Plan de Seguridad y Privacidad 2022

Tabla de contenido

Contenido

1. INTRODUCCIÓN

Colombia a través del Ministerio de Tecnologías de la Información y las Comunicaciones-MINTIC ha desarrollado políticas en cuanto a gobierno digital se refiere, que permiten que tanto el estado colombiano como los ciudadanos puedan trabajar sobre una base de eficiencia, transparencia y accesibilidad y orientándose al cumplimiento de directrices nacionales e internacionales.

Para poder llevar a cabo el cumplimiento de dichas políticas, es necesario que desde la gestión interna de las entidades se comprenda a todo nivel, la importancia de los diferentes habilitadores transversales de la política de gobierno digital[1] en la consecución de los objetivos propuestos donde la tecnología aporta al cumplimiento estratégico de la misionalidad de estas y por ende de la definición de cronogramas que permitan implementar toda la arquitectura de trabajo sobre el que hacer de la Entidad.

En el presente documento, se pretenden abordar los conceptos generales y repasar los controles definidos por norma ISO 27000:2013, para poder definir un cronograma de trabajo, que permita la implementación de la seguridad de la información a partir de los diferentes controles, políticas, procedimientos, riesgos y la capacitación o concientización a todos y cada uno de los funcionarios y contratistas del Instituto Nacional de Salud.

[1] MINTIC, Modelo de Seguridad, Bogotá, 2018.

2. OBJETIVOS

Objetivo General

Generar un avance importante en la implementación del Modelo de Seguridad y Privacidad de la Información de la Entidad.

Objetivos Específicos

a. Definir un cronograma de actividades que permita trabajar sobre la mejora continua del Modelo de Seguridad y Privacidad de la Información del Instituto Nacional de Salud.
b. Monitorear el cumplimiento y avance de la implementación del Modelo de Seguridad y Privacidad de la Información.

3. ALCANCE

Teniendo como base la implementación del Sistema de Gestión de Seguridad de la información (SGSI), que viene implementando el Instituto Nacional de Salud, se traza el presente plan para la vigencia 2022, buscando que la elección de las actividades permita la mejora continua del sistema junto con un impacto mayor dentro de la Entidad y de las partes involucradas.

En este sentido, la consolidación de la seguridad de la información dentro de la Entidad a partir del fortalecimiento del SGSI, el cual tiene como objetivo primordial la protección de todos los activos de información, especialmente la información física y electrónica que la Entidad almacene produzca y gestione a través de la implementación de controles físicos y lógicos que estén apuntando al cumplimiento de los controles definidos en numerales de la norma ISO 27001:2013.

Así mismo, adelantar una gestión efectiva de riesgos y un proceso de mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales.

En ese sentido, el documento busca dar un marco de trabajo que permita planear la ejecución anualizada y pormenorizada de las actividades que se pretenden adelantar, no buscando ser una camisa de fuerza frente a los tiempos y prioridades, sino más bien, un elemento de control que permita buscar la efectividad de las actividades y que el impacto sea el óptimo frente a las actividades elegidas sobre la implementación del Sistema y sobre el que hacer de la Entidad.

4. CONCEPTOS TÉCNICOS

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

- Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

- CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.
- Causa: Factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- **Consecuencia:** Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.

- **Control:** Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por la entidad.

- **Gestión del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

- **ICC**: Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Integridad:** Propiedad de exactitud y completitud.

- **Línea estratégica:** Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.

- **Mapa de riesgos:** Documento con la información resultante de la gestión del riesgo.

- **Política de administración del riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.

- **Primera línea de defensa:** Personas que se encuentras a cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.

- **Probabilidad:** Posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

- **Riesgo de corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **Riesgos de cumplimiento:** Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- **Riesgo de imagen o reputacional:** Posibilidad de ocurrencia de un evento que afecten la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.

- **Riesgos de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.

- **Riesgos estratégicos:** Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización publica y por tanto impactan toda la entidad.

- **Riesgos financieros:** Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

- **Riesgos gerenciales:** Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

- **Riesgo inherente:** Riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **Riesgos operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.

- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

- **Riesgos tecnológicos:** Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

- **Segunda línea de defensa:** Personas que asisten y guían a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.)

- **Tercera línea de defensa:** Personas que provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos,

validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.

- **Tolerancia al riesgo:** Preparación de la organización o de la parte involucrada para soportar el riesgo después del tratamiento de este con el fin de lograr sus objetivos.

- **Tratamiento al riesgo:** Respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

- **Vulnerabilidad:** Debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

5. JUSTIFICACIÓN

De acuerdo con el desarrollo del Sistema de Gestión de Seguridad y Privacidad de la Información SGSI en el Instituto Nacional de Salud, se tiene la necesidad de definir este documento, que busca dar las pautas de desarrollo del SGSI durante el periodo 2022, buscando dar cumplimiento a la declaración de aplicabilidad definida dentro del sistema a partir del anexo A de la norma ISO 27001:2013.

6. ACTIVIDADES A DESARROLLAR

El Plan definido da cumplimiento a las actividades asociadas a la gestión del Sistema de Gestión de Seguridad de la Información.

El detalle de las actividades a realizar, tiempo de ejecución de estas, responsable y participantes, para adelantar la implementación de este plan se definen a continuación.

No	Actividad	Fecha de inicio	Fecha final	Producto o resultado esperado
1. Activos de información				
1.1	Actualización instrumentos de identificación de activos de información	Marzo	Julio	Instrumentos de identificación de activos de información
1.2	Actualización de Activos de información	Julio	Noviembre	Matrices de activos
2. Plan de concienciación en Seguridad y Privacidad de la Información				
2.1	Actualización del Plan de Concienciación en Seguridad y Privacidad	Enero	Febrero	Documento Plan de Concienciación en Seguridad y Privacidad
2.2	Ejecución del Plan de	Febrero	Diciembre	Informe de ejecución Plan de

No	Actividad	Fecha de inicio	Fecha final	Producto o resultado esperado
	Concienciación en Seguridad y Privacidad.			Concienciación en Seguridad y Privacidad
3. Requisitos Legales de Seguridad y Privacidad				
3.1	Revisión de Requisitos Legales de Seguridad y Privacidad	Abril	Agosto	Actas de reunión / correos electrónicos
4. Dominios de la Norma ISO 27001:2013				
4.1	Revisión de Manual y Políticas de Seguridad del Sistema de Gestión de Seguridad de la Información.	Enero	Marzo	Documento Manual y Políticas de Seguridad de la Información.
4.2	Revisión de los controles de la norma ISO 27001:2013	Mayo	Diciembre	Herramienta de medición y seguimiento de controles de la norma ISO 27001:2013
5. Gestión de Incidentes de Seguridad de la Información				
5.1	Atención de	Enero	Diciembre	Aplicativo para Incidentes de

No	Actividad	Fecha de inicio	Fecha final	Producto o resultado esperado
	Incidentes de Seguridad de la Información			Seguridad de la información.
6. Indicadores del Sistema de Gestión de Seguridad de la Información				
6.1	Provisión de información de los indicadores del Sistema de Gestión de Seguridad de la Información	Junio	Diciembre	Evidencia para evaluación de los indicadores