 7. Detalle del Nivel de Madurez del Anexo A ISO/IEC 27001 19](#_Toc528828151)

**ÍNDICE DE ILUSTRACIONES**

[Ilustración 1. Niveles de Madurez del MPSI de MINTIC 11](#_Toc528828152)

[Ilustración 2. Resumen de cumplimiento de cláusulas ISO 27001:2013 14](#_Toc528828153)

[Ilustración 3. Cumplimiento de cláusulas mandatarias ISO 27001:2013 15](#_Toc528828154)

[Ilustración 4. Nivel de Madurez ISO/IEC 27001 en el Instituto Nacional de Salud 16](#_Toc528828155)

[Ilustración 5. Estado actual de cumplimiento del Anexo A - ISO 27001:2015 17](#_Toc528828156)

[Ilustración 6. Estado actual de cumplimiento de los objetivos de control del Anexo A - ISO 27001:2015 18](#_Toc528828157)

# OBJETIVO GENERAL

Presentar los resultados del análisis de Brechas ejecutado al Sistema de Gestión de Seguridad de la Información del Instituto Nacional de Salud, bajo la Norma ISO/IEC 27001:2013.

## 1.1 OBJETIVOS ESPECÍFICOS

* Presentar el nivel de cumplimiento del SGSI del Instituto Nacional de Salud, con relación a las cláusulas de obligatorio cumplimiento del estándar ISO/IEC 27001:2013.
* Hacer un análisis detallado de cada uno de los requerimientos por clausula, indicando el estado actual de Madurez
* Presentar gráficamente el porcentaje de cumplimiento de las cláusulas establecidas en la Norma ISO/IEC 27001:2013.
* Dar a conocer el porcentaje de cumplimiento de los controles actualmente implementados en el Instituto Nacional de Salud, con respecto a los objetivos de control y controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001:2013.
* Hacer un análisis detallado de cada uno de los controles de seguridad por objetivo de control, indicando la evidencia de implementación y el Nivel de Madurez
* Presentar gráficamente el porcentaje de cumplimiento de los objetivos de control establecidos en el Anexo A del estándar ISO/IEC 27001:2013.
* Generar conclusiones del Análisis.

# GLOSARIO DE TÉRMINOS

**Aceptación del riesgo:** Decisión de asumir el riesgo.

**Activo de Información:** Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio. En otras palabras, es todo aquello que tiene valor para la organización.

**Análisis de riesgo:** Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

**Autenticidad:** Se refiere a la capacidad de garantizar la identidad de los usuarios y procesos  
que manejan la información.

**Confidencialidad:** Propiedad que determina que la información no está disponible ni sea revelada a individuos, entidades o procesos no autorizados.

**Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

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

**Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

**Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

**Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

**Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

**Riesgo residual:** Nivel restante del riesgo después del tratamiento del riesgo.

**Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como, autenticidad, trazabilidad, no repudio y fiabilidad.

**Sistema de Gestión de Seguridad de la Información** Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la Seguridad de la Información.

**Tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo.

**Trazabilidad:** Las actuaciones pueden ser reproducidas mediante una secuencia de  
acciones determinando quien fue el autor de la acción.

**Valoración del riesgo:** Proceso global de análisis y evaluación del riesgo.

# METODOLOGÍA DESARROLLADA

Para el desarrollo del Análisis de Brechas, basado en la norma ISO/IEC 27001:2013, se ejecutaron las siguientes actividades:

1. Documentación: El análisis de la documentación existente en el INS es el soporte y la evidencia para verificar el nivel de implementación de cada cláusula y de cada objetivo de control del estándar.
2. Instrumento de Evaluación: Elaboración del instrumento para el Análisis de Brechas.
3. Nivel de Madurez: Definir la escala de madurez para la evaluación del estado actual.
4. Entrevistas: En las entrevistas se determina con cada área según el dominio a ser analizado, el estado de cumplimiento de cada una de las cláusulas y objetivos de control del estándar y su nivel de madurez.
5. Análisis de Brechas: Revisión del cumplimiento y el nivel de madurez para cada uno de los requerimientos Mandatorios y del Anexo A, el cual se realizará como se describe a continuación:
6. Identificar y registrar las evidencias de implementación de cada requisito del estándar.
7. Asignar una valoración cualitativa de cada requerimiento, según las evidencias identificadas de acuerdo con la valoración de la Tabla 4. Escala de valoración del cumplimiento.
8. Definir el nivel de Madurez Actual frente a las buenas prácticas establecidas en la norma para el cumplimiento de la ISO/IEC 27001, como se puede apreciar en la Tabla 4. Escala de nivel de Madurez del SGSI.
9. Presentación de Resultados: Presentar los resultados gráficos del Análisis de Brechas identificado en el Instituto Nacional de Salud con respecto al cumplimiento del estándar ISO/IEC 27001.

## EQUIPO DE TRABAJO

En la siguiente tabla se presenta el equipo con su correspondiente rol dentro del proyecto:

|  |  |
| --- | --- |
| **Consultor** | **Rol** |
| Elsa Marlen Baracaldo Huertas | Oficial de seguridad |
| Elizabeth Lopez Lopez | Profesional Especializado |
| Jairo Gomez Mariño | Profesional Especializado |

Tabla 1.Equipo de trabajo

## EQUIPO DE TRABAJO INSTITUTO NACIONAL DE SALUD

En la siguiente tabla se presenta el equipo por parte del Instituto Nacional de Salud que interactúo para lograr los objetivos de esta fase.

|  |  |
| --- | --- |
| **Nombre** | **Rol** |
| Elsa Baracaldo | Jefe OTIC |
| Elizabeth López | Profesional Especializado |
| Jairo Gómez | Profesional Especializado |

Tabla 2. Equipo de Trabajo Instituto Nacional de Salud

## ENTREVISTAS REALIZADAS

En la siguiente tabla se presentan las entrevistas que se llevaron a cabo en el Instituto Nacional de Salud, para realizar el levantamiento de información necesaria para desarrollar el Análisis de Brechas en ISO27001.

|  |  |  |
| --- | --- | --- |
| **Fecha** | **Entrevista** | **Tiempo** |
| Jueves, 13 de septiembre | R01 - Redes en Salud Pública | 2 horas |
| Martes, 18 de septiembre | R02 - Vigilancia y Análisis del Riesgo en Salud Pública | 2 horas |
| Lunes, 10 de septiembre | R03 - Investigación en Salud Pública | 2 horas |
| Martes, 11 de septiembre | R04 - Producción | 2 horas |
| Lunes, 10 de septiembre | R05 - Observatorio Nacional de Salud | 2 horas |
| Lunes, 17 de septiembre | A01 - Gestión Humana | 2 horas |
| Viernes, 14 de septiembre | A02 - Adquisición de Bienes y Servicios | 2 horas |
| Viernes, 14 de septiembre | A03 - Gestión Documental | 2 horas |
| Viernes, 14 de septiembre | A04 - Equipos de Laboratorio | 2 horas |
| Viernes, 14 de septiembre | A05 - Gestión Ambiental | 2 horas |
| Martes, 11 de septiembre | A07 - Gestión Jurídica | 2 horas |
| Miércoles, 19 de septiembre | A08 - Atención al Ciudadano | 2 horas |
| Lunes, 17 de septiembre | A09 - Gestión Financiera | 2 horas |
| Viernes, 14 de septiembre | A10 - Recursos Físicos | 2 horas |
| Lunes, 10 de septiembre | D01 - Planeación Institucional | 2 horas |
| Lunes, 10 de septiembre | D02 - Gestión de Calidad | 2 horas |
| Martes, 18 de septiembre | D03 - Comunicación Institucional | 2 horas |
| Lunes, 17 de septiembre | D04 - Tecnologías de Información y Comunicaciones | 2 horas |
| Lunes, 17 de septiembre | E01 - Control Interno Institucional | 2 horas |
| Martes, 18 de septiembre | Dirección General - Asesores | 2 horas |
| Martes, 18 de septiembre | Dirección General | 2 horas |
| Viernes, 14 de septiembre | Secretaría General | 2 horas |
| Martes, 18 de septiembre | Secretaria General - Asesores | 2 horas |

Tabla 3. Entrevistas de Contextualización y Levantamiento de Información en INS.

## ESCALA DE VALORACIÓN DEL NIVEL DE CUMPLIMIENTO DEL ISO/IEC 27001

Cada uno de los numerales o cláusulas de la ISO/IEC 27001:2013 contienen requerimientos específicos, los cuales fueron analizados para identificar el nivel de cumplimiento del estándar. La valoración del cumplimiento se realizó de acuerdo a la siguiente escala:

|  |  |
| --- | --- |
| Cumple | Se tienen evidencias de que la entidad cumple con el requerimiento. |
| Cumple Parcialmente | Aunque se evidencian avances en la implementación del requerimiento, se tienen algunas debilidades que deben ser remediadas para cumplir con el requerimiento. |
| No Cumple | No se ha iniciado con la implementación del requerimiento o los avances son mínimos. |
| N/A | Requerimiento no aplica a la entidad |

Tabla 4. Escala de Valoración del Cumplimiento

## ESCALA DE VALORACION DEL NIVEL DE MADUREZ DEL SGSI

La valoración del Nivel de Madurez del Sistema de Gestión de Seguridad de la Información se basó en el establecido en el Modelo de Seguridad y Privacidad de Información definido por el MINTIC, el cual contempla 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación, el cual busca establecer unos criterios de valoración a través de los cuales se determina el estado actual de la Seguridad de la Información del Instituto Nacional de Salud. A continuación, se presenta los 6 niveles establecidos para evaluar el nivel de madurez del SGSI del Instituto Nacional de Salud:

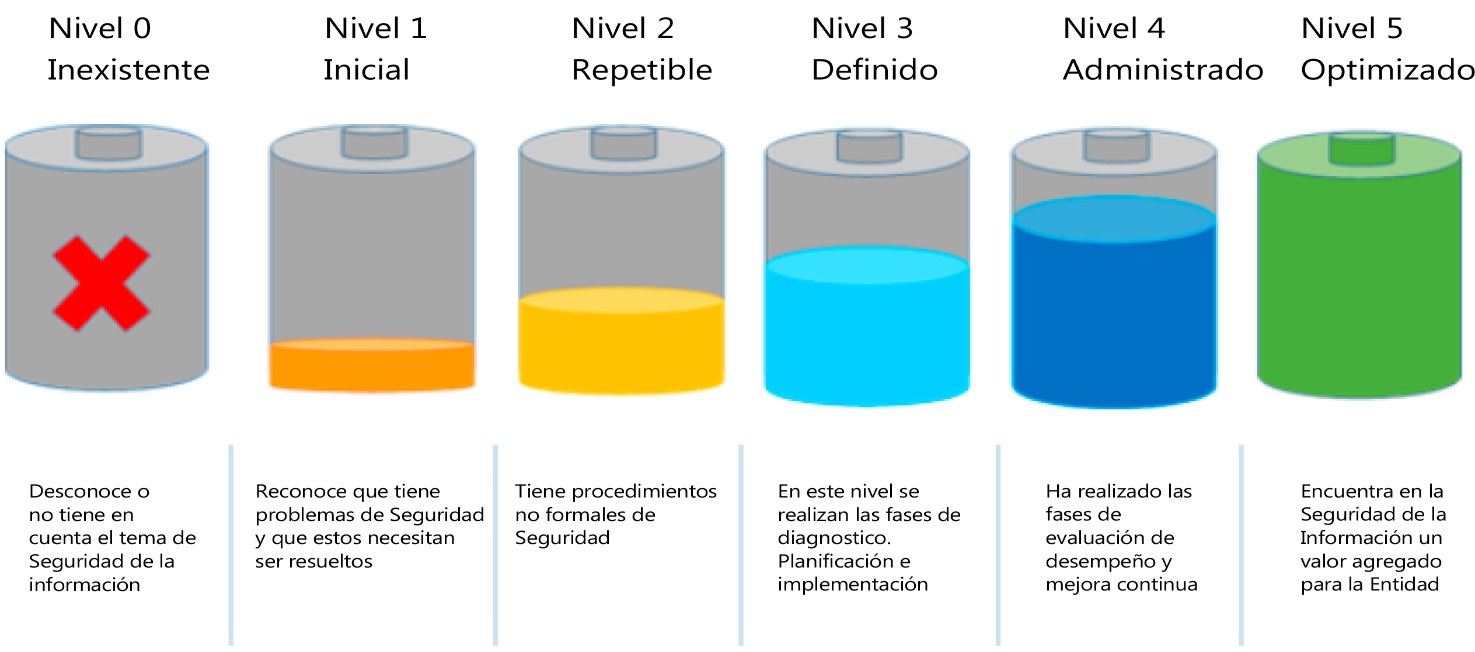


Ilustración 1. Niveles de Madurez del MPSI de MINTIC

El esquema presenta las siguientes características de cada uno de los niveles de madurez, con su descripción general.

| **Descripción** | **Calificación %** | **MPSI** | **Nivel de Madurez Controles** |
| --- | --- | --- | --- |
| Inexistente | 0 | \* Total falta de cualquier proceso reconocible. \* La institución ni siquiera ha reconocido que hay un problema a tratar.  \* No se aplican controles. | \* Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad. \* No se reconoce la información como un activo importante para su misión y objetivos estratégicos. \* No se tiene conciencia de la importancia de la seguridad de la información en la institución. |
| Inicial | 1% a 20% | \* Hay una evidencia de que la institución ha reconocido que existe un problema y que hay que tratarlo.  \* No hay procesos estandarizados.  \* La implementación de un control depende de cada individuo y es principalmente reactiva.  \* Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican. | \* Se han identificado las debilidades en la seguridad de la información. \* Los incidentes de seguridad de la información se tratan de forma reactiva. \* Se tiene la necesidad de implementar el SGSI-PDP, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la institución. |
| Repetible | 21% a 40% | \* Los procesos y los controles siguen un patrón regular.  \* Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas.  \* No hay formación ni comunicación formal sobre los procedimientos y estándares.  \* Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores. | \* Se identifican en forma general los activos de información. \* Se clasifican los activos de información. \* El personal administrativo tiene conciencia de la seguridad de la información. \* Los temas de seguridad y privacidad de la información se tratan en comités de propósito especifico. |
| Definido | 41% a 60% | \* Los procesos y los controles se documentan y se comunican. \* Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada. | \* La institución ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. \* La institución ha determinado los objetivos, alcance y límites de la seguridad de la información. \* La institución ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. \* La institución tiene procedimientos formales de seguridad de la Información \* La institución tiene roles y responsabilidades asignados en seguridad y privacidad de la información. \* La institución ha realizado un inventario de activos de información aplicando una metodología. \* La institución trata riesgos de seguridad de la información a través de una metodología. \* Se implementa el plan de tratamiento de riesgos. |
| Administrado | 61% a 80% | \* Los controles se monitorean y se miden.  \* Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente. | \* Se revisa y monitorea periódicamente los activos de información de la institución. \* Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información. \* Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. |
| Optimizado | 81% a 100% | \* Las buenas prácticas se siguen y automatizan.  \* Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua. | \* En este nivel se encuentran las organizaciones en las cuales la seguridad es un valor agregado. \* Se utilizan indicadores de efectividad para establecer si la institución encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales. |

Tabla 5. Escala de Valoración del Nivel de Madurez del MPSI de MINTIC

# RESULTADOS DEL ANÁLISIS DE BRECHAS

El Análisis de brechas respecto al estándar ISO/IEC 27001:2013 en el Instituto Nacional de Salud, se desarrolló teniendo en cuenta el análisis a la documentación entregada al equipo consultor, así como el levantamiento de información realizado con los responsables. Se identificó en primer lugar el cumplimiento con respecto a las cláusulas obligatorias del estándar y en segundo lugar el cumplimiento frente al Anexo A de la ISO/IEC 27001:2013.

## NIVEL DE CUMPLIMIENTO DE CLAUSULAS (ISO/IEC 27001:2013)

Los requisitos especificados en los numerales del 4 al 10 son de obligatorio cumplimiento para demostrar conformidad con la Norma ISO/IEC 27001:2013. A continuación, se listan dichas cláusulas.

* 4. Contexto de la Organización
* 5. Liderazgo
* 6. Planificación
* 7. Soporte
* 8. Operación
* 9. Evaluación de desempeño
* 10. Mejora

RESUMEN CUMPLIMIENTO (CLAUSULAS)

A continuación, se presenta un resumen del cumplimiento de las cláusulas obligatorias del estándar ISO/IEC 27001:2013:

Ilustración 2. Resumen de cumplimiento de cláusulas ISO 27001:2013

El cumplimiento de cada clausula por parte del Instituto Nacional de Salud se presenta en la Ilustración 3.

Ilustración 3. Cumplimiento de cláusulas mandatarias ISO 27001:2013

**Nota:**

El detalle del análisis realizado se encuentra en el **Anexo 1. Análisis GAP a clausulas mandatarias de ISO/IEC 27001:2013** de este documento.

## ANÁLISIS DE MADUREZ DEL SGSI 2018

A continuación, se presenta el nivel de madurez identificado para cada una de las cláusulas obligatorias del estándar ISO/IEC 27001:2013, frente al nivel de Madurez esperado para el año 2018 de la entidad.

|  |  |  |
| --- | --- | --- |
|  | **Nivel de Madurez** | |
| **REQUERIMIENTOS - SGSI** | **Nivel Actual** | **Nivel Deseado** |
| CONTEXTO DE LA ORGANIZACIÓN | 30% | 100% |
| LIDERAZGO | 54% | 100% |
| PLANIFICACIÓN | 34% | 100% |
| SOPORTE | 33% | 100% |
| OPERACIÓN | 13% | 100% |
| EVALUACIÓN DEL DESEMPEÑO | 7% | 100% |
| MEJORA | 0% | 100% |

Tabla 6. Detalle del Nivel de Madurez de Clausulas ISO/IEC 27001 Instituto Nacional de Salud

La ilustración 4, representa el nivel de madurez correspondiente a cada uno de los requisitos mandatorios del estándar ISO/IEC 27001:2013.Ilustración 4. Nivel de Madurez ISO/IEC 27001 en el Instituto Nacional de Salud

**Nota:**

El promedio en el 2018 de los niveles de madurez de las cláusulas mandatarias nos indica el nivel de madurez actual del INS respecto al estándar ISO/IEC 27001:2013, el cual es: **REPETIBLE con un 24%.**

## ANÁLISIS DE MADUREZ DEL SGSI 2019

A continuación, se presenta el nivel de madurez identificado para cada una de las cláusulas obligatorias del estándar ISO/IEC 27001:2013, frente al nivel de Madurez esperado para el año 2018 de la entidad.

|  |  |  |
| --- | --- | --- |
|  | **Nivel de Madurez** | |
| **REQUERIMIENTOS - SGSI** | **Nivel Actual** | **Nivel Deseado** |
| CONTEXTO DE LA ORGANIZACIÓN | 43% | 100% |
| LIDERAZGO | 76% | 100% |
| PLANIFICACIÓN | 70% | 100% |
| SOPORTE | 46% | 100% |
| OPERACIÓN | 47% | 100% |
| EVALUACIÓN DEL DESEMPEÑO | 23% | 100% |
| MEJORA | 0% | 100% |

Tabla 6. Detalle del Nivel de Madurez de Clausulas ISO/IEC 27001 Instituto Nacional de Salud

La ilustración 4, representa el nivel de madurez correspondiente a cada uno de los requisitos mandatorios del estándar ISO/IEC 27001:2013.Ilustración 4. Nivel de Madurez ISO/IEC 27001 en el

**Nota:**

El promedio en el 2019 de los niveles de madurez de las cláusulas mandatarias nos indica el nivel de madurez actual del INS respecto al estándar ISO/IEC 27001:2013, el cual es: **DEFINIDO con un 44%.**

## NIVEL DE IMPLEMENTACIÓN DE LOS REQURIMIENTOS DEL ANEXO A (ISO/IEC 27001:2015)

Como se mencionó anteriormente la segunda sección tiene que ver con el análisis del cumplimiento frente al Anexo A del estándar ISO/IEC 27002:2013. Los dominios para evaluar se listan a continuación:

* Dominio 5. Política de la Seguridad de la Información
* Dominio 6. Organización de la Seguridad de la Información
* Dominio 7. Seguridad de los Recursos Humanos
* Dominio 8. Gestión de Activos
* Dominio 9. Control de Acceso
* Dominio 10. Criptografía
* Dominio 11. Seguridad Física y del Entorno
* Dominio 12. Seguridad de las Operaciones
* Dominio 13. Seguridad de las Comunicaciones
* Dominio 14. Adquisición, desarrollo y mantenimiento
* Dominio 15. Relaciones con los Proveedores
* Dominio 16. Gestión de Incidentes de Seguridad de la Información
* Dominio 17. Aspectos de Seguridad Información en la Continuidad de Negocio
* Dominio 18. Cumplimiento

## RESUMEN IMPLEMENTACIÓN ANEXO A

A continuación, se presenta un resumen del cumplimiento identificado en los objetivos de control y controles de seguridad, establecidos en el Anexo A del estándar ISO/IEC 27001:2013:

Ilustración 5. Estado actual de cumplimiento del Anexo A - ISO 27001:2015

**Nota:**

El detalle del análisis 2018 realizado se encuentra en el **Anexo 2. Detalle Análisis de Cumplimiento Respecto a Controles del Anexo A (ISO/IEC 27002:2015)** de este documento.

A continuación, se presenta el nivel de cumplimiento de los objetivos de control y controles del Anexo A – ISO27001.

## RESUMEN IMPLEMENTACIÓN ANEXO A

A continuación, se presenta un resumen del cumplimiento identificado en los objetivos de control y controles de seguridad, establecidos en el Anexo A del estándar ISO/IEC 27001:2013:

Ilustración 6. Estado actual de cumplimiento de los objetivos de control del Anexo A - ISO 27001:2015

## ANÁLISIS DE MADUREZ DEL ANEXO A

A continuación, se presenta el nivel de madurez identificado para cada uno de los dominios y objetivos de control, el cual se obtuvo después de promediar el porcentaje del nivel de madurez de cada uno de los controles de seguridad de información establecidos en el Anexo A de ISO/IEC 27001:2013, frente al nivel de Madurez esperado para el año 2018 de la entidad.

|  |  |  |
| --- | --- | --- |
|  | **Nivel de Madurez** | |
| **REQUERIMIENTOS - SGSI** | **Nivel Actual** | **Nivel Deseado** |
| POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN | 80% | 100% |
| ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 32% | 100% |
| SEGURIDAD DE LOS RECURSOS HUMANOS | 56% | 100% |
| GESTIÓN DE ACTIVOS | 32% | 100% |
| CONTROL DE ACCESO | 60% | 100% |
| CRIPTOGRAFÍA | 20% | 100% |
| SEGURIDAD FÍSICA Y DEL ENTORNO | 59% | 100% |
| SEGURIDAD DE LAS OPERACIONES | 72% | 100% |
| SEGURIDAD DE LAS COMUNICACIONES | 76% | 100% |
| ADQUISICIÓN, DESARROLLO Y MANTENIEMIENTO DE SISTEMAS | 2% | 100% |
| RELACIONES CON LOS PROVEEDORES | 38% | 100% |
| GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 20% | 100% |
| ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO | 37% | 100% |
| CUMPLIMIENTO | 51% | 100% |

Tabla 7. Detalle del Nivel de Madurez del Anexo A ISO/IEC 27001

Como se observa en la Tabla 7, el Instituto Nacional de Salud presenta como resultado de implementación del Anexo A del estándar ISO/IEC 27001:2015 un nivel de madurez **DEFINIDO con un 45*%****.* En la ilustración 7, se representa el nivel de madurez correspondiente a 2019 en cada uno de los dominios del Anexo A ISO/IEC 27001:2015.

Nota:

El detalle del análisis realizado se encuentra en el Anexo 2. Detalle Análisis de Cumplimiento Respecto a Controles del **Anexo A**, de este documento.

## ANÁLISIS DE MADUREZ DEL ANEXO A

A continuación, se presenta el nivel de madurez identificado para cada uno de los dominios y objetivos de control, el cual se obtuvo después de promediar el porcentaje del nivel de madurez de cada uno de los controles de seguridad de información establecidos en el Anexo A de ISO/IEC 27001:2013, frente al nivel de Madurez esperado para el año 2018 de la entidad.

|  |  |  |
| --- | --- | --- |
|  | **Nivel de Madurez** | |
| **REQUERIMIENTOS - SGSI** | **Nivel Actual** | **Nivel Deseado** |
| POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN | 100% | 100% |
| ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 65% | 100% |
| SEGURIDAD DE LOS RECURSOS HUMANOS | 67% | 100% |
| GESTIÓN DE ACTIVOS | 37% | 100% |
| CONTROL DE ACCESO | 60% | 100% |
| CRIPTOGRAFÍA | 20% | 100% |
| SEGURIDAD FÍSICA Y DEL ENTORNO | 80% | 100% |
| SEGURIDAD DE LAS OPERACIONES | 79% | 100% |
| SEGURIDAD DE LAS COMUNICACIONES | 85% | 100% |
| ADQUISICIÓN, DESARROLLO Y MANTENIEMIENTO DE SISTEMAS | 87% | 100% |
| RELACIONES CON LOS PROVEEDORES | 80% | 100% |
| GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 40% | 100% |
| ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO | 70% | 100% |
| CUMPLIMIENTO | 73% | 100% |

Tabla 7. Detalle del Nivel de Madurez del Anexo A ISO/IEC 27001

Como se observa en la Tabla 7, el Instituto Nacional de Salud presenta como resultado de implementación del Anexo A del estándar ISO/IEC 27001:2015 un nivel de madurez **ADMINISTRADOcon un 67*%****.* En la ilustración 7, se representa el nivel de madurez correspondiente a cada uno de los dominios del Anexo A ISO/IEC 27001:2015.

# CONCLUSIONES

En el análisis de cumplimiento de las cláusulas del estándar ISO/IEC 27001:2013, se identificaron avances en las cláusulas de: Contexto de la organización, Liderazgo, Planificación, Soporte, Operación pero en general se requieren planes de acción en cada una de las cláusulas mandatorias para lograr el cumplimiento exigido por el Modelo de Seguridad y Privacidad de la Información del MINTIC, el cual requiere para este año un nivel de madurez del 100% para entidades de gobierno a nivel nacional como el INS.

El nivel de madurez de implementación de las cláusulas mandatorias del estándar ISO/IEC 27001:2013, se encuentra en Repetible con un 24%.

En cuanto al cumplimiento de los objetivos de control contemplados en el Anexo A del estándar ISO/IEC 27001:2013, se identifica esfuerzos realizados llegando a un nivel de madurez Definido con un 45%, pero al igual que con las cláusulas se requieren planes de acción en cada objetivo de control para garantizar el cumplimiento exigido por el Modelo de Seguridad y Privacidad de la Información del MINTIC.

En cada uno de los anexos que se presentan a continuación se contemplan planes de acción para mitigar las brechas identificadas tanto en las cláusulas mandatorias como en los objetivos de control del Anexo A del estándar ISO/IEC 27001:2013.

# BIBLIOGRAFÍA

* NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001:2013. Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. ICONTEC.
* NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27002:2013. Técnicas de Seguridad. Código de Practica para controles de Seguridad de la Información. ICONTEC.
* Modelo de Privacidad y Seguridad de la Información del Ministerio de Tecnologías de Información. MINTIC.
* ISO 22301: 2012: Business Continuity Management Systems – Requirements.

## 

# ANEXOS

## ANEXO 1. DETALLE ANÁLISIS GAP CLAUSULAS MANDATORIAS ISO/IEC 27001:2013

| **# ISO** | **Requisito** | **Descripción del requisito** | **¿Implementado?** | **Situación Actual** | **Madurez** | **% Madurez** | **Plan de Acción** | **Soportes** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **4** | **CONTEXTO DE LA ORGANIZACIÓN** | | | | | **30%** |  |  |
| **4.1** | **Conocimiento de la organización y su contexto** | |  |  |  | **40%** |  |  |
| 4.1 | Conocimiento de la organización y su contexto | la organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información. | **PARCIAL** | Se cuenta con un contexto a nivel del sistema integrado de gestión, pero se debe complementar con las cuestiones externas e internas pertinentes al sistema de gestión de la seguridad de la información. | Repetible | 80% | Actualizar en el manual del sistema integrado de gestión el contexto organizacional, con aspectos pertinentes a la seguridad de la información.  **Si se tiene solo se espera en la adopción y que la oficina de calidad vea EVIDENCIAS de la implementación** | 1. Manual del SIG Actualizado 2. Soporte de implementación del sistema de seguridad 3. Las cuestiones internas y externas están en el Anexo 23 del manual |
| **4.2** | **Comprensión de las necesidades y expectativas de las partes interesadas** | | | | | **20%** |  |  |
| 4.2 (a) | La organización debe determinar: | las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información | **PARCIAL** | Se tienen identificados los interesados al nivel del sistema integrado de gestión y en la **resolución 0186 de 2019** que define la política de seguridad de la información, pero se debe revisar para el sistema de gestión de la seguridad de la información. | Repetible | 50% | Actualizar en el manual del sistema integrado de gestión las partes interesada en el SGSI, así como sus necesidades y expectativas en materia de seguridad de la información.  **Si se tiene solo se espera en la adopción y que la oficina de calidad. Se cuenta con evidencias de la actualización de la Resolución 0186 de 2019.** | 1. Manual del SIG Actualizado 2. Actualización de la Resolución 0186 de 2019 ………OK |
| 4.2 (b) | los requisitos de estas partes interesadas pertinentes a seguridad de la información. **NOTA** Los requisitos de las partes interesadas pueden incluir los requisitos legales y de reglamentación, y las obligaciones contractuales. | **PARCIAL** | Se cuenta con requisitos de clientes internos y clientes externos en estudios previos, y clausulas en contratos. | Repetible | 100% | Actualizar en el manual del sistema integrado de gestión las partes interesadas en el SGSI, así como sus necesidades y expectativas en materia de seguridad de la información.  **Soporte de los requisitos de las partes interesadas pueden incluir los requisitos legales y de reglamentación, y las obligaciones contractuales.**  **Se debe radicar el Manual de Políticas Especificas** | 1. Manual del SIG Actualizado. 2. Soportes existentes  * Copia de un contrato evidenciando las cláusulas * Documentos de Acuerdo de confidencialidad * Política de seguridad 0186 de 2019 y las políticas especificas de seguridad |
| **4.3** | **Determinación del alcance del sistema de gestión de seguridad de la información** | | | | | **40%** |  |  |
| 4.3 (a) | La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance. Cuando se determina este alcance, la organización debe considerar: | las cuestiones externas e internas referidas en 4.1 | **PARCIAL** | Se cuenta con un alcance a nivel del sistema integrado de gestión y en la **resolución 0186 de 2019** que define la política de seguridad de la información, pero se debe complementar con las cuestiones externas e internas pertinentes al sistema de gestión de la seguridad de la información. | Repetible | 60% | Actualizar en el manual del sistema integrado de gestión el alcance del sistema de gestión de seguridad de la información y protección de datos personales | 1. Manual del SIG Actualizado 2. Actualización de la Resolución 0186 de 2019 ………OK, 3. Pendiente Protección de Datos |
| 4.3 (b) | los requisitos referidos en 4.2 | **PARCIAL** | Se tienen identificados los interesados al nivel del sistema integrado de gestión, pero se debe revisar su pertinencia con el sistema de gestión de seguridad de la información | Repetible | 60% | Actualizar en el manual del sistema integrado de gestión el alcance con las necesidades y expectativas de las partes interesadas en materia de seguridad de la información. | 1. Manual del SIG Actualizado |
| 4.3 (c) | las interfaces y dependencias entre las actividades realizadas por la organización, y las que realizan otras organizaciones. | **PARCIAL** | Se tienen identificados las interfaces y dependencias entre las actividades realizadas por la organización en el sistema de integrado de gestión, pero se debe revisar su pertinencia con el sistema de gestión de seguridad de la información | Repetible | 40% | Actualizar en el manual del sistema integrado de gestión el alcance con las interfaces entre las actividades realizadas con otras organizaciones | 1. Manual del SIG Actualizado |
| **4.4** | **Sistema de Gestión de Seguridad de la Información** | | | | | **40%** |  |  |
| 4.4 | Sistema de Gestión de Seguridad de la Información | la organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta Norma Internacional. | **PARCIAL** | En la resolución 0186 se documenta la necesidad de establecer un sistema de gestión de la seguridad de la información SGSI, pero actualmente no existe un manual que de los lineamientos de dicho sistema. | Inicial | 40% | Actualizar en el manual del sistema integrado de gestión todos los aspectos necesarios para el establecimiento del SGSI | 1. Manual del SIG Actualizado |
| **5** | **LIDERAZGO** | | | | | **54%** |  |  |
| **5.1** | **Liderazgo y compromiso** | | | | | **45%** |  |  |
| 5.1 (a) | La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información: | asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización | **SI** | En la Resolución 0186 de 2019, la Directora General aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Actualizar en el manual del sistema integrado de gestión la política y objetivos de seguridad de la información y protección de datos personales | 1. Manual del SIG Actualizado |
| 5.1 (b) | asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de negocio de la organización | **PARCIAL** | Desde la OTIC se ha realizado concienciación con las áreas sobre la importancia de la seguridad de la información. | Repetible | 100% | Se actualiza la Resolución 0186 de 2019 de manera que se incorporen no las responsabilidades de la OTIC en materia de seguridad de la información sino las responsabilidades que tienen todas las áreas del instituto | 1. Se actualiza la Política de seguridad 0186 de 2019 |
| 5.1 (c) | asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud. | Definido | 80% | Se actualiza la Resolución 0186 de 2019 de manera que se especifique que el instituto asegurara los recursos necesarios para el sistema de gestión de la seguridad de la información | 1. Se actualiza la Política de seguridad 0186 de 2019 |
| 5.1 (d) | comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información | **SI** | Desde la OTIC se ha realizado concienciación con las áreas sobre la importancia de la seguridad de la información.  Desde la OTIC se han realizado actividades de concientización y se actualizo la resolución por la 0186 de 2019 | Repetible | 60% | Se debe realizar un plan de sensibilización para contemplar los diferentes temas para reforzar el realizado en el 2018 y con el alto compromiso de la alta dirección, se actualizó por la Resolución 0186 de 2019 de manera que se especifique que la alta dirección comunicara periódicamente la importancia de la gestión de la seguridad de la información | 1. Actualización de la resolución 0186 de 2019 |
| 5.1 (e) | asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos | **PARCIAL** | Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados en la nueva resolución  Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados En la Resolución 0186 de 2019 | Repetible | 50% | Se actualizó por la Resolución 0186 de 2019 de manera que se especifique que la alta dirección revisara periódicamente el sistema de gestión de la seguridad de la información para que logre los resultados previstos |  |
| 5.1 (f) | dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información | **PARCIAL** | Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados en la nueva resolución  Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados En la Resolución 0186 de 2019 | Repetible | 40% | Se actualizó por la Resolución 0186 de 2019 de manera que se especifique que la alta dirección dirigirá y apoyara a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información |  |
| 5.1 (g) | promoviendo la mejora continua, y | **PARCIAL** | Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados en la nueva resolución  Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados En la Resolución 0186 de 2019 | Repetible | 40% | Se actualizó por la Resolución 0186 de 2019 de manera que se especifique que la alta dirección dirigirá y apoyara a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información |  |
| 5.1 (h) | apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad. | **PARCIAL** | Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados en la nueva resolución  Desde la OTIC se ha realizado seguimiento para que se cumplan los objetivos planteados En la Resolución 0186 de 2019 | Repetible | 40% | Se actualizó por la Resolución 0186 de 2019 de manera que se especifique que la alta dirección apoyara los roles necesarios para garantizar el cumplimiento de los objetivos de seguridad de la información |  |
| **5.2** | **Política** | | | | | **57%** |  |  |
| 5.2 (a) | La alta dirección debe establecer una política de la seguridad de la información que: | sea adecuada al propósito de la organización | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Se actualizo la resolución y esta adecuada a los requisitos de la NTC 2001 de 2013 donde se incluyen los objetivos y se garantiza los lineamientos de MinTic |  |
| 5.2 (b) | incluya objetivos de seguridad de la información (véase 6.2) o proporcione el marco de referencia para el establecimiento de los objetivos de la seguridad de la información | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Se actualizo la resolución y esta adecuada a los requisitos de la NTC 2001 de 2013 donde se incluyen los objetivos y se garantiza los lineamientos de MinTic.  Revisar la Resolución 1463 de 2017 para garantizar que la política de seguridad de la información incluya objetivos acordes al propósito de la organización |  |
| 5.2 (c) | incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información; y | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Se actualizo la resolución y esta adecuada a los requisitos de la NTC 2001 de 2013 donde se incluyen los objetivos y se garantiza los lineamientos de MinTic.  Revisar la Resolución 1463 de 2017 para garantizar que la política de seguridad de la información incluya el compromiso de cumplir los requisitos aplicables relacionados con la seguridad de la información |  |
| 5.2 (d) | incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información. | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Se actualizo la resolución y esta adecuada a los requisitos de la NTC 2001 de 2013 donde se incluyen los objetivos y se garantiza los lineamientos de MinTic.  Revisar la Resolución 1463 de 2017 para garantizar que la política de seguridad de la información incluya el compromiso de mejora continua del sistema de gestión de la seguridad de la información. |  |
| 5.2 (e) | La política de la seguridad de la información debe: | estar disponible como información documentada | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 100% | Se debe garantizar que la política de seguridad de la información esté disponible como información documentada | Se publica en la Intranet, internet y se socializa |
| 5.2 (f) | comunicarse dentro de la organización; y | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 100% | Se debe garantizar que la política de seguridad de la información se comunique adecuadamente dentro de la institución | Se publica en la Intranet, internet y se socializa |
| 5.2 (g) | estar disponible para las partes interesadas, según sea apropiado. | **PARCIAL** | Se Actualizo la Resolución 0186 de 2019  Resolución 1463 de 2017, únicamente se encuentra publicada a nivel interno, por lo que se debe dar a conocer a interesados a nivel externo. | Repetible | 80% | Se debe garantizar que la política de seguridad de la información esté disponible para las partes interesadas, por ejemplo: publicada en internet. | Se publica en la Intranet, internet y se socializa |
| **5.3** | **Roles, responsabilidades y autoridades de la organización** | | | | | **60%** |  |  |
| 5.3 (a) | La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen. La alta dirección debe asignar la responsabilidad y autoridad para: | asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma Internacional; e | **SI** | Se Actualizo la Resolución 0186 de 2019  En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Se debe revisar la Resolución 1463 de 2017 para garantizar que se encuentren definidos los roles y responsabilidades de seguridad de la información que garanticen la conformidad del sistema con los requisitos de la norma. | Resolución 0186 de 2019 |
| 5.3 (b) | informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información. | **SI** | Se ha informado a la alta dirección sobre temas referentes a la seguridad de la información mediante el Comité de Gestión y Desempeño cuando ha sido necesario. | Definido | 80% | Se debe revisar la Resolución 1463 de 2017 para garantizar que la alta dirección revise periódicamente el desempeño del sistema de gestión de la seguridad de la información. | Resolución 0186 de 2019 |
| **6** | **PLANIFICACIÓN** | | | | | **34%** |  |  |
| **6.1** | **Acciones para tratar riesgos y oportunidades** | | | | | **21%** |  |  |
| **6.1.1** | **Generalidades** | | | | | **60%** |  |  |
| 6.1.1 (a) | Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos a que se hace referencia en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario tratar, con el fin de: | asegurarse de que el sistema de gestión de la seguridad de la información pueda lograr sus resultados previstos | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 80% | Durante el establecimiento del sistema se deben definir objetivos alcanzables con el fin de prevenir o reducir efectos indeseados | 1. Documento entregado por la empresa, contrato de meritos |
| 6.1.1 (b) | prevenir o reducir efectos indeseados; y | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 80% | Durante el establecimiento del sistema se debe hacer un análisis de riesgos con el fin de prevenir o reducir efectos indeseados | 1. Documento entregado por la empresa, contrato de méritos 2. Para el 2019 se realizó la socialización y seguimiento de los riesgos. 3. Se desarrollo una herramienta que permitirá el seguimiento y entrega de evidencias de los Riesgos por las áreas responsables de los riesgos |
| 6.1.1 (c) | lograr la mejora continua. | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Revisar que el manual del sistema integrado de gestión contemple la mejora continua del sistema de gestión de seguridad de la información y protección de datos personales | 1. Manual de Calidad |
| 6.1.1 (d) | La organización debe planificar: | las acciones para tratar estos riesgos y oportunidades; y | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Durante el establecimiento del sistema se debe asegurar el planteamiento de acciones de mejora, para prevenir la materialización del riesgo.  **Pendiente para poder incluir si se materializa poder incluirlo en el sistema SIGEM,** | Pendiente para poder incluir si se materializa poder incluirlo en el sistema SIGEM, |
| 6.1.1 (e) | la manera de: 1) integrar e implementar estas acciones en sus procesos del sistema de gestión de la seguridad de la información, 2) evaluar la eficacia de estas acciones. | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Durante el establecimiento del sistema se debe garantizar que las acciones para el tratamiento de riesgos se hayan evaluado y validado su implementación. |  |
| **6.1.2** | **Evaluación de riesgos de seguridad de la información** | | | | | **4%** |  |  |
| 6.1.2 (a) | La organización debe definir y aplicar un proceso de evaluación de riesgos de la seguridad de la información que: | establezca y mantenga criterios de riesgo de la seguridad de la información que incluyan: 1) Los criterios de aceptación de riesgos; y 2) los criterios para realizar evaluaciones de riesgos de la seguridad de la información | **PARCIAL** | El sistema integrado de gestión cuenta con el documento POE-D02.0000-010 V02\_ Gestión del Riesgo\_ INS, el cual debe ser actualizado para que cumpla lo requerido para el análisis de riesgos de seguridad de la información | Inicial | 40% | Se debe revisar la metodología de gestión de riesgos de la institución, de manera que permita su aplicabilidad con riesgos de seguridad de la información.  **Se socializa la herramienta para implementar los seguimientos** | Se esta realizando la socialización teniendo en cuenta:   1. Los criterios de aceptación de riesgos; y 2) los criterios para realizar evaluaciones de riesgos de la seguridad de la información 2. Se cuenta con una herramienta el seguimiento de las áreas |
| 6.1.2 (b) | asegure que las evaluaciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables | **PARCIAL** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 40% | Realizar un análisis de riesgos de seguridad de la información teniendo en cuenta la metodología definida. | 1. Informe de análisis de riesgos |
| 6.1.2 (c) | identifique los riesgos de la seguridad de la información: 1) aplicar el proceso de evaluación de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información dentro del alcance del sistema de gestión de la seguridad de la información; e 2) identificar a los dueños de los riesgos | **SI** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 60% | Realizar un análisis de riesgos de seguridad de la información teniendo en cuenta la metodología definida. | 1. Informe del 2018. 2. Informe de análisis de riesgos |
| 6.1.2 (d) | analice los riesgos de la seguridad de la información: 1) evaluar las consecuencias potenciales si se materializaran los riesgos identificados en 6.1.2 c) 1); 2) evaluar la probabilidad realista de que ocurran los riesgos identificados en 6.1.2 c) 1); y 3) determinar los niveles de riesgo | **Aplica** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 20% | Realizar un análisis de riesgos de seguridad de la información teniendo en cuenta la metodología definida. | 1. Informe de análisis de riesgos |
| 6.1.2 (e) | evalúe los riesgos de seguridad de la información: 1) comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en 6.1.2 a) y 2) priorizar los riesgos analizados para el tratamiento de riesgos. | **APLICA** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 40% | Realizar un análisis de riesgos de seguridad de la información teniendo en cuenta la metodología definida. | 1. Informe de análisis de riesgos |
| **6.1.3** | **Tratamiento de riesgos de seguridad de la información** | | | | | **0%** |  |  |
| 6.1.3 (a) | La organización debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información para: | seleccionar las opciones apropiadas de tratamiento de riesgos de la seguridad de la información, teniendo en cuenta los resultados de la evaluación de riesgos | **NO** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 40% | Una vez realizado el análisis de riesgos de seguridad de la información, seleccionar las opciones apropiadas de tratamiento de riesgos teniendo en cuenta la metodología definida. | Informe de análisis de riesgos |
| 6.1.3 (b) | determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos de la seguridad de la información | **NO** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 60% | Una vez realizado el análisis de riesgos de seguridad de la información, determinar todos los controles que sean necesarios para implementar las opciones escogidas para el tratamiento de riesgos teniendo en cuenta la metodología definida. | Informe de análisis de riesgos |
| 6.1.3 (c) | comparar los controles determinados en 6.1.3 b) con los del Anexo A, y verificar que no se han omitidos controles necesarios | **NO** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 40% | Una vez realizado el análisis de riesgos de seguridad de la información, revisar los controles para el tratamiento de riesgos con el fin de que no sean omitidos controles necesarios. | Informe de análisis de riesgos |
| 6.1.3 (d) | producir una declaración de aplicabilidad que contenga los controles necesarios (véanse 6.1.3 b) y c)) y la justificación de las inclusiones, ya sea que se implementen o no, y la justificación para las exclusiones de los controles del Anexo A | **NO** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 100% | Elaborar la declaración de aplicabilidad que contenga los controles necesarios sobre el Anexo A de la ISO27001 con sus respectivas justificaciones. | Informe de Declaratoria |
| 6.1.3 (e) | formular un plan de tratamiento de riesgos de la seguridad de la información; y | **NO** | Para el 2019 se realizó un plan de tratamientos de riesgos | Inexistente | 60% | Formular el plan de tratamiento de riesgos de la seguridad de la información. | Informe de análisis de riesgos |
| 6.1.3 (f) | obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información. | **NO** | Para el 2019 se realizó un análisis formal de riesgos en seguridad de la información y las reuniones con los dueños de los riesgos. | Inexistente | 100% | Presentar y obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información. | PENDIENTE |
| **6.2** | **Objetivos de seguridad de la información y planes para lograrlo** | | | | | **46%** |  |  |
| 6.2 (a) | La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes. Los objetivos de seguridad de la información deben: | ser coherentes con la política de seguridad de la información | **SI** | Se cuenta la Resolución 0186 de 2019 para garantizar que los objetivos de seguridad de la información son coherentes con la política de seguridad de la información. la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 100% | Se debe actualizar.  Se actualizo la Resolución 0186 de 2019 | Resolución 0186 de 2019 |
| 6.2 (b) | ser medibles (si es posible) | **NO** | Los objetivos son generales y no se tienen asociados indicadores específicos para medirlos. | Inexistente | 0% | Se debe revisar la Resolución 1463 de 2017 para garantizar que los objetivos de seguridad de la información sean medibles | revisar |
| 6.2 (c) | tener en cuenta los requisitos de la seguridad de la información aplicables, y los resultados de la evaluación y del tratamiento de los riesgos | **NO** | En la actualidad ya se realizó un análisis formal de riesgos en seguridad de la información | Inexistente | 40% | Se implementará el sistema que permitirá realizar, seguimientos, controles a los tratamientos de riesgos | 1. Resolución 0186 de 2019 2. Sistema de evaluación de riesgos |
| 6.2 (d) | ser comunicados; y | **PARCIAL** | Resolución 0186 de 2019, se encuentra publicada en la intranet del INS, aunque falta que sea comunicada a partes interesadas externas | Repetible | 60% | Una vez actualizada la Resolución 0186 de 2019 debe ser publicada y comunicada de manera que todas las partes interesadas puedan conocerla. | Se hace necesario socializarla más |
| 6.2 (e) | ser actualizados, según sea apropiado. | **SI** | Se realizo la actualización de los objetivos de seguridad de la información a través de la Resolución 0186 de 27 febrero  2019 | Definido | 100% | Se actualizo la Resolución 1463 de 2017 para garantizar que los objetivos de seguridad de la información y se actuación los objetivos | Verificar la revisión de los objetivos |
| 6.2 (f) | Cuando se hace la planificación para lograr sus objetivos de la seguridad de la información, la organización debe determinar: | lo que se va a hacer | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  El INS cuenta con un PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en el que se contempla mediante la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Se debe revisar el manual del sistema integrado de gestión para que se incluya como se va hacer para lograr los objetivos de la seguridad de la información, así como los recursos necesarios, responsables, y el método para evaluar los resultados. | Manual de calidad |
| 6.2 (g) | que recursos se requerirán | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  El INS cuenta con un PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en el que se contempla mediante la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Se debe revisar el manual del sistema integrado de gestión para que se incluya como se va hacer para lograr los objetivos de la seguridad de la información, así como los recursos necesarios, responsables, y el método para evaluar los resultados. | Manual de calidad |
| 6.2 (h) | quién será responsable | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  El INS cuenta con un PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en el que se contempla mediante la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Se debe revisar el manual del sistema integrado de gestión para que se incluya como se va hacer para lograr los objetivos de la seguridad de la información, así como los recursos necesarios, responsables, y el método para evaluar los resultados. | Manual de calidad |
| 6.2 (i) | cuando se finalizará; y | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  El INS cuenta con un PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en el que se contempla mediante la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 60% | Se debe revisar el manual del sistema integrado de gestión para que se incluya como se va hacer para lograr los objetivos de la seguridad de la información, así como los recursos necesarios, responsables, y el método para evaluar los resultados. | Manual de calidad |
| 6.2 (j) | cómo se evaluarán los resultados. | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 80% | Se debe revisar el manual del sistema integrado de gestión para que se incluya como se va hacer para lograr los objetivos de la seguridad de la información, así como los recursos necesarios, responsables, y el método para evaluar los resultados. | Manual de calidad |
| **7** | **SOPORTE** | | | | | **33%** |  |  |
| **7.1** | **Recursos** | | | | | **60%** |  |  |
| 7.1 | Recursos | La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información. | **SI** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud.  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. | Definido | 80% | Se debe revisar el manual del sistema integrado de gestión para que se incluya que el INS determinara y proporcionara los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información. | Se efectuó la contratación y el alcance fue análisis de riesgos, procedimientos |
| **7.2** | **Competencia** | | | | | **30%** |  |  |
| 7.2 (a) | La organización debe: | determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, y | **PARCIAL** | En la Resolución 0186 de 2019 se generan roles y responsabilidades sobre el sistema de gestión de seguridad de la información | Inexistente | 40% | En la Resolución 0186 de 2019 se generan roles y responsabilidades sobre el sistema de gestión de seguridad de la información  Se debe revisar el manual del sistema integrado de gestión para que se incluya la competencia necesaria de las personas que realizan un trabajo que afecta el desempeño de la seguridad de la información, basándose en la educación, formación o experiencia adecuadas | la Resolución 0186 de 2019 |
| 7.2 (b) | asegurarse de que estas personas sean competentes, basándose en la educación, formación o experiencia adecuadas | **PARCIAL** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. Dicha consultoría incluye la certificación de personal del INS como auditores internos en ISO27001 | Definido | 60% | Se debe revisar el manual del sistema integrado de gestión para que se incluya la competencia necesaria de las personas que realizan un trabajo que afecta el desempeño de la seguridad de la información, basándose en la educación, formación o experiencia adecuadas | Manual de SIG |
| 7.2 (c) | cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y | **PARCIAL** | La alta Dirección con su apoyo y compromiso de la implementación del sistema de seguridad ha realizado la contratación dos años consecutivos por medio de una consultoría la cual realizo un diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada, adicionalmente se realizó una socialización de los riesgos, se entregó herramientas para su aplicación, seguimiento, control, se trabajó los procedimientos y las políticas específicas para Instituto Nacional de Salud  Actualmente el INS ha asignado recursos para la contratación de una consultoría que realice el diagnóstico del estado del modelo de seguridad y privacidad de la información (MSPI) del INS, la revisión y actualización de la documentación y el levantamiento de los riesgos en todos los procesos de la entidad para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada en el Instituto Nacional de Salud. Dicha consultoría incluye la certificación de personal del INS como auditores internos en ISO27001 | Definido | 60% | Se debe revisar el manual del sistema integrado de gestión para que se incluya que se tomaran las acciones necesarias para que las personas que realizan un trabajo que afecta el desempeño de la seguridad de la información adquieran la competencia necesaria y se evalúen la eficacia de las acciones tomadas | Manual de sIG |
| 7.2 (d) | conservar la información documentada apropiada, como evidencia de la competencia. | **NO** | No se conserva información documentada como evidencia de las competencias en seguridad de la información | Inexistente | 0% | Se debe revisar el manual del sistema integrado de gestión para que se incluya que se tomaran las acciones necesarias para que  conserve la información documentada, como evidencia de la competencia adquirida por las personas que realizan un trabajo que afecta el desempeño de la seguridad de la información. | averiguar |
| **7.3** | **Toma de conciencia** | | | | | **20%** |  |  |
| 7.3 (a) | Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de: | la política de la seguridad de la información; | **PARCIAL** | Actualmente la política se encuentra publicada en la intranet, y se envían tips por correo relacionados con dicha política | Definido | 60% | **Definir los planes necesarios para generar** concientización y capacitación sobre la política de la seguridad de la información de la institución. | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| 7.3 (b) | su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; y | **NO** | Los funcionarios y contratistas aun no tienen conciencia de su contribución a la eficacia del sistema de gestión de la seguridad de la información | Inexistente | 20% | Definir los planes necesarios para generar concientización y capacitación sobre la necesidad de la contribución de los funcionarios a la eficacia del sistema de gestión de la seguridad de la información, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| 7.3 (c) | las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información. | **NO** | Los funcionarios y contratistas aun no tienen conciencia de las implicaciones que tiene la no conformidad de los requisitos del sistema de gestión de la seguridad de la información. | Inexistente | 20% | Definir los planes necesarios para generar concientización y capacitación sobre las implicaciones de la no conformidad con los requisitos del sistema de gestión de la seguridad de la información. | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| **7.4** | **Comunicación** | | | | | **0%** |  |  |
| 7.4 (a) | La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, que incluyan: | el contenido de la comunicación | **NO** | Se han enviado correos para sensibilizar al personal en seguridad de la información, pero no se cuenta con un plan formal de comunicaciones del sistema de gestión de seguridad de la información que contemple aspectos como: contenido, cuando comunicar, a quien comunicar, quien debe comunicar, y los procesos para llevar a cabo la comunicación | Inexistente | 20% | Se debe definir un plan de comunicaciones donde se determine la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, donde se establezca el contenido de cada comunicación, cuando comunicar, a quien comunicar, quien debe comunicar, proceso para llevar a cabo la comunicación | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| 7.4 (b) | cuando comunicar | **NO** | Se han enviado correos para sensibilizar al personal en seguridad de la información, pero no se cuenta con un plan formal de comunicaciones del sistema de gestión de seguridad de la información que contemple aspectos como: contenido, cuando comunicar, a quien comunicar, quien debe comunicar, y los procesos para llevar a cabo la comunicación | Inexistente | 20% | Se debe definir un plan de comunicaciones donde se determine la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, donde se establezca el contenido de cada comunicación, cuando comunicar, a quien comunicar, quien debe comunicar, proceso para llevar a cabo la comunicación | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| 7.4 (c) | a quién comunicar | **NO** | Se han enviado correos para sensibilizar al personal en seguridad de la información, pero no se cuenta con un plan formal de comunicaciones del sistema de gestión de seguridad de la información que contemple aspectos como: contenido, cuando comunicar, a quien comunicar, quien debe comunicar, y los procesos para llevar a cabo la comunicación | Inexistente | 20% | Se debe definir un plan de comunicaciones donde se determine la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, donde se establezca el contenido de cada comunicación, cuando comunicar, a quien comunicar, quien debe comunicar, proceso para llevar a cabo la comunicación | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| 7.4 (d) | quién debe comunicar; y | **NO** | Se han enviado correos para sensibilizar al personal en seguridad de la información, pero no se cuenta con un plan formal de comunicaciones del sistema de gestión de seguridad de la información que contemple aspectos como: contenido, cuando comunicar, a quien comunicar, quien debe comunicar, y los procesos para llevar a cabo la comunicación | Inexistente | 20% | Se debe definir un plan de comunicaciones donde se determine la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, donde se establezca el contenido de cada comunicación, cuando comunicar, a quien comunicar, quien debe comunicar, proceso para llevar a cabo la comunicación | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| 7.4 (e) | los procesos para llevar a cabo la comunicación. | **NO** | Se han enviado correos para sensibilizar al personal en seguridad de la información, pero no se cuenta con un plan formal de comunicaciones del sistema de gestión de seguridad de la información que contemple aspectos como: contenido, cuando comunicar, a quien comunicar, quien debe comunicar, y los procesos para llevar a cabo la comunicación | Inexistente | 20% | Se debe definir un plan de comunicaciones donde se determine la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de la seguridad de la información, donde se establezca el contenido de cada comunicación, cuando comunicar, a quien comunicar, quien debe comunicar, proceso para llevar a cabo la comunicación | Plan de sensibilización  Sensibilización de 2018 y 2019 riesgos |
| **7.5** | **Información documentada** | | | | | **53%** |  |  |
| **7.5.1** | **Generalidades \*consultar Nota en la norma** | | | | | **40%** |  |  |
| 7.5.1 (a) | El sistema de gestión de la seguridad de la información de la organización debe incluir: | la información documentada requerida por esta Norma Internacional; y | **PARCIAL** | Como parte del sistema se cuenta con la Resolución 0186 de 2019 y algunos procedimientos que deben ser actualizados | Repetible | 40% | Información documentada requerida por esta norma:  \* Resolución 0186 de 2019 actualizada \* Manual del sistema integrado de gestión actualizado \* Análisis de riesgos de seguridad de la información  \* Declaración de aplicabilidad \* Plan de tratamiento de riesgos de la seguridad de la información. \* Plan de concientización y capacitación sobre la política de la seguridad de la información de la institución. \* Plan de comunicaciones \* Manual de políticas de seguridad de la información \* Procedimientos de seguridad de la información \* Manual de protección de datos personales \* Procedimientos de datos personales | Actualización de Análisis de riesgos  Herramienta de riesgos |
| 7.5.1 (b) | la información documentada que la organización ha determinado que es necesaria para la eficacia del sistema de gestión de la seguridad de la información. | **PARCIAL** | Como parte del sistema se cuenta con la Resolución 0186 de 2019 y algunos procedimientos que deben ser actualizados | Repetible | 40% | Información documentada requerida por esta norma:   \* Resolución 0186 de 2019 actualizada \* Manual del sistema integrado de gestión actualizado \* Análisis de riesgos de seguridad de la información  \* Declaración de aplicabilidad \* Plan de tratamiento de riesgos de la seguridad de la información. \* Plan de concientización y capacitación sobre la política de la seguridad de la información de la institución. \* Plan de comunicaciones \* Manual de políticas de seguridad de la información \* Procedimientos de seguridad de la información \* Manual de protección de datos personales \* Procedimientos de datos personales |  |
| **7.5.2** | **Creación y actualización** | | | | | **60%** |  |  |
| 7.5.2 (a) | Cuando se crea y actualiza información documentada, la organización debe asegurarse de que lo siguiente sea apropiado: | la identificación y descripción (por ejemplo, título, fecha, autor o número de referencia) | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.2 (b) | el formato (por ejemplo, idioma, versión del software, gráficos) y sus medios de soporte (por ejemplo, papel, electrónico) | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.2 (c) | la revisión y aprobación con respecto a la idoneidad y adecuación. | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| **7.5.3** | **Control de la información documentada** | | | | | **60%** |  |  |
| 7.5.3 (a) | La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta Norma Internacional se debe controlar para asegurarse de que: | esté disponible y adecuada para su uso, donde y cuando se necesite; y | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.3 (b) | esté protegida adecuadamente (por ejemplo, contra pérdida de la confiabilidad, uso inadecuado, o pérdida de integridad). | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.3 (c) | Para el control de la información documentada, la organización debe tratar las siguientes actividades, según sea aplicable: | distribución, acceso, recuperación y uso; | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.3 (d) | almacenamiento y preservación, incluida la preservación de la legibilidad; | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.3 (e) | control de cambios (por ejemplo, control de versión); y | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| 7.5.3 (f) | retención y disposición. | **SI** | Se cuenta con un procedimiento de gestión documental que hace parte del sistema integrado de gestión | Definido | 60% | La documentación del sistema de gestión de seguridad de la información entregada por la consultoría cumplirá con lo establecido por el Manual del sistema integrado de gestión |  |
| **8** | **OPERACIÓN** | | | | | **13%** |  |  |
| **8.1** | **Planificación y control operacional** | | | | | **40%** |  |  |
| 8.1 | Planificación y control operacional | La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requisitos y para implementar las acciones determinadas en el apartado 6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en el apartado 6.2. La organización debe mantener información documentada en la medida necesaria para tener la confianza en que los procesos se han llevado a cabo según lo planificado. La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos, cuando sea necesario. La organización debe asegurar que los procesos contratados externamente estén controlados. | **NO** | Se tienen implementados controles que protegen la confidencialidad, integridad y disponibilidad de la información gestionada en la institución, pero requieren revisión. Adicionalmente se requiere verificar que lo establecido en la Resolución 0186 de 2019 se cumpla. | Repetible | 60% | \* La documentación entregada por la consultoría del sistema de gestión de seguridad de la información deberá ser aprobada por la alta dirección \* Se deben garantizar el cumplimiento de las políticas establecidas para la seguridad de la información \* Se debe hacer seguimiento del sistema mediante las métricas establecidas. |  |
| **8.2** | **Evaluación de riesgos de seguridad de la información** | | | | | **0%** |  |  |
| 8.2 | Evaluación de riesgos de seguridad de la información | La organización debe llevar a cabo evaluaciones de riesgos de la seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos, teniendo en cuenta los criterios establecidos en el apartado 6.1.2 a). |  | Se cuenta con un informe de 2019 realizado por la consultaría de análisis formal de riesgos en seguridad de la información | Inexistente | 40% | \* se cuenta con un análisis de riesgos de seguridad de la información, según la metodología aprobada para dicho análisis. | Informe de análisis de Riesgos  Herramienta de Riesgos |
| **8.3** | **Tratamiento de riesgos de seguridad de la información** | | | | | **0%** |  |  |
| 8.3 | Tratamiento de riesgos de seguridad de la información | La organización debe implementar el plan de tratamiento de riesgos de la seguridad de la información. | **NO** | Para el 2019 se empezó a ejecutar el análisis de riesgos y el plan de tratamiento de riesgos, según la metodología aprobada para dicho análisis. | Inexistente | 40% | \* Para el 2019 se ejecutado el análisis de riesgos y el plan de tratamiento de riesgos, según la metodología aprobada para dicho análisis. | Informe del GAP |
| **9** | **EVALUACIÓN DEL DESEMPEÑO** | | | | | **7%** |  |  |
| **9.1** | **Monitoreo, medición, análisis y evaluación** | | | | | **20%** |  |  |
| 9.1 (a) | La organización debe evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información. La organización debe determinar: | a qué es necesario hacer seguimiento y qué es necesario medir, incluidos los procesos y controles de la seguridad de la información | **NO** | Se cuenta con indicadores que permitan evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información en la institución | Inexistente | 20% | Determinar a qué es necesario hacer seguimiento y qué es necesario medir. | Informe del GAP |
| 9.1 (b) | los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos | **NO** | Se cuenta con indicadores que permitan evaluar el desempeño de la seguridad de la información y la eficacia del sistema de gestión de la seguridad de la información en la institución | Inexistente | 0% | \* Determinar los métodos de seguimiento, medición, análisis y evaluación \* Definir métricas o indicadores del SGSI. | GAP, indicadores |
| 9.1 (c) | cuando se deben llevar a cabo el seguimiento y la medición | **NO** | No se tienen tiempos establecidos para hacer el seguimiento y la medición del sistema de gestión de seguridad de la información | Inexistente | 0% | Determinar cuándo se debe llevar a cabo el seguimiento y la medición. | PENDIENTE |
| 9.1 (d) | quién debe llevar a cabo el seguimiento y la medición | **SI** | En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Determinar quién debe llevar a cabo el seguimiento y la medición. |  |
| 9.1 (e) | cuando se deben analizar y evaluar los resultados del seguimiento y de la medición; y | **NO** | No se tienen tiempos establecidos para analizar y evaluar los resultados del seguimiento y la medición | Inexistente | 0% | Determinar cuándo se deben analizar y evaluar los resultados del seguimiento y de la medición. |  |
| 9.1 (f) | quién debe analizar y evaluar estos resultados. | **SI** | En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. | Definido | 80% | Determinar quién debe analizar y evaluar estos resultados. |  |
| **9.2** | **Seguimiento, medición, análisis y evaluación** | | | | | **0%** |  |  |
| 9.2 (a) | La organización debe llevar a cabo auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información: | es conforme con: 1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y 2) los requisitos de esta Norma Internacional | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | Realizar auditorías periódicas al sistema de gestión de seguridad de la información y protección de datos personales para asegurar conformidad con los requisitos de la organización y de esta esta norma internacional. | Falta la auditoria de documentación |
| 9.2 (b) | está implementado y mantenido eficazmente. | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | Realizar auditorías periódicas al sistema de gestión de seguridad de la información y protección de datos personales para asegurar que está implementado y mantenido eficazmente. |  |
| 9.2 (c) | La organización debe: | planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoría deben tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorías previas | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | La organización debe planificar, establecer, implementar y mantener un programa de auditoría para el sistema de gestión de seguridad de la información y protección de datos personales |  |
| 9.2 (d) | para cada auditoría, definir los criterios y el alcance de ésta | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | La organización debe definir los criterios y el alcance de cada auditoría |  |
| 9.2 (e) | seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | La organización debe asegurarse de la objetividad e imparcialidad del proceso de auditoría |  |
| 9.2 (f) | asegurarse de que los resultados de las auditorías se informan a la dirección pertinente; y | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | La organización debe asegurar que los resultados de las auditorías se informan a la alta dirección cuando sea pertinente |  |
| 9.2 (g) | conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta. | **NO** | No se han llevado a cabo auditorías al sistema de gestión de la seguridad de la información | Inexistente | 0% | La organización debe asegurar la conservación de la información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta. |  |
| **9.3** | **Revisión por la dirección** | | | | | **0%** |  |  |
| 9.3 (a) | La alta dirección debe revisar el sistema de gestión de la seguridad de la información de la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas. La revisión por la dirección debe incluir consideraciones sobre: | el estado de las acciones desde anteriores revisiones por la dirección | **NO** | Con la consultoría se entregó el informe de Seguridad de la Información  Se ha informado a la alta dirección sobre temas referentes a la seguridad de la información mediante el Comité de Gestión y Desempeño cuando ha sido necesario. | Inexistente | 40% | La alta dirección debe revisar, el estado de las acciones desde anteriores revisiones por la dirección | Con la consultoría se entregó el informe de Seguridad de la Información |
| 9.3 (b) | los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información | **NO** | Con la consultoría se entregó el informe de Seguridad de la Información para asegurarse de su conveniencia, adecuación y eficacia | Inexistente | 40% | La alta dirección debe revisar los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información | Con la consultoría se entregó el informe de Seguridad de la Información |
| 9.3 (c) | retroalimentación\* sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a: 1) no conformidades y acciones correctivas; 2) seguimiento y resultados de las mediciones; 3) resultados de la auditoría; y 4) cumplimiento de los objetivos de la seguridad de la información | **NO** | La alta dirección no ha revisado el sistema de gestión de la seguridad de la información periódicamente para asegurarse de su conveniencia, adecuación y eficacia | Inexistente | 0% | La alta dirección debe revisar retroalimentación sobre el desempeño de la seguridad de la información, como: 1) no conformidades y acciones correctivas; 2) seguimiento y resultados de las mediciones; 3) resultados de la auditoría; y 4) cumplimiento de los objetivos de la seguridad de la información |  |
| 9.3 (d) | retroalimentación de las partes interesadas; | **NO** | La alta dirección no ha revisado el sistema de gestión de la seguridad de la información periódicamente para asegurarse de su conveniencia, adecuación y eficacia | Inexistente | 0% | La alta dirección debe revisar la retroalimentación de las partes interesadas |  |
| 9.3 (e) | resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos; y | **NO** | La alta dirección no ha revisado el sistema de gestión de la seguridad de la información periódicamente para asegurarse de su conveniencia, adecuación y eficacia | Inexistente | 0% | La alta dirección debe revisar los resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos | Informarlen |
| 9.3 (f) | las oportunidades de mejora continua. | **NO** | La alta dirección no ha revisado el sistema de gestión de la seguridad de la información periódicamente para asegurarse de su conveniencia, adecuación y eficacia | Inexistente | 0% | La alta dirección debe revisar las oportunidades de mejora continua |  |
| **10** | **MEJORA** | | | | | **0%** |  |  |
| **10.1** | **No conformidades y acciones correctivas** | | | | | **0%** |  |  |
| 10.1 (a) | Cuando ocurra una no conformidad, la organización debe: | reaccionar ante la no conformidad, y según sea aplicable 1) tomar acciones para controlarla y corregirla, y 2) hacer frente a las consecuencias; | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución reaccione ante las no conformidades, y tome las acciones necesarias para controlarlas y corregirlas |  |
| 10.1 (b) | evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante: 1) la revisión de la no conformidad 2) la determinación de las causas de la conformidad, y 3) la determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución evalué la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte |  |
| 10.1 (c) | implementar cualquier acción necesaria; | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución implemente las acciones necesarias |  |
| 10.1 (d) | revisar la eficacia de las acciones correctivas tomadas, y | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución revise la eficacia de las acciones correctivas tomadas |  |
| 10.1 (e) | hacer cambios al sistema de gestión de la seguridad de la información, si es necesario. | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución realice cambios al sistema de gestión de la seguridad de la información, si es necesario. |  |
| 10.1 (f) | Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas. La organización debe conservar información documentada adecuada, como evidencia de: | la naturaleza de las no conformidades y cualquier acción posterior tomada; y | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución conserve la evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada |  |
| 10.1 (g) | los resultados de cualquier acción correctiva. | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución conserve la evidencia de los resultados de cualquier acción correctiva. |  |
| **10.2** | **Mejora continua** | | | | | **0%** |  |  |
| 10.2 | Mejora continua | La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información. | **NO** | Aun no se realiza el proceso de mejora para el sistema de gestión de seguridad de la información, que incluya la identificación de no conformidades y el planteamiento de acciones correctivas | Inexistente | 0% | Se debe asegurar que la institución mejore continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información. |  |

## ANEXO 2. DETALLE ANÁLISIS DE GAP REQUERIMIENTOS ANEXO A - ISO/IEC 27001:2013

| **# ISO** | **Control** | **Descripción del control** | **Aplicación** | **Situación actual** | **¿Implementado?** | **Madurez** | **% Madurez** | **Plan de Acción** | **Soportes** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **5** | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** | | | |  |  | **100%** |  |  |
| **5.1** | **Orientación de la dirección para la gestión de seguridad de la información** | | | |  |  | **100%** |  |  |
|  | Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes. | | | | | | | |  |
| 5.1.1 | Políticas para la seguridad de la información | Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes. | **Aplica** | En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. Adicionalmente, existe un manual de políticas de seguridad de la información en versión borrador. | **SI** | Administrado | 100% | Revisar las políticas de seguridad de la información para que estén acordes con los objetivos estratégicos del INS  CUMPLIDO | Ya se actualizo |
| 5.1.2 | Revisión de las políticas para seguridad de la información | Las políticas para seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas. | **Aplica** | La última vez que se revisó las políticas de seguridad de la información fue cuando se aprobó la Resolución 0186 de 2019. | **SI** | Administrado | 100% | Se recomienda que la política de la seguridad de la información no solo se revise anualmente, sino también cuando ocurran cambios significativos en el INS, a nivel de procesos misionales, o si se han identificado vulnerabilidades del SGSI que deban ser corregidas inmediatamente. |  |
| **6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |  |  | **32%** |  |  |
| **6.1** | **Organización interna** | | |  |  |  | **44%** |  |  |
|  | Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización. | | | | | | |  |  |
| 6.1.1 | Roles y responsabilidades de Seguridad de la información | Se debe definir y asignar todas las responsabilidades de la seguridad de la información. | **Aplica** | \* En la Resolución 0186 de 2019, el director general aprueba la actualización de la política de seguridad de la información, la cual incluye: objetivos de la seguridad de la información, alcance, políticas específicas, responsables. \* El Comité de Gestión y Desempeño cuenta con funciones de seguridad de la información. \* Actualmente el Oficial de Seguridad de la Información es el jefe de la Oficina de Tecnología de la Información y Comunicaciones | **SI** | Administrado | 100% | Se recomienda definir quién será el responsable de la seguridad de la información, así como los integrantes del comité de seguridad de la información o aquel que desempeñe las funciones y responsabilidades de este. | Actualmente el Oficial de Seguridad de la Información es el jefe de la Oficina de Tecnología de la Información y Comunicaciones |
| 6.1.2 | Segregación de funciones | Las funciones en conflicto y áreas de responsabilidad deben ser separadas para reducir las oportunidades de modificación no autorizada o involuntaria, o el mal uso de los activos de la organización. | **Aplica** | A nivel de seguridad de la información no se encuentra definidos roles y perfiles que garanticen una adecuada segregación de funciones | **NO** | Inexistente | 40% | Se recomienda que el responsable de la seguridad de la información se encuentre aislado de procesos en los que exista conflicto de intereses para el desarrollo de sus funciones. | Para ejercer responsabilidad debe estar en otra área |
| 6.1.3 | Contacto con las autoridades | Se deben mantener contactos apropiados con las autoridades pertinentes. | **Aplica** | Actualmente la Oficina de las Tecnologías de la Información se encuentra inscrita en foros de Ciberseguridad de entidades como MIN Defensa, MINTIC, Policía Nacional y CSIRT. | **SI** | Definido | 60% | Se recomienda contar con el asesoramiento de proveedores expertos en seguridad de la información, para que guíen al INS en la aplicación de las mejores prácticas. |  |
| 6.1.4 | Contacto con grupos de interés especial | Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad. | **Aplica** | Actualmente la Oficina de las Tecnologías de la Información se encuentra inscrita en foros de Ciberseguridad de entidades como MIN Defensa, MINTIC, Policía Nacional y CSIRT. | **SI** | Definido | 60% | Se recomienda contar con el asesoramiento de proveedores expertos en seguridad de la información, o convenios con entidades expertas en dicho ámbito para que guíen al INS en la aplicación de las mejores prácticas. |  |
| 6.1.5 | Seguridad de la información en gestión de proyectos | La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. | **Aplica** | Se tienen en cuenta aspectos de seguridad de la información en proyectos que se desarrollan en otras áreas diferentes a la OTIC. | **PARCIAL** | Inicial | 40% | Se recomienda contar con el asesoramiento de proveedores expertos en seguridad de la información, o convenios con entidades expertas en dicho ámbito para que guíen al INS en la aplicación de las mejores prácticas. |  |
| **6.2** | **Dispositivos móviles y teletrabajo** | | | |  |  | **20%** |  |  |
|  | Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles. | | | |  |  |  |  |  |
| 6.2.1 | Política para dispositivos móviles | Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | **Aplica** | Se cuenta la práctica de verificar que los dispositivos móviles en los que se va a configurar el correo electrónico cuenten con aplicaciones seguras, que en caso de no tener dicha configuración no se configura el servicio de correo.  Los funcionarios pueden llevar dispositivos móviles, y algunos contratistas trabajan en computadores personales. | **PARCIAL** | Inicial | 20% | Definir políticas para dispositivos móviles | DEFINIR |
| 6.2.2 | Teletrabajo | Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información que es accesada, procesada o almacenada en los lugares en los que se realiza teletrabajo. | **Aplica** | \* No se tiene definida una política de teletrabajo. \* Existen VPNs para funcionarios de la OTIC para actividades de soporte. Las VPNS se asignan para ingenieros de fábrica y grupo de infraestructura para acceso a servidores, aplicaciones como: RedData, Sihevi, PCC, Sivigila web. \* Se cuenta con instructivo para VPNs \* Las VPNs son autorizadas por la OTIC, utilizan credenciales del directorio activo. \* Se tiene usuario de TeamViewer en la Dirección de vigilancia, el cual se utiliza para dar soporte a usuario final del aplicativo SIVIGILA en departamentos y municipios. \* Se cuenta con 200 licencias de Office 365, para Altos directivos y gerencias medias. | **PARCIAL** | Inicial | 20% | Validar si es necesario implementar una estrategia de teletrabajo y definir las políticas en este sentido. | VALIDAR 0++ |
| **7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | | | |  |  | **56%** |  |  |
| **7.1** | **Antes de asumir el empleo** | | | |  |  | **80%** |  |  |
|  | Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran. | | | | |  |  |  |  |
| 7.1.1 | Selección | Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. | **Aplica** | \* Se cuenta con un procedimiento de vinculación de personal. \* Se verifica los antecedentes mínimos exigidos por ley y según la ley de anti tramites como: antecedentes de fiscalía, de contraloría, de policía, y de procuraduría. \* Adicionalmente se pide otra información como: Certificación bancaria, certificado de afiliación de pensiones, y de EPS \* Si el cargo es directivo se envía a la directora \* Cada dirección selecciona a la persona por meritocracia / concurso. Solo se revisa experiencia y capacitación. | **SI** | Administrado | 80% | Se recomienda verificar los antecedentes de todos los candidatos a un cargo, de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. |  |
| 7.1.2 | Términos y condiciones del empleo | Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información. | **Aplica** | \* Se tienen cláusulas de confidencialidad tanto para funcionarios como para contratistas. Algunos cargos específicos tienen acuerdos especiales de manejo de información. \* Los ingenieros de desarrollo tienen clausulas especiales en el manejo de desarrollo de software, cláusula de propiedad intelectual, regulaciones legales. | **SI** | Administrado | 80% | Revisar los acuerdos contractuales con empleados y contratistas, así como sus responsabilidades en cuanto a seguridad de la información. |  |
| **7.2** | **Durante la ejecución del empleo** | | | |  |  | **27%** |  |  |
|  | Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. | | | | | |  |  |  |
| 7.2.1 | Responsabilidades de la dirección | La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización. | **Aplica** | \* Talento Humano entrega las funciones que debe desempeñar el funcionario nuevo, mediante oficio y realiza una inducción institucional. \* Adicionalmente en el puesto de trabajo se hace una nueva inducción por el jefe directo. \* Se hace un proceso de reinducción cada dos años. \* No se hace inducción en temas referentes a la seguridad de la información. | **NO** | Inexistente | 0% | Definir las responsabilidades de la dirección en la política del SGSI-PDP |  |
| 7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información | Todos los empleados de la organización, en donde sea pertinente y los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. | **Aplica** | \* Talento Humano entrega las funciones que debe desempeñar el funcionario nuevo, mediante oficio y realiza una inducción institucional. \* Adicionalmente en el puesto de trabajo se hace una nueva inducción por el jefe directo. \* Se hace un proceso de reinducción cada dos años. \* No se hace inducción en temas referentes a la seguridad de la información. | **NO** | Inexistente | 0% | Establecer la toma de conciencia y la formación en la seguridad de la información en la política del SGSI-PDP |  |
| 7.2.3 | Proceso disciplinario | Se debe contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | **Aplica** | Se cuenta con proceso disciplinario por manejo inadecuado de información. Control interno, ejecuta el procedimiento a funcionarios y contratistas según procedimiento operativo estándar disciplinario bajo la ley 734 de 2002. | **SI** | Administrado | 80% | Definir un proceso disciplinario en caso de una violación a las políticas de seguridad de la información |  |
| **7.3** | **Terminación y cambio de empleo** | | | | | | **60%** |  |  |
|  | Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo. | | | | | |  |  |  |
| 7.3.1 | Terminación o cambio de responsabilidades de empleo | Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir. | **Aplica** | \* Cuando un funcionario sale a vacaciones, o de licencia, se bloquean los accesos durante dicho periodo. Cuando se retira también se notifica a la OTIC. \* El proceso Contractual envían un archivo con un acumulado de las personas a las que se les termina el contrato. \* En el directorio activo se encuentra la fecha de caducidad del contrato para que venzan los permisos de acceso. \* Las notificaciones se hacen por correo. \* No se notifica cuando existen cambios a nivel de cargos entre áreas. Si se requiere algún cambio de permisos requiere la autorización del jefe inmediato.  \* Para el retiro se hace un acto administrativo aceptando la renuncia, se informa que debe llenar acta de entrega de cargo, diligenciar el paz y salvo del jefe inmediato, de almacén, de biblioteca, de tesorería y de contabilidad, entrega el carnet y la tarjeta de ingreso y se archiva en la historia laboral. \* Durante el acto administrativo se notifica a TI \* No se solicita paz y salvo a contratistas cuando se retiran. Se requiere un mecanismo para la entrega del cargo antes de que se vaya el contratista. \* No se tiene procedimiento por despido únicamente por renuncia. | **PARCIAL** | Definido | 60% | Revisar la pertinencia de las cláusulas de confidencialidad en cargos críticos del INS y ajustarlas |  |
| **8** | **GESTIÓN DE ACTIVOS** | | | | | | **32%** |  |  |
| **8.1** | **Responsabilidad por los activos** | | | | | | **55%** |  |  |
|  | Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. | | | | | |  |  |  |
| 8.1.1 | Inventario de activos | Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | **Aplica** | Se cuenta con un Inventario de activos de información, el cual está valorado de acuerdo a la ley de transparencia y la ley protección de datos personales. Falta valorar los activos de información de acuerdo a los impactos por perdida de Confidencialidad, Integridad y Disponibilidad | **PARCIAL** | Repetible | 40% | Definir la metodología para desarrollar el inventario de activos y llevarlo a cabo |  |
| 8.1.2 | Propiedad de los activos | Los activos mantenidos en el inventario deben ser propios. | **Aplica** | En el inventario se encuentra definido el responsable de cada activo. La consultoría tiene el objetivo de revisar dicho inventario. | **SI** | Optimizado | 100% | Definir la metodología para desarrollar el inventario de activos y llevarlo a cabo |  |
| 8.1.3 | Uso aceptable de los activos | Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información. | **Aplica** | Existe un instructivo de reglas de uso de dispositivos informáticos. Se debe establecer políticas para el uso aceptable de activos. | **PARCIAL** | Inicial | 20% | Definir política sobre el uso aceptable de los activos |  |
| 8.1.4 | Devolución de activos | Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren en su custodia, al terminar su empleo, contrato o acuerdo. | **Aplica** | Existe procedimiento de almacén para la devolución de activos por parte de funcionarios, luego de lo cual emiten un paz y salvo. Los contratistas no cuentan con dicho procedimiento, por lo cual se requiere formalizar dicha entrega. Esto debe aplicar tanto para equipos como para activos de información. Por ahora los contratistas deben devolver los activos al supervisor. | **PARCIAL** | Definido | 60% | Definir política sobre el uso aceptable de los activos |  |
| **8.2** | **Clasificación de la información** | | | | | | **20%** |  |  |
|  | Objetivo: Asegurar que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. | | | | | |  |  |  |
| 8.2.1 | Clasificación de la información | La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | **Aplica** | El inventario está valorado de acuerdo a la ley de transparencia y la ley protección de datos personales. Falta valorar los activos de información de acuerdo a los impactos por perdida de Confidencialidad, Integridad y Disponibilidad | **PARCIAL** | Definido | 60% | Desarrollar la metodología para la clasificación de la información en el INS |  |
| 8.2.2 | Etiquetado de la información | Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. | **Aplica** | No se tienen etiquetados documentos por su clasificación. | **NO** | Inexistente | 0% | Desarrollar procedimiento para el etiquetado de la información en el INS |  |
| 8.2.3 | Manejo de activos | Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. | **Aplica** | No se tienen políticas de manejo de activos según su clasificación. | **NO** | Inexistente | 0% | Definir política sobre el uso aceptable de los activos |  |
| **8.3** | **Manejo de los medios** | | | | | | **20%** |  |  |
|  | Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte. | | | | | |  |  |  |
| 8.3.1 | Gestión de medios removibles | Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | **Aplica** | \* No existen políticas para medios removibles. \* Todos los equipos tienen habilitados los puertos USB. \* Se utilizan medios de almacenamiento personales para backups, como: Discos duros, USB, dvds. | **NO** | Inexistente | 0% | Desarrollar políticas de manejo de medios removibles |  |
| 8.3.2 | Eliminación de los medios | Los medios deben ser desechados de forma segura cuando ya no son necesarios, utilizando procedimientos formales. | **Aplica** | \* Cuando se va a dar de baja un equipo se formatea con formato rápido \* Cuando se entrega un equipo a otro funcionario, sin pasar por almacén no se formatea el equipo. | **PARCIAL** | Repetible | 40% | Formalizar políticas de eliminación de medios |  |
| 8.3.3 | Transferencia de medios físicos | Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. | **Aplica** | \* Gestión documental, realiza el transporte de archivo físico. \* Lo hacen directamente sin terceos \* Transportan por medio de vehículo de la entidad sin los medios de seguridad adecuados. | **PARCIAL** | Inicial | 20% | Formalizar políticas de transferencia de medios que contienen información contra acceso no autorizado, uso indebido o corrupción durante el transporte. |  |
| **9** | **CONTROL DE ACCESO** | | | | | | **60%** |  |  |
| **9.1** | **Requisitos del negocio para control de acceso** | | | | | | **50%** |  |  |
|  | Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información. | | | | | |  |  |  |
| 9.1.1 | Política de control de acceso | Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | **Aplica** | \* El canal para solicitar la creación de usuarios es a través del Service Manager. \* No se encuentra documentados los perfiles de acceso, aunque se crean perfiles básicos de dominio y de internet, permisos adicionales deben ser solicitados por los jefes inmediatos. \* Los accesos a los sistemas de información son administrados por cada dirección. | **PARCIAL** | Inicial | 20% | Formalizar las políticas de control de acceso a información y a instalaciones de procesamiento de información. |  |
| 9.1.2 | Acceso a redes y a servicios en red | Los usuarios solo deben disponer de acceso a la red y servicios en red a los cuales han sido específicamente autorizados para su uso. | **Aplica** | \* La OTIC gestiona los accesos de los usuarios al dominio, a la red y el acceso a internet. \* Los accesos a los sistemas de información son administrados por cada dirección. | **PARCIAL** | Administrado | 80% | Formalizar las políticas de control de acceso a información y a instalaciones de procesamiento de información. |  |
| **9.2** | **Gestión de acceso de usuarios** | | | | | | **60%** |  |  |
|  | Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios. | | | | | |  |  |  |
| 9.2.1 | Registro y eliminación de usuarios | Se debe implementar un proceso formal de registro y eliminación de usuarios, para permitir la asignación de los derechos de acceso. | **Aplica** | \* La creación de usuarios llega por Service Manager \* La modificación o bloqueo de una cuenta llega por correo a la jefatura de la OTIC. \* No se tiene un proceso formal para la eliminación de cuentas de usuario. | **PARCIAL** | Administrado | 80% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios que incluyan: la creación, modificación, eliminación y revisión de dichos accesos. |  |
| 9.2.2 | Suministro de acceso de usuarios | Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios a todos los sistemas y servicios. | **Aplica** | \* La creación de usuarios llega por Service Manager \* La modificación o bloqueo de una cuenta llega por correo a la jefatura de la OTIC. \* No se tiene un proceso formal para la eliminación de cuentas de usuario. | **PARCIAL** | Administrado | 80% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios que incluyan: la creación, modificación, eliminación y revisión de dichos accesos. |  |
| 9.2.3 | Gestión de derechos de acceso privilegiado | Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. | **Aplica** | \* No existe procedimiento formal para modificación o eliminación de permisos. \* No se encuentra documentada la creación o modificación de perfiles de administrador en servidores o sistemas de información. | **NO** | Inexistente | 0% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios, incluyendo cuentas de administrador |  |
| 9.2.4 | Gestión de información de autenticación secreta de usuarios | La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. | **Aplica** | \* Se asigna una contraseña temporal diferente por persona que debe cambiarse después del primer inicio de sesión. Se debe cambiar cada 3 meses. \* Cada dirección es administrador de los sistemas de información de su área, muchas de las cuales no cumplen con una política estándar de control de acceso | **PARCIAL** | Administrado | 80% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios que incluyan: la creación, modificación, eliminación y revisión de dichos accesos. |  |
| 9.2.5 | Revisión de los derechos de acceso de usuarios | Los dueños de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. | **Aplica** | \* Cada dirección es administrador de los sistemas de información de su área, muchas de las cuales no cumplen con una política estándar de control de acceso \* Una vez al año se revisan las cuentas de usuario que no están activas, pero no se encuentra formalizado dicho procedimiento. \* Existe un formato del sistema integrado de gestión para el registro del monitoreo y acceso a las plataformas, en el que se registra: usuarios y perfiles, periodo de validez, usuario de consulta, tipo de permiso (lectura y escritura). | **PARCIAL** | Repetible | 40% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios que incluyan: la creación, modificación, eliminación y revisión de dichos accesos. |  |
| 9.2.6 | Cancelación o ajuste de los derechos de acceso | Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. | **Aplica** | \* Las cuentas de contratistas se bloquean automáticamente en el dominio porque tienen configurada la fecha de vencimiento del contrato. \* Cuando un funcionario sale a vacaciones o de permiso se notifica a la OTIC y se procede con la desactivación de la cuenta de usuario. \* Una vez al año se revisan las cuentas de usuario que no están activas, pero no se encuentra formalizado dicho procedimiento. | **PARCIAL** | Administrado | 80% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios que incluyan: la creación, modificación, eliminación y revisión de dichos accesos. |  |
| **9.3** | **Responsabilidades de los usuarios** | | | | | | **80%** |  |  |
|  | Objetivo: Hacer que los usuarios se responsabilicen por salvaguardar su información de autenticación. | | | | | |  |  |  |
| 9.3.1 | Uso de información de autenticación secreta | Se debe exigir a los usuarios que cumplan las prácticas de la organización en el uso de información de autenticación secreta. | **Aplica** | \* Las contraseñas expiran cada 3 meses, es alfanumérica de 10 o más dígitos. no es mandatorio el uso de mayúscula, minúscula, caracteres especiales, no recuerda histórico \* Se asigna una contraseña temporal diferente por persona que debe cambiarse después del primer inicio de sesión. Se debe cambiar cada 3 meses. \* Existen cuentas asociadas a servicios que se encuentran en la OU management service account, que nunca expiran. \* Las cuentas de usuarios administradores al igual que las de los usuarios genéricos cambian cada 3 meses. \* Existen cuentas compartidas. | **PARCIAL** | Administrado | 80% | Formalizar políticas de manejo de contraseñas |  |
| **9.4** | **Control de acceso a sistemas y aplicaciones** | | | | | | **48%** |  |  |
|  | Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones. | | | | | |  |  |  |
| 9.4.1 | Restricción de acceso a información | El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. | **Aplica** | \* Cada dirección es administrador de los sistemas de información de su área, muchas de las cuales no cumplen con una política estándar de control de acceso. \* No se tiene una política de control de acceso. | **PARCIAL** | Inicial | 20% | Formalizar políticas y procedimientos para la gestión de accesos a sistemas y servicios que incluyan: la creación, modificación, eliminación y revisión de dichos accesos. |  |
| 9.4.2 | Procedimiento de conexión segura | Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura. | **Aplica** | No se está aplicando este control actualmente. | **NO** | Inexistente | 0% | Garantizar conexiones seguras a los sistemas y aplicaciones |  |
| 9.4.3 | Sistema de gestión de contraseñas | Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas. | **Aplica** | \* No se exigen contraseñas fuertes \* Las contraseñas expiran cada 3 meses, es alfanumérica de 10 o más dígitos. no es mandatorio el uso de mayúscula, minúscula, caracteres especiales, no recuerda histórico \* Se asigna una contraseña temporal diferente por persona que debe cambiarse después del primer inicio de sesión. Se debe cambiar cada 3 meses. \* Cada dirección es administrador de los sistemas de información de su área, muchas de las cuales no cumplen con una política estándar de control de acceso \* Algunos sistemas como Enterprise, SISDOC, planes de mejoramiento, PQRSD, Intranet y certificaciones laborales en línea se encuentran unidos al dominio. | **PARCIAL** | Definido | 60% | Formalizar políticas de manejo de contraseñas |  |
| 9.4.4 | Uso de programas utilitarios privilegiados | Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones. | **Aplica** | \* Los equipos unidos al dominio no tienen permiso de administrador por tanto no pueden instalar software. \* Si se requiere la instalación de algún software específico se solicita a través del Service Manager y lo gestiona la Mesa de Ayuda. | **SI** | Administrado | 80% | Formalizar políticas sobre el uso no autorizado de programas utilitarios |  |
| 9.4.5 | Control de acceso a códigos fuente de programas | Se debe restringir el acceso a códigos fuente de programas. | **Aplica** | Los códigos fuente se encuentran en repositorios independientes, con control de acceso. | **SI** | Administrado | 80% | Implementar controles que prevengan el acceso no autorizado a códigos fuente de programas desarrollados inhouse o adquiridos. |  |
| **10** | **CRIPTOGRAFÍA** | | | | | | **20%** |  |  |
| **10.1** | **Controles criptográficos** | | | | | | **20%** |  |  |
|  | Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información. | | | | | |  |  |  |
| 10.1.1 | Política sobre el uso de controles criptográficos | Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información. | **Aplica** | \* Se tiene inventario de los certificados, no se tiene procedimiento o políticas obre controles criptográficos. \* Certificado público para comunicaciones unificadas que funciona sobre Lync 2013, página web, servidor aplicaciones producción, aula virtual, investigación CENS, correo \* Certificado validación extendida, certificados básicos, con certicamara, gcs gestión de seguridad electrónica \* Se tiene CA propia \* Se utilizan certificaos fuertes para servicios críticos | **PARCIAL** | Repetible | 40% | \* Se recomienda identificar todos los certificados y controles criptográficos que se utilizan en el INS \* Generar la política para el uso adecuado de controles criptográficos |  |
| 10.1.2 | Gestión de claves | Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida. | **Aplica** | \* Se tiene inventario de los certificados, no se tiene procedimiento o políticas obre controles criptográficos. \* No Se tiene una política sobre el uso, protección y tiempo de vida de claves criptográficas. | **NO** | Inexistente | 0% | \* Se recomienda identificar todos los certificados y controles criptográficos que se utilizan en el INS \* Generar la política para el uso adecuado de controles criptográficos |  |
| **11** | **SEGURIDAD FÍSICA Y DEL ENTORNO** | | | | | | **59%** |  |  |
| **11.1** | **Áreas seguras** | | | | | | **67%** |  |  |
|  | Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. | | | | | |  |  |  |
| 11.1.1 | Perímetro de seguridad física | Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. | **Aplica** | \* Se tiene un perímetro de seguridad externo y se tienen definidas áreas seguras internas, como: DataCenter, Bioterio, planta de sueros, laboratorios en general, COE Centro operativo de emergencias, Tesorería y almacén los cuales cuentan con controles de acceso específicos gestionados por cada área. \* Se cuenta con un servicio vigilancia privada, que consta de 8 guardas en sede principal, 1 en la hacienda, 1 en armero (finca). \* También se cuenta con circuito cerrado de televisión, que consta de 78 cámaras, el cual es del tercero, ellos custodian los backups, y el software de registro de acceso. \* En la entrada se cuenta con Talanqueras que son del instituto, para acceso de funcionarios, los contratistas no cuenta con tarjetas de acceso. \* El archivo central tiene servicio de vigilancia, no tiene circuito cerrado de televisión, el archivo se encuentra bajo llave, está ubicado en una zona insegura, ha tenido problemas de goteras. | **SI** | Administrado | 80% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| 11.1.2 | Controles de ingreso físicos | Las áreas seguras se deben proteger mediante controles de ingreso apropiados para asegurar que solamente se permite el acceso a personal autorizado. | **Aplica** | \* Se tiene un perímetro de seguridad externo y se tienen definidas áreas seguras internas, como: DataCenter, Bioterio, planta de sueros, laboratorios en general, COE Centro operativo de emergencias, Tesorería y almacén los cuales cuentan con controles de acceso específicos gestionados por cada área. \* Se cuenta con un servicio vigilancia privada, que consta de 8 guardas en sede principal, 1 en la hacienda, 1 en armero (finca). \* También se cuenta con circuito cerrado de televisión, que consta de 78 cámaras, el cual es del tercero, ellos custodian los backups, y el software de registro de acceso. \* En la entrada se cuenta con Talanqueras que son del instituto, para acceso de funcionarios, los contratistas no cuenta con tarjetas de acceso. \* El archivo central tiene servicio de vigilancia, no tiene circuito cerrado de televisión, el archivo se encuentra bajo llave, está ubicado en una zona insegura, ha tenido problemas de goteras. | **SI** | Administrado | 80% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| 11.1.3 | Seguridad de oficinas, salones e instalaciones | Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones. | **Aplica** | \* Se tienen definidas áreas seguras internas, como: DataCenter, Bioterio, planta de sueros, laboratorios en general, COE Centro operativo de emergencias, Tesorería y almacén los cuales cuentan con controles de acceso específicos gestionados por cada área. \* El resto cuenta con llave para el control de acceso. | **SI** | Administrado | 80% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| 11.1.4 | Protección contra amenazas externas y ambientales | Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | **Aplica** | \* El INS cuenta con plantas y UPS que entran en funcionamiento ante la ausencia de energía eléctrica. \*Adicionalmente cuenta con planes de emergencia, así como con un programa de calidad de vertimientos, uso de agua, gestión de residuos, uso racional de energía, aire limpia, protección fauna y flora, control de plagas. \* Actualmente no cuenta con un DataCenter alterno, ni un centro alterno de operaciones. | **PARCIAL** | Repetible | 40% | Se recomienda que se implementen los controles necesarios para mitigar incendios, inundaciones, así como aquellos que le permitan al INS estar preparado contra desastres naturales, como: plan de recuperación de desastre tecnológicos, plan de continuidad del negocio y plan de emergencias. |  |
| 11.1.5 | Trabajo en áreas seguras | Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. | **Aplica** | \* Se tienen definidos procedimientos para el acceso a áreas seguras como: DataCenter, Bioterio, planta de sueros, laboratorios en general, COE Centro operativo de emergencias, los cuales están gestionados por cada área. \* Existen otras zonas seguras que no tienen definido dichos procedimientos. | **PARCIAL** | Repetible | 40% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| 11.1.6 | Áreas de despacho y carga | Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | **Aplica** | Las áreas de despacho y carga son controladas por el servicio de vigilancia privada y el grupo de instalaciones | **SI** | Administrado | 80% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| **11.2** | **Equipos** | | | | | | **51%** |  |  |
|  | Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. | | | | | |  |  |  |
| 11.2.1 | Ubicación y protección de los equipos | Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, y las posibilidades de acceso no autorizado. | **Aplica** | \* La mayoría de los equipos asignados a los funcionarios y contratistas son equipos de escritorio, los cuales no tienen guaya para prevenir robos. \* Por otra parte los servidores se encuentran ubicados en el DataCenter que es un área segura con control de acceso. | **PARCIAL** | Administrado | 80% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| 11.2.2 | Servicios de suministro | Los equipos deben estar protegidos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | **Aplica** | \* El INS cuenta con plantas y UPS que entran en funcionamiento ante la ausencia de energía eléctrica. \* El DataCenter actualmente tiene problemas con el aire acondicionado y con el sistema contraincendios. \* El DataCenter, tiene control de acceso con tarjeta y huella (formato de ingreso), no se tienen cámaras. \* Única acometida eléctrica con circuitos eléctricos independientes. | **PARCIAL** | Repetible | 40% | Se deben definir políticas donde se establezca que elementos prioritarios, como: Aires acondicionados, plantas eléctricas, UPS, sistema contra incendios cuenten con un plan de mantenimiento preventivo y correctivo adecuado que garanticen una operacional apropiada de dichos elementos. |  |
| 11.2.3 | Seguridad del cableado | El cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a los servicios de información debe ser protegido contra interceptación, interferencia o daño. | **Aplica** | \* Cableado categoría 6a \* !3 centros de cableado con acceso por llave \* Se tiene diagrama de red \* Toda el cableado se encuentra protegido con canaletas \* La red es certificada \* Los puntos de red distribuidos por las sedes, permiten la conexión a la red y salida a internet ya que entregan direccionamiento por DHCP. \* Las únicas Ips fijas son para usuarios que se conectan por VPN y para impresoras. \* La red se encuentra segmentada pero no cuenta con controles adicionales. | **PARCIAL** | Inicial | 20% | Se recomienda que los puntos de red cuenten con controles de acceso a la red adecuados. |  |
| 11.2.4 | Mantenimiento de equipos | Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. | **Aplica** | \* Se realizan mantenimientos preventivos y correctivos de 1 a 2 veces al año \* Los equipos son del INS \* Las garantías salen del INS, se saca backup, pero no se formatea el equipo. | **PARCIAL** | Inicial | 20% | Se deben definir políticas donde se establezca la periodicidad del mantenimiento a equipos de cómputo. |  |
| 11.2.5 | Retiro de activos | Los equipos, información o software no se deben retirar de su sitio sin autorización previa. | **Aplica** | \* Todos los equipos que se van a retirar requieren autorización del jefe directo y del supervisor de vigilancia. \* No se tienen controles a nivel de Discos duros y USB | **PARCIAL** | Administrado | 80% | Se recomienda revisar los controles implementados para garantizar el acceso seguro a las instalaciones únicamente por el personal autorizado, dejando registro de dicho acceso. |  |
| 11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. | **Aplica** | Los equipos que salen de las oficinas no tienen controles de seguridad como cifrado disco duro, solo cuenta con el usuario de dominio, antivirus Kaspersky y conexión por VPNs | **PARCIAL** | Inicial | 20% | Se recomienda implementar soluciones de cifrado para equipos que salen de las instalaciones del INS. |  |
| 11.2.7 | Eliminación segura o reutilización de equipos | Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato sensible o software licenciado haya sido eliminado o sobrescrito en forma segura antes de su eliminación o reutilización. | **Aplica** | \* Los equipos se devuelven a almacén para ser reasignados, el usuario que lo tenía asignado autoriza el formateo. \* Se puede hacer traslado del equipo entre funcionarios, en cuyo caso no se formatea el equipo. \* La mesa de ayuda da el concepto de obsolescencia tecnológica y almacén llama al Martillo, para hacer la disposición segura del equipo. | **PARCIAL** | Definido | 60% | Formalizar políticas de eliminación o reutilización de equipos de cómputo. |  |
| 11.2.8 | Equipos sin supervisión de los usuarios | Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada. | **Aplica** | Se tiene un bloqueo de pantalla que se activa luego de 10 minutos de inactividad. | **PARCIAL** | Administrado | 80% | Implementar políticas de bloqueo de equipos ante la inactividad en estos. |  |
| 11.2.9 | Política de escritorio limpio y pantalla limpia | Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información. | **Aplica** | Se tiene política de pantalla limpia aplicada a través de dominio. No se tiene políticas para que los funcionarios mantengan el escritorio de trabajo sin documentos que puedan ser confidenciales a la mano. | **PARCIAL** | Definido | 60% | Hacer conciencia en el personal administrativo sobre las ventajas de mantener el puesto de trabajo limpio. |  |
| **12** | **SEGURIDAD DE LAS OPERACIONES** | | | | | | **72%** |  |  |
| **12.1** | **Procedimientos operacionales y responsabilidades** | | | | | | **55%** |  |  |
|  | Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. | | | | | |  |  |  |
| 12.1.1 | Procedimientos de operación documentados | Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan. | **Aplica** | La OTIC cuenta con una carpeta compartida en la que se mantiene un inventario de sistemas y la documentación de configuración de servicios. | **SI** | Administrado | 80% | Desarrollar y formalizar procedimientos operativos de la plataforma tecnológica |  |
| 12.1.2 | Gestión de cambios | Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. | **Aplica** | Se notifica a los usuarios sobre cambios que se realizan en los sistemas, pero no se documenta los cambios. Se notifica por correo electrónico si el cambio fue exitoso. Los cambios en las plataformas se realizan los viernes en la noche. Algunos servicios tecnológicos del INS son servicio 7x24. | **PARCIAL** | Repetible | 40% | Desarrollar y formalizar el procedimiento de gestión de cambios |  |
| 12.1.3 | Gestión de capacidad | Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema. | **Aplica** | \* Se revisa manualmente el Estatus del sistema de almacenamiento (Pure Storage), el cual tiene una capacidad de 16Tb, actualmente tiene un uso del 20%, para correo electrónico, máquinas virtuales y bases de datos \* No se hace gestión de capacidad | **PARCIAL** | Inicial | 20% | Desarrollar políticas de gestión de la capacidad de la plataforma tecnológica |  |
| 12.1.4 | Separación de los ambientes de desarrollo, ensayos, y operacionales | Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional. | **Aplica** | \* Se tienen ambientes de desarrollo en los equipos de los desarrolladores, ambiente de pruebas y de producción, mediante maquinas separadas para cada ambiente.  \* En SharePoint se hace mediante la creación de ambientes para pruebas y producción. | **PARCIAL** | Administrado | 80% | Separar los ambientes de producción, pruebas y desarrollo tanto a nivel lógico como físico. |  |
| **12.2** | **Protección contra códigos maliciosos** | | | | | | **80%** |  |  |
|  | Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. | | | | | |  |  |  |
| 12.2.1 | Controles contra códigos maliciosos | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | **Aplica** | \* Se cuenta con firewall perimetral en alta disponibilidad. \* En los equipos de escritorio se cuenta con antivirus Kaspersky que tiene módulos de (aplicación, mail, file server) \* También se cuenta con antispam marca Sofos, el cual permite la administración de listas blancas y listas negras, así como el análisis de adjuntos | **SI** | Administrado | 80% | Garantizar la actualización permanente de la solución de antivirus. Validar otras soluciones, como aquellas que permiten una protección avanzada ante amenazas |  |
| **12.3** | **Copias de respaldo** | | | | | | **20%** |  |  |
|  | Objetivo: Proteger contra la pérdida de datos. | | | | | |  |  |  |
| 12.3.1 | Copias de respaldo de la información | Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordada. | **Aplica** | \* Los backups se realizan por los mismos funcionarios en medios removibles asignados por la OTI o personales \* Se tienen definidos tiempos de almacenamiento de backups \* Se tienen Backups digitales a disco y en Asure \* No se hace restauración periódica de backups \* Se tienen políticas de backups definidas en procedimientos | **PARCIAL** | Inicial | 20% | Desarrollar políticas de restauración de backups. |  |
| **12.4** | **Registro y seguimiento** | | | | | | **80%** |  |  |
|  | Objetivo: Registrar eventos y generar evidencia. | | | | | |  |  |  |
| 12.4.1 | Registro de eventos | Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | **Aplica** | \* Se tiene logs de eventos, de sistema, de aplicación. \* Todos los logs de auditoria están habilitados \* Los logs se conservan por 6 meses \* No se tiene backups de los logs se van reemplazando automáticamente. | **PARCIAL** | Administrado | 80% | Definir políticas para la conservación y revisión de registros |  |
| 12.4.2 | Protección de la información de registro | Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado. | **Aplica** | Solo el administrador del dominio puede borrar registros, actualmente el único administrador es la ing. Johana | **SI** | Administrado | 80% | Definir políticas para la conservación y revisión de registros |  |
| 12.4.3 | Registros del administrador y del operador | Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad. | **Aplica** | Se tienen logs de los cambios que realizan los administradores en los sistemas. | **SI** | Administrado | 80% | Definir políticas para la conservación y revisión de registros |  |
| 12.4.4 | Sincronización de relojes | Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. | **Aplica** | \* Se cuenta con la herramienta NetTime para la sincronización de la hora legal colombiana en todos los servidores. \* Los equipos de usuario sincronizan la hora contra el controlador de dominio. \* Los dispositivos de red como Firewall y Switches no tienen dicha configuración. | **PARCIAL** | Administrado | 80% | Garantizar que todos los equipos conectados a la red se encuentren sincronizando relojes con el controlador de dominio. |  |
| **12.5** | **Control de software operacional** | | | | | | **100%** |  |  |
|  | Objetivo: Asegurarse de la integridad de los sistemas operacionales. | | | | | |  |  |  |
| 12.5.1 | Instalación de software en sistemas operativos | Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. | **Aplica** | Los usuarios no tienen permitida la instalación de software sin la autorización de la mesa de ayuda o de la OTIC | **SI** | Optimizado | 100% | Realizar seguimiento a la instalación de software no autorizado en equipos de la red |  |
| **12.6** | **Gestión de la vulnerabilidad técnica** | | | | | | **90%** |  |  |
|  | Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas. | | | | | |  |  |  |
| 12.6.1 | Gestión de las vulnerabilidades técnicas | Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | **Aplica** | \* El último análisis de vulnerabilidades se realizó en el 2014 por parte de la OTIC \* Los análisis de vulnerabilidades se hacen cada vez que se contrata a un tercero, año 2014 y 2018 y se hacen únicamente para servidores de función critica. \* Se realiza actualización de los sistemas operativos mediante WSUS. \* También se gestionan posibles incidentes según boletines de COLCERT \* Algunos proveedores como los del firewall, gestionan las vulnerabilidades proactivamente. | **PARCIAL** | Administrado | 80% | Realizar análisis de vulnerabilidades periódicos |  |
| 12.6.2 | Restricciones sobre la instalación de software | Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios. | **Aplica** | Los usuarios no tienen permitida la instalación de software sin la autorización de la mesa de ayuda o de la OTIC | **SI** | Optimizado | 100% | Realizar seguimiento a la instalación de software no autorizado en equipos de la red |  |
| **12.7** | **Consideraciones de auditoría de los sistemas de información** | | | | | | **80%** |  |  |
|  | Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos. | | | | | |  |  |  |
| 12.7.1 | Controles de auditoría de los sistemas de información | Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. | **Aplica** | \* Se tiene logs de eventos, de sistema, de aplicación. \* Todos los logs de auditoria están habilitados \* Los logs se conservan por 6 meses \* No se tiene backups de los logs se van reemplazando automáticamente. | **PARCIAL** | Administrado | 80% | Desarrollar políticas relacionadas con registros de auditoria en la plataforma tecnológica del INS |  |
| **13** | **SEGURIDAD DE LAS COMUNICACIONES** | | | | | | **76%** |  |  |
| **13.1** | **Gestión de seguridad de redes** | | | | | | **67%** |  |  |
|  | Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. | | | | | |  |  |  |
| 13.1.1 | Controles de redes | Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones. | **Aplica** | \* Se cuenta con firewall perimetral únicamente \* La red se encuentra segmentada por: DMZ, usuarios y proveedores \* No se tienen controles adicionales en la red interna. | **PARCIAL** | Definido | 60% | Revisar si se hace necesaria la adquisición de otras soluciones de seguridad perimetral, como: IPS, IDS, firewall de aplicaciones, firewall de bases de datos, etc. |  |
| 13.1.2 | Seguridad de los servicios de red | Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente. | **Aplica** | \* Se cuenta con firewall perimetral únicamente \* La red se encuentra segmentada por: DMZ, usuarios y proveedores. \* Se cuenta con redes WIFI con acceso según el perfil de los funcionarios. (Snake Red, Dirección General, Dirección COE, Outgrot, Invitados, Internet wifi para la gente) la única red que no llega a la red de servidores es la red de internet para le gente. \* Se tienen políticas de acceso a redes sociales en el horario de 12 a 2. \* El acceso a YouTube se encuentra limitado por el tamaño del canal. \* Se puede monitorear las paginas a las que acceden los funcionarios. \* Se cuenta con bloqueos de correos masivos. \* Se tienen FTP internos y externos (dirección de vigilancia) \* Se cuenta con Sitios de colaboración en SharePoint (publicar eventos, informes de gestión) \* Se tiene almacenamiento de SAN \* Se cuenta con una solución para el monitoreo de la red Operation Manager. \* No se tienen controles adicionales en la red interna. \* No se tienen otras soluciones seguridad perimetral como IDS, IPS \* No se tienen firewall de aplicaciones o de bases de datos | **PARCIAL** | Definido | 60% | Revisar si se hace necesaria la adquisición de otras soluciones de seguridad perimetral, como: IPS, IDS, firewall de aplicaciones, firewall de bases de datos, etc. |  |
| 13.1.3 | Separación en las redes | Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. | **Aplica** | La red se encuentra segmentada por: VLAN para bróker, telefonía, wifi, bloque A, bloque B, DataCenter, pero no se tiene controles entre dichas redes | **SI** | Administrado | 80% | Se deben implementar controles entre los segmentos de red, para asegurar que solo se permiten los accesos autorizados |  |
| **13.2** | **Transferencia de información** | | | | | | **85%** |  |  |
|  | Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. | | | | | |  |  |  |
| 13.2.1 | Políticas y procedimientos de transferencia de información | Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. | **Aplica** | \* En el comité propiedad intelectual se tratan temas de intercambio de información entre convenios. \* No existen políticas, ni procedimientos de transferencia de información segura. | **PARCIAL** | Administrado | 80% | Definir políticas y procedimientos para la transferencia de información |  |
| 13.2.2 | Acuerdos sobre transferencia de información | Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas. | **Aplica** | \* En el comité de propiedad intelectual se definen cláusulas de transferencia de información para algunos convenios específicos. \* La información de convenios se transfiere mediante el protocolo FTP. Algunos entes que acceden a dicha información son el DANE, MINSALUD, Superintendencia de servicios públicos domiciliarios. | **PARCIAL** | Administrado | 80% | Definir acuerdos para la transferencia de información con proveedores. |  |
| 13.2.3 | Mensajes electrónicos | Se debe proteger apropiadamente la información incluida en los mensajes electrónicos. | **Aplica** | \* El servicio de correo electrónico se tiene implementado sobre Exchange 2013. \* Se tienen adicionalmente 200 buzones con office 365. \* Se cuenta con una solución de antispam SOPHOS \* Sobre el Exchange no existen controles que garanticen la confidencialidad de los correos electrónicos enviados. \* Se cuenta con bloqueos de envíos masivos. | **PARCIAL** | Administrado | 80% | Definir políticas para el uso adecuado del servicio de correo electrónico. |  |
| 13.2.4 | Acuerdos de confidencialidad o de no divulgación | Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | **Aplica** | \* Se tienen acuerdos de confidencialidad con funcionarios y contratistas. \* Adicionalmente en el comité de propiedad intelectual se definen acuerdos, procedimientos, y aprobaciones en materia de propiedad intelectual. | **SI** | Optimizado | 100% | Revisar la pertinencia de las cláusulas de confidencialidad en cargos críticos del INS y ajustarlas |  |
| **14** | **ADQUISICIÓN, DESARROLLO Y MANTENIEMIENTO DE SISTEMAS** | | | | | | **0%** |  |  |
| **14.1** | **Requisitos de seguridad de los sistemas de información** | | | | | | **0%** |  |  |
|  | Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas. | | | | | |  |  |  |
| 14.1.1 | Análisis y especificación de los requisitos de seguridad de la información | Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. | **Aplica** | \* Se incluye un módulo de administración de usuarios y perfiles, autenticación, auditoría.  \* Se cifran las contraseñas.  \* No se incluye modelamiento de amenazas, casos de abuso, revisión de código para desarrollos externos, análisis de riesgos. | **PARCIAL** | Definido | 60% | Definir requisitos de seguridad de la información para el desarrollo de sistemas de información |  |
| 14.1.2 | Seguridad de los servicios de las aplicaciones en redes públicas | La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas. | **Aplica** | \* No se realiza análisis de vulnerabilidades, de hardening. \* No se cuenta con guías de aseguramiento.  \* Se hace parcheo  \* Implementación de certificado SSL  \* Aseguramiento a nivel de red. | **PARCIAL** | Definido | 60% | Revisar la seguridad de las aplicaciones en redes publicas |  |
| 14.1.3 | Protección de transacciones de servicios de aplicaciones | La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada. | **Aplica** | \* Se controlan las comunicaciones en el FW, se utiliza un pool de puertos dinámicos. | **NO** | Inexistente | 0% | Revisar la seguridad de las aplicaciones en redes publicas |  |
| **14.2** | **Seguridad en los procesos de desarrollo y de soporte** | | | | | | **0%** |  |  |
|  | Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información. | | | | | |  |  |  |
| 14.2.1 | Política de desarrollo seguro | Reglas para el desarrollo de software y sistemas deben establecerse y aplicarse a los desarrollos dentro de la organización. | **Aplica** | \* No existe política de desarrollo seguro. | **NO** | Inexistente | 0% | Definir políticas de desarrollo seguro |  |
| 14.2.2 | Procedimientos de control de cambios en sistemas | Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | **Aplica** | \* Se tiene un formato de cambios, sin embargo, no se cuenta con aprobación de cambios, no incluye rollback, ni está documentado el procedimiento. | **PARCIAL** | Inicial | 20% | Definir procedimientos de control de cambios en sistemas |  |
| 14.2.3 | Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones | Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales. | **Aplica** | \* No se realizan pruebas de seguridad después de cambios. | **NO** | Inexistente | 0% | Definir procedimientos para la revisión técnica de aplicaciones después de cambios |  |
| 14.2.4 | Restricciones sobre cambios en los paquetes de software | Se deben desalentar las modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deben controlar estrictamente. | **Aplica** | \* No hay un procedimiento documentado de gestión de cambios. | **NO** | Inexistente | 0% | Definir procedimientos de control de cambios en sistemas |  |
| 14.2.5 | Principio de construcción de los sistemas seguros | Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. | **Aplica** | \* No existe política de desarrollo seguro. | **NO** | Inexistente | 0% | Definir políticas de desarrollo seguro |  |
| 14.2.6 | Ambiente de desarrollo seguro | Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. | **Aplica** | \* Los ambientes de desarrollo están en los PC de los desarrolladores. No hay servidores como tal.  \* Existen servidores de pruebas. | **PARCIAL** | Inicial | 20% | Separar los ambientes de producción, pruebas y desarrollo tanto a nivel lógico como físico. |  |
| 14.2.7 | Desarrollo contratado externamente | La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratada. | **Aplica** | \* Las direcciones contratan externamente desarrollos. \* No hay una política de desarrollo con terceros. \* Desde OTIC se les suministra la metodología de desarrollo para que la sigan. | **PARCIAL** | Inicial | 20% | Definir políticas para la supervisión y el seguimiento de los proveedores de tecnología |  |
| 14.2.8 | Ensayos de seguridad de sistemas | Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad. | **Aplica** | No se hacen pruebas a los controles de seguridad. | **NO** | Inexistente | 0% | Desarrollar políticas de seguridad de la información para la realización de pruebas y aceptación de los sistemas de información |  |
| 14.2.9 | Ensayo de aceptación de sistemas | Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de ensayo y criterios relacionados. | **Aplica** | No se hacen pruebas a los controles de seguridad. | **NO** | Inexistente | 0% | Desarrollar políticas de seguridad de la información para la realización de pruebas y aceptación de los sistemas de información |  |
| **14.3** | **Datos de ensayo** | | | | | | **0%** |  |  |
|  | Objetivo: Asegurar la protección de los datos usados para ensayos. | | | | | |  |  |  |
| 14.3.1 | Protección de los datos de ensayo | Los datos de ensayo se deben seleccionar cuidadosamente, proteger y controlar. | **Aplica** | No se cuenta con un procedimiento de enmascaramiento o anonimización de datos. | **NO** | Inexistente | 0% | Anonimizar los datos de prueba |  |
| **15** | **RELACIONES CON LOS PROVEEDORES** | | | | | | **38%** |  |  |
| **15.1** | **Seguridad de la información en las relaciones con los proveedores** | | | | | | **7%** |  |  |
|  | Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores. | | | | | |  |  |  |
| 15.1.1 | Política de seguridad de la información para las relaciones con proveedores | Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar. | **Aplica** | No se cuenta con una política de seguridad de la información para las relaciones con los proveedores | **PARCIAL** | Inicial | 20% | Desarrollar políticas de seguridad de la información para las relaciones con proveedores |  |
| 15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | **Aplica** | La política de seguridad actualmente se encuentra publicada en la Intranet y no en un lugar de fácil acceso para proveedores. | **NO** | Inexistente | 0% | Desarrollar políticas de seguridad de la información para las relaciones con proveedores |  |
| 15.1.3 | Cadena de suministro de tecnología de información y comunicación | Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnologías de información y las comunicaciones. | **Aplica** | No se tiene acuerdos con proveedores para tratar los riesgos de seguridad de la información asociados a los servicios contratados | **NO** | Inexistente | 0% | Desarrollar políticas de seguridad de la información para las relaciones con proveedores |  |
| **15.2** | **Gestión de la prestación de servicios de proveedores** | | | | | | **70%** |  |  |
|  | Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores. | | | | | |  |  |  |
| 15.2.1 | Seguimiento y revisión de los servicios de los proveedores | Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. | **Aplica** | Se hacen seguimientos por parte del supervisor del contrato, pero no se hacen auditorias | **PARCIAL** | Administrado | 80% | Desarrollar políticas de seguridad de la información para las relaciones con proveedores, que incluya la revisión de los servicios de los proveedores |  |
| 15.2.2 | Gestión de cambios a los servicios de los proveedores | Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos. | **Aplica** | \* La gestión de cambios a los servicios de los proveedores la realiza gestión contractual. \* Se tienen contratos con proveedores tecnológicos como Asure y el canal de internet, pero no se tienen dichos controles estipulados. | **PARCIAL** | Definido | 60% | Desarrollar políticas de seguridad de la información para las relaciones con proveedores, que permitan gestionar adecuadamente los cambios a los servicios de los proveedores |  |
| **16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | | | | | | **20%** |  |  |
| **16.1** | **Gestión de incidentes y mejoras en la seguridad de la información** | | | | | | **20%** |  |  |
|  | Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades. | | | | | |  |  |  |
| 16.1.1 | Responsabilidades y procedimientos | Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| 16.1.2 | Reporte de eventos de seguridad de la información | Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| 16.1.3 | Reporte de debilidades de seguridad de la información | Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| 16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos. | Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| 16.1.5 | Respuesta a incidentes de seguridad de la información | Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| 16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| 16.1.7 | Recolección de evidencia | La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. | **Aplica** | \* No se cuenta con un procedimiento formal para la gestión de incidentes en seguridad de la información \* Se reacción ante el incidente de forma reactiva. | **PARCIAL** | Inicial | 20% | Definir un proceso para la gestión de incidentes de seguridad de la información |  |
| **17** | **ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO** | | | | | | **37%** |  |  |
| **17.1** | **Continuidad de seguridad de la información** | | | | | | **33%** |  |  |
|  | Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización. | | | | | |  |  |  |
| 17.1.1 | Planificación de la continuidad de la seguridad de la información | La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. | **Aplica** | \* No se cuenta con DataCenter alterno. \* Se tiene alta disponibilidad de las plataformas y las soluciones más críticas, como: - Se tiene el servicio SQL server en clúster - Se tiene el servicio de Exchange DAC alta disponibilidad (configuración manual) - Directorio activo en alta disponibilidad - Firewall en alta disponibilidad - Se tiene un Switch Core con fuente redundante - Se tienen 2 switches de SAN en alta disponibilidad \* Se cuenta con el servicio de Asure, para tener servidores en la nube, actualmente solo se tiene la aplicación de trasplantes, el cual cuenta con procedimiento para ponerlo en operación de ser necesario. \* No se tienen planes para garantizar la seguridad de la información ante un desastre o contingencia. | **PARCIAL** | Repetible | 40% | \* Validar cuales son los servicios que no se encuentran en alta disponibilidad y definir el plan de acción. \* Definir una política para la continuidad de la seguridad de la información |  |
| 17.1.2 | Implementación de la continuidad de la seguridad de la información | La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. | **Aplica** | \* No se cuenta con DataCenter alterno. \* Se tiene alta disponibilidad de las plataformas y las soluciones más críticas, como: - Se tiene el servicio SQL server en clúster - Se tiene el servicio de Exchange DAC alta disponibilidad (configuración manual) - Directorio activo en alta disponibilidad - Firewall en alta disponibilidad - Se tiene un Switch Core con fuente redundante - Se tienen 2 switches de SAN en alta disponibilidad \* Se cuenta con el servicio de Asure, para tener servidores en la nube, actualmente solo se tiene la aplicación de trasplantes, el cual cuenta con procedimiento para ponerlo en operación de ser necesario. \* No se tienen planes para garantizar la seguridad de la información ante un desastre o contingencia. | **PARCIAL** | Repetible | 40% | \* Validar cuales son los servicios que no se encuentran en alta disponibilidad y definir el plan de acción. \* Definir una política para la continuidad de la seguridad de la información |  |
| 17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. | **Aplica** | Se hacen pruebas a las plantas eléctricas y UPS para garantizar la continuidad de la energía eléctrica. | **PARCIAL** | Inicial | 20% | \* Validar cuales son los servicios que no se encuentran en alta disponibilidad y definir el plan de acción. \* Definir una política para la continuidad de la seguridad de la información |  |
| **17.2** | **Redundancias** | | | | | | **40%** |  |  |
|  | Objetivo: Asegurar de la disponibilidad de instalaciones de procesamiento de información. | | | | | |  |  |  |
| 17.2.1 | Disponibilidad de instalaciones de procesamiento de información. | Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | **Aplica** | \* No se cuenta con DataCenter alterno. \* Se tiene alta disponibilidad de las plataformas y las soluciones más críticas, como: - Se tiene el servicio SQL server en clúster - Se tiene el servicio de Exchange DAC alta disponibilidad (configuración manual) - Directorio activo en alta disponibilidad - Firewall en alta disponibilidad - Se tiene un Switch Core con fuente redundante - Se tienen 2 switches de SAN en alta disponibilidad \* Se cuenta con el servicio de Asure, para tener servidores en la nube, actualmente solo se tiene la aplicación de trasplantes, el cual cuenta con procedimiento para ponerlo en operación de ser necesario. \* No se tienen planes para garantizar la seguridad de la información ante un desastre o contingencia. | **PARCIAL** | Repetible | 40% | \* Validar cuales son los servicios que no se encuentran en alta disponibilidad y definir el plan de acción. \* Definir una política para la continuidad de la seguridad de la información |  |
| **18** | **CUMPLIMIENTO** | | | | | | **51%** |  |  |
| **18.1** | **Cumplimiento de requisitos legales y contractuales** | | | | | | **76%** |  |  |
|  | Objetivo: Evitar incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad. | | | | | |  |  |  |
| 18.1.1 | Identificación de la legislación aplicable y los requisitos contractuales | Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben identificar explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización. | **Aplica** | Se tienen identificados los decretos, leyes, circulares y acuerdos que le aplican a la institución en la página web de la institución. | **SI** | Administrado | 80% | Identificar los requisitos legales en materia de seguridad de la información que le aplican al INS y aplicarlos. |  |
| 18.1.2 | Derechos de propiedad intelectual | Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. | **Aplica** | \* Existe un comité propiedad intelectual, donde se trata este tema y se establecen acuerdos, clausulas y convenios. \* La OTIC adicionalmente cuenta con un acuerdo de propiedad intelectual para desarrolladores. | **SI** | Administrado | 80% | Definir procedimientos para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. |  |
| 18.1.3 | Protección de registros | Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislatorios, reglamentarios, contractuales y de negocio. | **Aplica** | Los registros físicos son custodiados por cada grupo de cada dirección. | **SI** | Administrado | 80% | Implementar controles para asegurar la protección adecuada de los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislatorios, reglamentarios, contractuales y de negocio. |  |
| 18.1.4 | Privacidad y protección de información de identificación personal (datos personales) | Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable. | **Aplica** | \* Actualmente se cuenta con una política de protección de datos personales. \* Se tienen formato de autorización de manejo de datos personales. \* Se tienen avisos en algunos sistemas de información publicados en internet, donde le indica al usuario que sus datos serán tratados conforme la Ley 1581. \* Faltan algunos mecanismos establecidos en la ley 1581, por lo que la consultoría que se está llevando a cabo incluye un diagnóstico y recomendaciones para dar cumplimiento con la Ley de protección de datos personales y sus correspondientes decretos. | **PARCIAL** | Definido | 60% | Fortalecer la protección de datos de personales, mediante la creación de un sistema de gestión |  |
| 18.1.5 | Reglamentación de controles criptográficos | Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | **Aplica** | Se usan certificados digitales los cuales dan cumplimiento con la legislación y reglamentación aplicable. | **SI** | Administrado | 80% | \* Se recomienda identificar todos los certificados y controles criptográficos que se utilizan en el INS \* Generar la política para el uso adecuado de controles criptográficos |  |
| **18.2** | **Revisiones de seguridad de la información** | | | | | | **27%** |  |  |
|  | Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales. | | | | | |  |  |  |
| 18.2.1 | Revisión independiente de la seguridad de la información | El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | **Aplica** | \* No se han realizado auditorías externas para revisar como se está gestionando la seguridad de la información en la entidad. \* Parte de la consultoría es llevar a cabo una auditoria que demuestre el nivel de cumplimiento y las opciones de mejora del SGSI en la entidad. | **NO** | Inexistente | 0% | Se debe realizar una revisión independiente de la seguridad de la información al menos una vez al año |  |
| 18.2.2 | Cumplimiento con las políticas y normas de seguridad | Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. | **Aplica** | Actualmente la entidad ha contratado la consultoría para dar cumplimiento al modelo de seguridad y privacidad de la información establecido por MINTIC, ya que se sabe que se requiere incrementar esfuerzos en este sentido. | **PARCIAL** | Inicial | 20% | Revisar con regularidad el cumplimiento del procesamiento y procedimientos de información con las políticas y normas de seguridad apropiadas. |  |
| 18.2.3 | Revisión del cumplimiento técnico | Los sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información. | **Aplica** | \* Los sistemas de información que son desarrollados en la OTIC, cumplen con mejores prácticas en materia de seguridad de la información. \* Por otra parte algunos sistemas específicos que han nacido como proyectos en cada dirección no cumplen con dichas prácticas, por lo que requieren ser revisados. | **PARCIAL** | Definido | 60% | Revisar con regularidad los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de la información. |  |