PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ELABORADO POR:
PROFESIONAL ESPECIALIZADO
OFICIAL DE SEGUIRIDAD DE LA INFORMACIÓN

GRUPO ÁREA GESTIÓN DE SISTEMAS

INSTITUTO NACIONAL DE CANCEROLOGÍA

2025-2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el Instituto Nacional de Cancerología (INC), las tecnologías de la información y comunicaciones (TIC) son vitales para optimizar nuestros procesos, pero su uso conlleva riesgos inherentes que pueden afectar la disponibilidad, privacidad e integridad de la información. Aunque contamos con un robusto Sistema de Gestión de Seguridad de la Información (SGSI) para mitigar estas amenazas, el factor humano sigue siendo el eslabón más vulnerable, siendo la causa principal de muchos incidentes por falta de conocimiento. Por ello, la sensibilización y capacitación del personal son cruciales para salvaguardar nuestros activos informáticos.

El contexto actual de ciberseguridad global es cada vez más complejo, con amenazas emergentes como el ransomware, el uso malicioso de la inteligencia artificial (IA) para robos de identidad y ataques sofisticados. Para enfrentar estos desafíos, el INC se alinea con las actualizaciones normativas como la ISO 27001:2022, que incorpora nuevos controles para abordar las amenazas actuales y reforzar la resiliencia, y la ISO/IEC 42001:2023 para la gestión responsable de sistemas de IA. Estas iniciativas, junto con nuestra consultoría de continuidad del negocio y los resultados de nuestra encuesta de seguridad digital 2024, son fundamentales para fortalecer nuestras estrategias de capacitación y asegurar que todo el personal del INC sea un pilar en la seguridad de la información.

2. OBJETIVO

Fortalecer la postura de seguridad y continuidad digital del INC mediante la sensibilización y capacitación del personal, asegurando la confidencialidad, integridad y disponibilidad de la información, la ciberseguridad, la resiliencia operativa y la protección de los datos personales de pacientes y colaboradores.

2.1. OBJETIVOS ESPECIFICOS

1. Fomentar una cultura de seguridad de la información transversal en el INC.
2. Garantizar que el personal comprenda la importancia de la información y los activos digitales del instituto.
3. Reducir la incidencia de brechas de seguridad y filtraciones de datos, incluyendo las amenazas emergentes potenciadas por IA generativa y ataques a la cadena de suministro.
4. Mejorar la capacidad de los usuarios para identificar, reportar y responder eficazmente a incidentes de seguridad.
5. Promover la aplicación de buenas prácticas de seguridad en todas las actividades laborales diarias, incluyendo el trabajo remoto y la telesalud.
6. Capacitar al personal para reconocer y neutralizar tácticas de ingeniería social y otros métodos de ataque comunes, especialmente los avanzados por IA.
7. Incrementar la conciencia del personal y los pacientes sobre el manejo de datos personales y la privacidad de la información
8. Asegurar la comprensión de los principios clave de la gestión de la IA según ISO 42001.

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

A continuación, se presenta un análisis tipo DOFA (debilidades, oportunidades, fortalezas y amenazas) identificado por el instituto con relación a la situación actual de capacitación y sensibilización en seguridad y continuidad digital.

FACTORES INTERNOS DEL INSTITUTO

DEBILIDADES (-)	
1	La entidad debe fortalecer los programas de divulgación y sensibilización a proveedores y terceros frente al SGSI, especialmente en el contexto de los riesgos de la cadena de suministro.
2	El impacto de las capacitaciones presenciales es bajo, debido a la baja asistencia a las mismas por parte del personal del INC
3	Alta rotación del personal trae como consecuencia la perdida de trasmisión de conocimiento en Seguridad.
4	El instituto adolece de seguimiento débil a los funcionarios y/o contratistas, proveedores y terceros frente al cumplimiento del plan de capacitación SGSI, debido a la supervisión descentralizada
5	Alta Rotación del personal operativo responsable de plataformas, debido a cambios de outsourcing y cambio de tecnologías de seguridad de la información
6	Resistencia al cambio y al control por parte de los usuarios, como se evidencia en un 5% que no utiliza contraseñas seguras y un 21% que no utiliza MFA en su cuenta de Microsoft 365.
7	Un 34% de los usuarios no mantiene su información completamente sincronizada y respaldada en OneDrive o SharePoint, lo que indica una brecha en la apropiación de buenas prácticas de respaldo.

FORTALEZAS (+)	
1	Personal calificado de seguridad, rigurosidad técnica y con habilidades de liderazgo.
2	Programas de sensibilización y transferencia de conocimiento actualizados e implementados.
3	Se actualizo la política de Seguridad de la información a la norma ISO27001:2013, y se implementó la política de Tratamiento de datos personales, incluyendo soporte para interoperabilidad de la historia clínica
4	Operación de SGSI basado en ciclo PHVA que promueve y gestiona la confidencialidad, Integridad y Disponibilidad de la información

FACTORES EXTERNOS AL INSTITUTO

AMENAZAS (-)	
1	Apropiarse de los cambios normativos y legislativos vigentes que afecten el SGSI y el SGIA (ISO 42001).
2	Evolución acelerada de ataques de seguridad encaminados hacia las plataformas en la nube.
3	Dar cumplimiento a los nuevos requerimientos de seguridad e interoperabilidad (Gobierno Digital y GOV.CO)
4	Nuevas amenazas de seguridad informática debido al Teletrabajo. Telemedicina, IOT y la inteligencia artificial, con el aumento de ataques de spear-phishing, falsificación de identidades y malware generados por IA.
5	El robo de identidad evolucionado, utilizando IA para evadir la verificación de identidad.
6	Baja apropiación de Proveedores de Sistemas Biomédicos frente a sus responsabilidades de seguridad debido a sus modelos de contratación, impactando la cadena de suministro y la ciberseguridad.
7	Ataques de ransomware que continúan intensificándose y apuntando a proveedores críticos, con el potencial de paralizar servicios.

OPORTUNIDADES (+)	
1	Aprender de los incidentes conocidos ocurridos en otras Entidades y Organizaciones del sector.
2	Mantener comunicación activa con Organismos o Entidades Externas frente a temas de Seguridad que permite ampliar el panorama y la visión para la Entidad.
3	Lograr que los objetivos de la Entidad se cumplan con un alto nivel de Seguridad en el manejo de la Información.
4	Colaborar con otras Entidades Públicas del sector que hayan adoptado la metodología MSPI e ISO 27001mediante la apropiación de una Cultura del

			SGSI, y, ahora, ISO 42001, mediante la apropiación de una Cultura del SGSI y SGIA.
5	Adecuaciones de redes y comunicaciones y seguridad para adopción de protocolo IPV6, y control de acceso a la red.	5	Implantación de Planes de Contingencia y transformación Digital
6	La entidad realiza seguimiento y monitoreo de plan de sensibilización de seguridad mediante encuesta anual para medir la efectividad y eficacia de este.	6	Aceleración de implantación de Telesalud y telemedicina e inteligencia artificial.
7	Actualizacion de Capacitación de seguridad de la información en Campus Virtual para inducción y reinducción de personal	7	Actualizaciones de la Norma Iso27001:2022 e Iso 27002:2022, enfocadas en la automatización y simplificación de la seguridad
8	Conciencia de la importancia de proteger la información confidencial (99%), con un Alto conocimiento de las políticas de seguridad de la información (91% de los encuestados)	8	La integración de la norma ISO/IEC 42001 para la gestión de sistemas de IA, permitiendo un desarrollo y uso responsable de la IA.

3.1. NORMATIVIDAD

ISO/IEC 42001:2023: "Tecnologías de la información - Inteligencia artificial - Sistema de gestión". Esta norma proporciona un marco para la gobernanza y gestión de riesgos de la IA a lo largo de su ciclo de vida, incluyendo estructuras de gobernanza, identificación y mitigación de riesgos, gestión de datos, transparencia y pautas éticas.

COMPES 4144 – Política Nacional de Inteligencia Artificial: formula una política nacional de Inteligencia Artificial cuyo objetivo es generar las capacidades para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de IA. Establece lineamientos de política que abordan riesgos y efectos no deseados relacionados con la IA, y políticas relacionadas con la seguridad y la confianza en la IA.

ISO/IEC 27001:2022: Esta norma define los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Presenta cambios importantes contra la versión de 2013, en la cantidad y la forma de clasificar los controles de seguridad, reduciendo a un total 93 controles, identificando 8 controles para personas, 14 controles físicos, 34 controles tecnológicos y 37 controles organizacionales. La norma atiende las necesidades de protección para las tendencias y nuevos enfoques de ciberseguridad: inteligencia de amenazas, seguridad de la información para el uso de servicios en la nube, automatización de la seguridad, preparación de las TIC para la continuidad del negocio, monitoreo de la seguridad física, gestión de la configuración, eliminación de información, enmascaramiento de datos, prevención de fuga de datos, actividades de monitoreo, filtrado Web y codificación segura.

Resolución 500 de 2021 de Mintic – por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad MSPI como habilitador de la Política de Gobierno Digital, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital

Conpes 3995 de 2020: Política de confianza de seguridad digital: Establece debilidades en las capacidades de orientación y educación en seguridad digital de los ciudadanos, del sector público y del sector privado

Guía #14: Plan de capacitación, sensibilización y comunicación de la seguridad de la información: Metodología de seguridad y privacidad de la información MINTIC Versión 1.0 de fecha 17/03/2016

ISO/IEC 27001:2013: Es la evolución certificable del código de buenas prácticas ISO 17799. Define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.

Decreto 612 de 2018: Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al plan de acción por parte de las entidades del estado.

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley Estatutaria 1581 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales

Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones

Circular externa 007 de 2018 Superfinanciera: Por la cual se Imparten instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.

3.2. DEFINICIONES TÉCNICAS

Acuerdo de Nivel de Servicio (SLA): Es un acuerdo entre un proveedor de servicios de TI y un cliente.

Advertencias de Seguridad: Es una lista de vulnerabilidades de seguridad conocidas y compiladas gracias a la aportación de proveedores de productos externos. La lista contiene instrucciones para medidas preventivas y para el manejo de infracciones de seguridad una vez ocurran.

Alerta de Seguridad: Se trata de una advertencia producida por la Gestión de la Seguridad de TI que generalmente se hace pública cuando se prevé el surgimiento de infracciones de seguridad o cuando ya están ocurriendo. Se busca asegurar que los usuarios y el personal de TI sean capaces de identificar cualquier ataque y de tomar medidas de precaución.

Ciberamenazas: Se refiere a aquellas actividades 'malignas' que tienen lugar en un entorno digital. El objetivo de estas ciberamenazas es el de comprometer la seguridad de un sistema alterando sus atributos de disponibilidad, integridad, confidencialidad autenticidad, no repudio entre otros.

Ciberseguridad: Es la práctica de la protección de los activos de información, la redes y sistemas de información, de los usuarios de dichos sistemas y de otras personas afectadas por las ciberamenazas.(amenazas digitales).

Cuestionario Encuesta: Se trata de un cuestionario que sirve de encuesta para medir la satisfacción del cliente.

Incidente: Un Incidente se define como una interrupción no planificada o como la reducción de calidad de algún servicio de TI.

Seguridad informática: se describe como la distinción táctica y operacional de la seguridad. Se trata de implementar medidas técnicas que preservaran las infraestructuras, plataformas, servicios de redes y

comunicaciones que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa.

Seguridad de la información: es la disciplina que se encarga de trazar las estrategias de seguridad y privacidad y los planes de acción para tratar los riesgos, bajo la normativa o las buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de activos de información.

SGSI: Sistema de Gestión de Seguridad de la Información

Inteligencia Artificial (IA): Sistemas que pueden aprender, razonar, percibir, comprender, generar o tomar decisiones de manera autónoma, a menudo con el objetivo de realizar tareas que típicamente requieren inteligencia humana.

Sistema de Gestión de Inteligencia Artificial (SGIA): Un conjunto de elementos interrelacionados o interactuantes de una organización destinados a establecer políticas y objetivos, así como procesos para lograr esos objetivos, en relación con el desarrollo, provisión o uso responsable de sistemas de IA, según ISO/IEC 42001.

Ciberresiliencia: La capacidad de una organización para anticipar, resistir, recuperarse y evolucionar ante las amenazas cibernéticas.

Análisis de impacto de Negocio (BIA) es un proceso crucial dentro de la gestión de la continuidad del negocio que identifica y evalúa el impacto potencial que la interrupción de las funciones y procesos críticos de una organización podría tener.

Plan de recuperación ante desastres (DRP):es un plan estratégico desarrollado para asegurar la rápida recuperación y continuidad de los sistemas de tecnología de la información (TI) y datos críticos después de un desastre o interrupción.

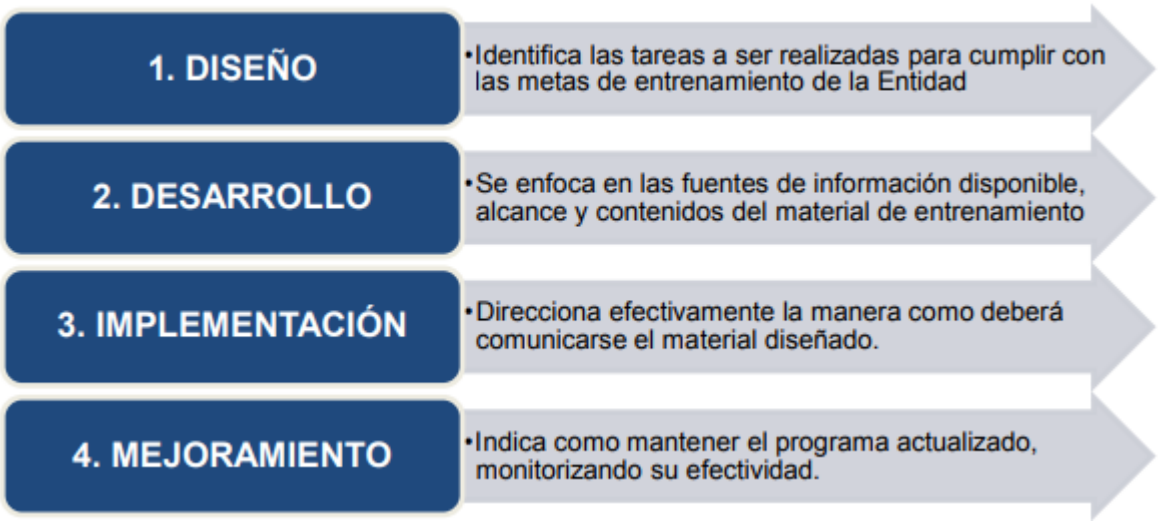
Plan de Continuidad del Negocio (PCN):es un conjunto integral de estrategias, procedimientos y recursos que una organización establece para asegurar que sus funciones y operaciones críticas puedan continuar o ser reanudadas rápidamente después de una interrupción, desastre o crisis.

Sistema de Gestión de Inteligencia Artificial (SGIA): Se refiere a un sistema que gestiona el uso responsable y ético de la Inteligencia Artificial (IA) dentro de la institución. Establecer directrices, controles y procesos para asegurar que los sistemas de IA sean transparentes, justos, seguros y cumplan con las regulaciones.

4. DESARROLLO DEL PLAN

4.1 METODOLOGÍA DE SENSIBILIZACIÓN Y CAPACITACIÓN

El plan de capacitación y sensibilización de seguridad y continuidad digital se lleva a cabo con base a las siguientes 4 fases:



4.1.1 FASE DE DISEÑO

La entidad cuenta con un programa de entrenamiento y sensibilización centralizado liderado por Grupo Area de Gestión y Desarrollo del Talento Humano. Este grupo delega al Grupo Área Gestión de sistemas la definición de estrategia y diseño del plan de capacitación y sensibilización en seguridad y continuidad digital.

El desarrollo y adaptación de los diseños, materiales para sensibilización y capacitación, y el despliegue se construyen en el Grupo Area gestión de sistemas con el apoyo de la Oficina asesora de planeación y sistemas (Oficina de comunicaciones), utilizando las estrategias de comunicación orientadas a cliente externo e interno implantadas para tal fin, como los son las que se identifican a continuación

- Correo electrónico institucional
- Sistema Multivisual y Auditorios
- Carteleras
- Boletines virtuales
- Lista de difusión
- Papel Tapiz de equipos.
- Microsoft Teams.
- Microsoft Forms.
- Campus Virtual.
- Sistema de envío de correos masivos (Microsoft).
- Plataforma de entrenamiento de ciberseguridad de proveedores de seguridad y de terceros.
- Plataforma de gamificación de ciberseguridad de la OSI (https://cyberscouts.osi.es/)
- Kit de Concienciación INCIBE (https://www.incibe.es/empresas/formacion/kit-concienciacion)

4.1.1.1 Identificación de necesidades

Se realiza un análisis del contexto interno y externo de la entidad, con relación a seguridad de la información, para identificar cuáles son los riesgos que pueden o afectan su capacidad para lograr los resultados esperados frente al SGSI; así como identificar cuáles son las necesidades y expectativas de las partes interesadas.

Las necesidades de capacitación y sensibilización se identifican utilizando las siguientes fuentes de información:

- La estructura organizacional.
- La verificación de los incidentes de seguridad de la información.
- Los informes de materialización de riesgos de seguridad digital.
- Los indicadores de seguridad digital en SIAPINC.
- Análisis de eventos de las herramientas de monitoreo y controles de seguridad.
- Amenazas identificadas para el sector salud en las mesas de trabajo de Ciberseguridad y ciberdefensa del Ministerio de Salud.
- Plan de capacitación y sensibilización ejecutado en la vigencia anterior.
- Informes de Amenazas Cibernéticas Informes 360 de seguridad INC de fabric Fortinet
- Informe de resultados de Encuesta de Satisfacción, uso y apropiación de tecnologías de la información y de seguridad
- Informes mensuales de Ciberseguridad Darktrace
- Informes de SOC Colsof y SOC Darktarce
- Informes y reportes anuales externos de encuestas y estado de la seguridad, publicados por fabricantes y aliados de segruidad informática.
- Boletines de Csirt Salud y de entidades aliadas.
- Reuniones de infraestructuras criticas cibernéticas de CCCOI

4.1.1.2 Identificación de roles involucrados

Se identifican entonces los siguientes roles y necesidades de sensibilización y capacitación en seguridad y continuidad digital.

PERFIL	ROL	NECESIDAD DE CAPACITACIÓN/SENSIBILIZACIÓN
DIRECTIVOS	• Propiciar el cumplimiento de las recomendaciones e instrucciones en materia de seguridad de la información en toda la institución • Autorizar a los colaboradores bajo su responsabilidad para participar de sensibilizaciones presenciales • Participar de acuerdo con su disponibilidad en las actividades presenciales del plan de sensibilización.	• Conocer y entender las leyes y directivas que forman la base del programa de seguridad SGSI y del SGIA. • Comprender el liderazgo y compromisos con la seguridad de la información y la gestión de IA (ISO 42001) que su rol tiene. • Sensibilización sobre manejo de datos personales y los impactos de la IA en la privacidad. • Actualización en modelos de ciberseguridad y ciberdefensa, incluyendo amenazas emergentes de IA y ataques a infraestructuras críticas. • Conocer funcionamiento y buenas prácticas de seguridad para sistemas de IA. • Actualización en las herramientas de seguridad informática, incluyendo las específicas para la protección de IA.

RESPONSABLES DE SEGURIDAD DE LA INFORMACION	• Diseñar, estructurar e implementar el plan de sensibilización en seguridad de la información, teniendo presente la misión de la Entidad y la relevancia que se busca para la cultura de la Entidad. • Identificar las necesidades y las prioridades que tenga la Entidad respecto al tema de sensibilización en seguridad de la información • Participar en el diseño de los materiales del programa de sensibilización • Propiciar el cumplimiento de las recomendaciones e instrucciones en materia de seguridad de la información que se divulguen dentro del marco del plan de sensibilización en seguridad de la información. • Consolidar las mediciones sobre la efectividad del programa de sensibilización, e Identificar oportunidades de mejora para la planificación, diseño, implementación y evaluación de este.	• Actualización en modelos de ciberseguridad y ciberdefensa. • Conocer funcionamiento y buenas prácticas de seguridad • Actualización en las herramientas de seguridad informática. • Actualización en modelos de ciberseguridad y ciberdefensa, incluyendo amenazas emergentes de IA y ataques a infraestructuras críticas. • Conocer funcionamiento y buenas prácticas de seguridad para sistemas de IA. • Actualización en las herramientas de seguridad informática, incluyendo las específicas para la protección de IA. • Actualización en normas de continuidad de negocio. • Conciencia sobre la importancia de la autenticación multifactorial (MFA) y la correcta gestión de contraseñas, dando ejemplo a los demás usuarios de la institución.
ADMINISTRADORES DE PLATAFORMAS Y SISTEMAS DE INFORMACION	• Participar en las actividades de sensibilización en seguridad de la información • Identificar los mecanismos que permitan implementar las recomendaciones y buenas prácticas del programa de sensibilización • Difundir entre los usuarios de los sistemas de información la adopción de las buenas prácticas de seguridad • Evaluar en conjunto con el responsable de proceso la efectividad de las actividades del programa de sensibilización en seguridad • Fomentar la implementación de las buenas prácticas de seguridad de la información propuestas por la campaña de sensibilización.	• Preparación y actualización a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del INC de manera apropiada. incluyendo la seguridad de los sistemas de IA. • Capacitación sobre protocolo IPV6 • Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales • Conocer sus responsabilidades con el SGSI y el SGIA. • Conocimientos avanzados sobre protección y administración de archivos en la nube, incluyendo la gestión de datos para sistemas de IA
LIDERES DE	• Fomentar la aplicación de las buenas	• Conocer y entender su

PROCESOS	prácticas de seguridad en sus grupos Area • Propiciar el cumplimiento de las recomendaciones e instrucciones en materia de seguridad de la información que se divulguen dentro del marco del plan de sensibilización en seguridad de la información. • Coordinar al interior de sus procesos la participación de los colaboradores en las actividades del plan de sensibilización. • Medir la eficacia de los resultados de las actividades de sensibilización en las que participan los colaboradores de sus procesos • Socializar riesgos de seguridad digital, ciberdefensa y ciberseguridad, y manejo de datos personales al interior de áreas.	compromiso y el de su grupo con las políticas de seguridad de la información y Política de tratamiento de datos personales • Conocer sus responsabilidades con el SGSI y el SGIA. • Sensibilización sobre tratamiento de datos personales, y la implicación de la IA en su manejo. • Sensibilización sobre controles de seguridad implantados para proteger la infraestructura que soporta cada proceso, incluyendo los sistemas de IA. • Asistir y participar en Sensibilización de riesgos de seguridad digital, y de seguridad de la informacion, con énfasis en los riesgos de la IA. • Conocimientos básicos sobre protección de archivos en la nube.
LIDERES INGRESO Y RETIRO DE PERSONAL	• Fomentar la aplicación de las buenas prácticas de seguridad • Propiciar la socialización y el cumplimiento de los procesos de ingreso y retiro de personal • Incluir al SGSI y la seguridad de la información en los planes de Inducción reinducción del instituto	• Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales • Conocer sus responsabilidades con el SGSI, y el SGIA. • Sensibilización sobre tratamiento de datos personales, considerando el ciclo de vida del personal y el uso de IA en la gestión de RRHH. • Sensibilización de riesgos de seguridad digital, y seguridad de la información. • Conocimientos básicos sobre protección de archivos en la nube.
PROVEEDORES Y TERCERIZADOS	• Fomentar la aplicación de las buenas prácticas de seguridad y tratamiento de datos. • Propiciar el cumplimiento de los procesos de ingreso y retiro de personal • Socializar cambios de controles y seguridad en sus plataformas administradas. • Propiciar el cumplimiento de las	• Deben tener un buen nivel de preparación y actualización a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del INC de manera apropiada, incluyendo la seguridad de los sistemas de IA. • Conocer funcionamiento y buenas prácticas de seguridad.

	recomendaciones e instrucciones en materia de seguridad de la información que se divulguen dentro del marco del plan de sensibilización en seguridad de la información.	• Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la información y Política de manejo de datos personales • Conocer sus responsabilidades con el SGSI y el SGIA. • Conocimientos avanzados sobre protección de archivos en la nube. Entender y cumplir con los requisitos de seguridad en la cadena de suministro de TI y IA.
• **USUARIOS FINALES** (Abarca a los usuarios finales internos del INC, a estudiantes, docentes e investigadores, y al personal de proveedores, externos y tercerizados.)	• Participar de todos los procesos de capacitación relacionados con seguridad de la información. • Propiciar el cumplimiento de las recomendaciones e instrucciones en materia de seguridad de la información que se divulguen dentro del marco del plan de sensibilización en seguridad de la información. • Contestar evaluaciones y encuestas generadas en el instituto sobre SI.	• Requieren de un alto grado de sensibilización sobre la seguridad de la información y las reglas de comportamiento adecuadas con los sistemas y servicios que tienen a disposición, de los derechos del ciudadano y sus deberes con el tratamiento de datos personales e información sensible en el INC. • Sensibilización de riesgos de seguridad digital, ciberseguridad, y seguridad de la información, incluyendo los ataques de ingeniería social avanzados por IA Conocimientos básicos sobre protección de archivos en la nube. • Fortalecer conocimientos avanzados en higiene de seguridad informática, escritorio limpio y pantalla limpia. • Conciencia sobre la importancia de la autenticación multifactor (MFA) y la correcta gestión de contraseñas, reforzando las buenas prácticas de los usuarios que ya las aplican. • Capacitación específica sobre el respaldo y sincronización de información en OneDrive y SharePoint para aumentar el porcentaje de usuarios que lo realizan completamente.
PACIENTE Y CIUDADANO	• Receptor de campañas de sensibilización a través de medios de comunicación del INC. • Ejercer sus derechos en el tratamiento de datos personales	• Se requiere crear conciencia en la ciudadanía sobre la necesidad del buen uso de las TIC, impulsar el conocimiento de los usuarios en seguridad digital, y conocer la percepción del usuario en cuanto

		a la confianza digital en los servicios y sistemas del instituto. • Sensibilizar sus derechos de datos personales y darle a conocer los canales de comunicación con el INC. • Conciencia sobre la protección de datos personales en el contexto de la telemedicina y el uso de la IA en la salud.

4.2.2 FASE DE DESARROLLO

4.2.2.1 Temáticas de capacitación y sensibilización

En la fase de desarrollo se definen las temáticas que debe cubrir el plan de capacitación y sensibilización en seguridad y continuidad digital, las cuales se presentan a continuación:

Conocimiento general del sistema de gestión de seguridad de la información (SGSI)

- Concepto de seguridad de la información
- Concepto Seguridad Informática
- Riesgos de seguridad de la información
- Cómo está estructurado el sistema de gestión de seguridad de la información y el SGIA
- Quienes son los actores del sistema de gestión de seguridad de la información y el SGIA
- Estrategia de Seguridad digital y estrategia de seguridad de IA.

Socializar avance sobre la estrategia de Seguridad de la información.

- Socialización de resultados del SGSI
- Socialización de Avances sobre controles de Ciberseguridad y cierre de brechas, incluyendo aquellas relacionadas con IA.

Conocimiento de las políticas de seguridad de la información

- Socialización de la política general de la seguridad de la información
- Capacitación registro activos de información, incluyendo activos de información relacionados con IA.
- Socializar actualización documental por cambio de la Norma ISO27001:2022, y y la implementación de controles de seguridad de la norma ISO 42001.
- Socializar enfoque y arquitectura de seguridad Zero Trust (Cero Confianza).

Conocimiento de las políticas de Tratamiento de datos Personales

- Capacitación de Derechos de los titulares y deberes de tratamiento de datos personales, con énfasis en el manejo de datos en sistemas de IA.
- Socialización de Procedimientos y canales de comunicación
- Socialización de actualización de la política de Tratamiento de datos personales.

Socialización de Controles

- Socialización de Manual de Política de Seguridad y privacidad
- Socialización de Manual de tratamiento de datos personales
- Socialización de manual DRP (Continuidad informática)
- Comunicaciones sobre Apagado y reinicio de equipos
- Socialización de Buenas prácticas de seguridad para dispositivos móviles
- Socialización Medidas de Seguridad para redes Sociales
- Socialización de Manual de Contraseñas y control de acceso
- Socializar técnicas criptográficas y manual de criptografía
- Socializar manual y gestión de capacidad.
- Socialización de metodología BIA, DRP y PCN
- Socializar controles de seguridad del SGIA
- Socialización de actualización de declaración de controles.

Amenazas informáticas

- Guía de ciberataques: Ataques a contraseñas
- Guía de ciberataques: Ataques por ingenieria social
- Guía de ciberataques: Ataques por ingeniería social 2
- Guía de ciberataques: Ataques a las conexiones -1
- Guía de ciberataques: Ataques a las conexiones – 2
- Guía de ciberataques: Ataques por malware 1
- Guía de ciberataques: Ataques por malware 2
- Guía de ciberataques INC - Buenas Prácticas e Higiene de seguridad
- Curso/Video Fortinet NSE1(Network Security associate). Sobre actores, ciberamenazas y consejos sobre cómo proteger la información
- Aprendiendo a identificar Fraudes Online
- Plataforma de gamificación de ciberseguridad de la OSI (https://cyberscouts.osi.es/)
- Adaptación de Kit de Concienciación INCIBE (https://www.incibe.es/empresas/formacion/kit-concienciacion)
- Sensibilización sobre ransomware y ataques a la cadena de suministro.
- Introducción a la seguridad de la IA: Uso adecuado y autorizado, identificación de sesgos, protección de modelos, seguridad de datos de entrenamiento.

Responsabilidades Disciplinarias

- Responsabilidades Sobre el cuidado y buen uso de elementos tecnológicos
- Faltas disciplinarias y seguridad de la información.

Materiales de sensibilización para la comunidad

- Guía de Ciberseguridad para Niños y Adultos
- Derechos y deberes de tratamiento de datos personales
- Información sobre la protección de la privacidad en el uso de servicios de telemedicina e IA en el INC.
- Materiales sobre la confianza digital y el uso responsable de la IA.

4.2.2.2 Materiales de sensibilización obligatorios

Se definen como materiales obligatorios dentro del periodo para todo el personal y colaboradores, los siguientes:

- Curso de Seguridad de inducción y reinducción
- Amenazas informáticas en el INC
- Guía de ciberataques INC - Buenas Prácticas e Higiene de seguridad
- Socialización de Manual de Política de Seguridad y privacidad
- Socialización de Manual de tratamiento de datos personales
- Socialización de manual DRP (Continuidad informática) y plan de continuidad de negocio. (BCP)
- Socialización introductoria sobre ISO 42001 y la gestión de seguridad de IA.

4.2.2.3 Desarrollo de Materiales de sensibilización y capacitación

Se relaciona el desarrollo y/o actualización del siguiente material de sensibilización para cubrir las temáticas del plan de capacitación del instituto:

MATERIAL	TEMATICA CUBIERTA	RESPONSABLE DESARROLLO	METODO DE DESPLIEGUE
Guía de ciberataques: Ataques a contraseñas	Ataques a contraseñas, y mejores prácticas. Socialización de Manual de contraseñas y control de acceso del INC	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Guía de ciberataques: Ataques por ingenieria social	Reconocer y actuar ante Ataques basados en el engaño y la manipulación del talento humano	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Guía de ciberataques: Ataques por ingeniería social 2	Reconocer y actuar ante Ataques basados en el engaño y la manipulación del talento humano	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Guía de ciberataques: Ataques a las conexiones -1	Reconocer y actuar ante ataques donde se utilizan software y herramientas con las que saltarse las medidas de seguridad e infectar o tomar control de dispositivos de usuarios.	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Guía de ciberataques: Ataques a las conexiones – 2	Reconocer y actuar ante ataques donde se utilizan software y herramientas con las que saltarse las medidas	Oficial de seguridad de la información	Correo electrónico o Dircom, Pagina web institucional

	de seguridad e infectar o tomar control de dispositivos de usuarios.	Oficina de comunicaciones	
Guía de ciberataques: Ataques por malware 1	Reconocer y actuar ante ataques de virus y malware	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Guía de ciberataques: Ataques por malware 2	Reconocer y actuar ante ataques de virus y malware	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Guía de ciberataques INC - Buenas Prácticas e Higiene de seguridad	Decálogo de buenas prácticas en ciberseguridad para mejorar la protección de los dispositivos y la seguridad de la información de los usuarios frente a los ciberataques	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom, Pagina web institucional
Sensibilización tratamiento de datos personales en el INC	Sensibilización sobre política y Tratamiento de datos personales en el INC	Oficial de seguridad de la información Oficina de comunicaciones	Correo electrónico o Dircom
Sensibilización tratamiento de datos personales en el INC	Sensibilización sobre derechos y deberes de tratamiento de datos personales	Oficial de seguridad de la información Oficina de comunicaciones	Presentación Feria de acreditación, o Dircom
Curso inducción reinducción en seguridad de la información	Sensibilización sobre de Políticas, y manuales de seguridad, tratamiento de datos personales y SGSI. Higiene de seguridad básica Pautas de comportamiento de usuarios para Seguridad de la información	Grupo área desarrollo Talento humano Oficial de seguridad de la información Grupo área Docencia	Campus Virtual

	Reconocimiento de tipo de atacantes		
Qué hacer ante la pérdida de dispositivos móviles	Amenazas informáticas Higiene de Seguridad	Oficial de Seguridad de la información Oficina Asesora de Comunicaciones	Correo electrónico - Dircom
Cartilla de gestión de riesgos	Sensibilización de gestión de riesgos, incluido seguridad digital y continuidad	Oficial de Seguridad de la información Profesional de Riesgo de Oficina de Planeación Oficina Asesora de Comunicaciones	Correo electrónico - Dircom
Cartillas de protocolos Ciberseguridad electoral	Sensibilización sobre medidas de prevención y ataques durante las jornadas relacionadas con temas electorales de 2023-2024	Oficial de Seguridad de la información Oficina Asesora de Comunicaciones	Correo electrónico - Dircom
Capacitación sobre el cuidado y buen uso de los equipos tecnológicos	Sensibilización sobre buen uso de los equipos tecnológicos, y su informacion contenida	Coordinadora Grupo Soporte hardware y redes Coordinador Control Interno Disciplinario	Capacitación TEAMS o Dircom
Capacitación Activos de Informacion	Sensibilización sobre el registro de activos de informacion, y el marcado y clasificación de activos de información.	Oficial de Seguridad de la información Coordinadora gestión Documental	Capacitación TEAMS
Capacitaciones sobre herramientas de ofimática	Sensibilización sobre manejo de herramientas de ofimática, para el manejo seguro de teleconferencias, y uso de nubes institucionales.	Coordinadora Grupo Soporte hardware y redes Especialista Office 365 -Outsourcing	Capacitación TEAMS

Boletines de seguridad	Boletines sobre amenazas de seguridad	Oficial de Seguridad de la información	Correo electrónico o Plataforma Mailrelay
Código general disciplinario	Sensibilización de disposiciones generales del código general disciplinario relacionadas con seguridad digital	Control interno Disciplinario	Dircom, Correo electrónico
Correo electrónico Certificado	Capacitación sobre servicio de correo electrónico certificado	Coordinadora grupo área gestión Documental Oficial de seguridad de la informacion	Microsoft Teams o dircom
Sensibilización en el manejo de documentos obsoletos	Sensibilización en el manejo de documentos obsoletos	Coordinadora grupo área gestión Documental Oficial de seguridad de la informacion	Presencial o Correo Electrónico o Oficio Siapinc
Sensibilización sobre líneas de defensa de riesgos	Sensibilización sobre modelo esquema líneas de defensa de riesgos	Líder oficina Control Interno Profesional de riesgos Oficial de seguridad de la informacion	Siapinc (Folleto)
Sensibilización sobre actualización documental de norma iso27001:2022	Socializar manual y gestión de capacidad.	Oficial de seguridad de la informacion	Teams, Dircom
Socialización de Manual DRP	Socializar manual de contingencia tecnología a skateholders	Oficial de seguridad de la informacion	Capacitación en comité MIPG
Curso Fortinet NSE1(Network Security associate).	Curso certificado valido x 2 años sobre las ciber amenazas actuales y brinda consejos sobre como proteger la información	Oficial de seguridad de la informacion Oficina de Comunicaciones Gerente de cuenta Fortinet - Colsof	Plataforma Online Fortinet https://training.fortinet.com/
Socialización de enfoque Zero Trust	Socialización cambio de enfoque arquitectura de seguridad con enfoque	Oficial de seguridad de la informacion	Presentación Comité Directivo

	Zero Trust (Cero Confianza).	Arquitecto de TI Coordinador de Grupo Sistemas	
Cursos ciberseguridad con gamificación de la OSI	Cursos de ciberseguridad para usuarios finales	Oficial de seguridad de la informacion	Plataforma Online de la OSI https://cyberscouts.osi.es/
Guía de CiberSeguridad para Niños y Adultos	Curso de ciberseguridad para pacientes, usuarios finales y sus familias.	Oficial de seguridad de la informacion	Documento facilitado por Fabricante Fortinet. Correo electrónico
Socialización sobre criptografía	Socializar técnicas criptográficas y manual de criptografía	Oficial de seguridad de la informacion	Dircom
Sensibilización sobre firmas digitales	Socializar técnicas de firma digital implantadas en el INC	Coordinadora de gestión Documental	Dircom, Teams
Socializar gestión de telemetría	Socializar manual y gestión de telemetría y capacidad.	Oficial de seguridad de la informacion	Dircom. Sensibilización interna de sistemas
Socializar guía de identificación de fraudes online	Socializar Guía Aprendiendo a identificar Fraudes Online	Oficial de seguridad de la informacion Grupo de Comunicaciones	Dircom.
Sensibilización de Cibersegruidad	Sensibilización de ciberseguridad y controles institucionales	Oficial de seguridad de la información Proveedor de NDR	Microsoft Teams
Sensibilización de seguridad en IA	Sensibilización sobre uso seguro de la IA	Oficial de seguridad de la información Laboratorio de Cocreación	Dircom, Microsoft Teams
Sensibilización de criptografía	Sensibilización sobre uso de criptografía en el INC	Oficial de seguridad de la información	Dircom
Sensibilización de capacidad y telemetría	Sensibilización sobre monitoreo de capacidad	Oficial de seguridad de la información Coordinadora de hardware y redes	Dircom

Sensibilización en Continuidad de Negocio	Sensibilización sobre plan de continuidad de Negocio y BIA	Oficial de seguridad de la información Consultor de Continuidad Líder de Continuidad Operacional	Auditorio, Microsoft Teams, Dircom

4.2.3 FASE IMPLEMENTACIÓN (CRONOGRAMA)

A continuación, se presenta el cronograma de implementación del Plan de sensibilización y capacitación de seguridad y continuidad digital, con un alcance de ejecución de 2 años para el periodo 2025-2026. Se priorizarán las actividades relacionadas con la integración de la ISO 42001 y los riesgos de ciberseguridad global. Se buscará optimizar la difusión a través de los canales digitales más utilizados por los empleados, como el correo electrónico (Outlook 365) y Microsoft Teams, dada su alta satisfacción, uso y apropiación.

PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN 2025 - 2026	**475 días**	**lun 3/03/25**	**vie 25/12/26**		
PLANEACIÓN	**76 días**	**lun 3/03/25**	**lun 16/06/25**		
Identificación de necesidades de capacitación	15 días	lun 3/03/25	vie 21/03/25		CISO
Actualización de Análisis Dofa	2 días	lun 5/05/25	mar 6/05/25		CISO
Actualización Definición de Perfiles y Necesidades	10 días	jue 6/03/25	mié 19/03/25		CISO
definición de metas de capacitación	3 días	lun 17/03/25	mié 19/03/25		CISO
Diseño de la estrategia	6 días	lun 24/03/25	lun 31/03/25		CISO
Definición de temáticas de capacitación y sensibilización	6 días	lun 31/03/25	lun 7/04/25		CISO;Lider Oficina Control Interno;Lider Oficina Control Interno disciplinario;Coordinadora Gestion Documental;Coordinadora Grupo Soporte, hardware y redes;Profesional de Riesgo;Especialista Microsoft Office365
Definición de medios y estrategias de Comunicación	5 días	lun 14/04/25	vie 18/04/25		CISO;Oficina de Comunicaciones
Elaboración de Cronograma de Plan de Capacitación	5 días	jue 1/05/25	mié 7/05/25		CISO
Alineación de metodología con MSPI Mintic	3 días	lun 12/05/25	mié 14/05/25		CISO;Oficina de Comunicaciones

Revisión de alineación con el plan de Comunicaciones	7 días	jue 15/05/25	vie 23/05/25		Profesional Organizacion y Metodos;CISO
Aprobación comité de mi PG	5 días	jue 22/05/25	mié 28/05/25		CISO;Oficina de Comunicaciones
Versionamiento con OyM	6 días	lun 2/06/25	lun 9/06/25		Comite de Mi PG
Publicación de Plan de capacitación en Pag Web	3 días	jue 12/06/25	lun 16/06/25		CISO;Oficina de Comunicaciones
DISEÑO/ACTUALIZACIÓN DE MATERIAL DE CAPACITACIÓN	**89 días**	**mar 8/07/25**	**vie 7/11/25**		
Guía de ciberataques: Ataques por contraseñas	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques: Ataques por ingenieria social	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques: Ataques por ingeniería social 2	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques: Ataques a las conexiones -1	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques: Ataques a las conexiones – 2	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques: Ataques por malware 1	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques: Ataques por malware 2	10 días	lun 21/07/25	vie 1/08/25		CISO
Guía de ciberataques INC - Buenas Prácticas e Higiene de seguridad	10 días	lun 21/07/25	vie 1/08/25		CISO
Socialización de Política de riesgo de seguridad digital	10 días	mar 8/07/25	lun 21/07/25	24	Profesional de Riesgo;CISO;Oficina de Comunicaciones;Oficna de Comunicaciones
Capacitación sobre el cuidado y buen uso de los equipos tecnológicos,	10 días	mar 8/07/25	lun 21/07/25		Coordinadora Grupo Soporte, hardware y redes;Lider Oficina Control Interno disciplinario
Capacitación Activos de Informacion	10 días	mar 8/07/25	lun 21/07/25		CISO;Coordinadora Gestion Documental;Epecialista Ofiamtica 365 -Outsourcing
Capacitaciones sobre herramientas de ofimática	10 días	mar 22/07/25	lun 4/08/25	27	Coordinadora Grupo Soporte, hardware y redes;Especialista Microsoft Office365
Código general disciplinario	10 días	mar 5/08/25	lun 18/08/25	28	Lider Oficina Control Interno disciplinario;Oficina de Comunicaciones

Correo electrónico Certificado	10 días	vie 15/08/25	jue 28/08/25	29	Coordinadora Gestion Documental;Especialista Microsoft Office365;Oficina de Comunicaciones
Sensibilización en el manejo de documentos obsoletos	10 días	vie 15/08/25	jue 28/08/25		Coordinadora Gestion Documental;Oficina de Comunicaciones
Sensibilización sobre líneas de defensa de riesgos	10 días	mar 26/08/25	lun 8/09/25	31	Lider Oficina Control Interno;Profesional de Riesgo
Sensibilización tratamiento de datos personales en el INC	10 días	vie 29/08/25	jue 11/09/25	32	CISO;Lider Oficina Control Interno;Lider Oficina Juridica
Revisión Curso inducción reinducción en seguridad de la información	51 días	vie 29/08/25	vie 7/11/25		CISO;Profesional Grupo Desarrollo y Talento Humano
Qué hacer ante la pérdida de dispositivos móviles	10 días	vie 29/08/25	jue 11/09/25		CISO
Socializaciones técnicas criptográficas y manual de criptografía	10 días	vie 29/08/25	jue 11/09/25		CISO
Socialización manual y gestión de capacidad.	10 días	vie 29/08/25	jue 11/09/25		CISO;Coordinadora Grupo Soporte, hardware y redes
Actualización Socialización de Manual de Contraseñas y control de acceso	10 días	vie 29/08/25	jue 11/09/25		CISO
Socialización Medidas de Seguridad para redes Sociales	10 días	vie 29/08/25	jue 11/09/25		CISO
Socialización actualización documental por cambio de la Norma ISO27001:2022	10 días	vie 29/08/25	jue 11/09/25		CISO
Socialización cambio de arquitectura de seguridad con enfoque Zero Trust (Cero Confianza).	10 días	vie 12/09/25	jue 25/09/25	40	CISO;Coordinadora Grupo Soporte, hardware y redes
Alistamiento Tenan Curso Fortinet NSE1(Network Security associate).	10 días	vie 12/09/25	jue 25/09/25		CISO
Guía de CiberSeguridad para Niños y Adultos	10 días	vie 12/09/25	jue 25/09/25		CISO
Socialización de manual DRP (Continuidad informática)	10 días	vie 12/09/25	jue 25/09/25		CISO
Sensibilización Aprendiendo a identificar Fraudes Online	10 días	vie 12/09/25	jue 25/09/25		CISO
Sensibilización Curso cibersegruidad OSI con plataforma de Gamificación	10 días	vie 26/09/25	jue 9/10/25	45	CISO

Socialización sobre criptografía	26 días	vie 26/09/25	vie 31/10/25		CISO
Sensibilización sobre firmas digitales	26 días	vie 26/09/25	vie 31/10/25		CISO
Socializar gestión de telemetría	26 días	vie 26/09/25	vie 31/10/25		CISO
Sensibilización de Cibersegruidad	26 días	vie 26/09/25	vie 31/10/25		CISO
Sensibilización de seguridad en IA	26 días	vie 26/09/25	vie 31/10/25		CISO
Sensibilización de criptografía	26 días	vie 26/09/25	vie 31/10/25		CISO
Sensibilización de capacidad y telemetría	26 días	vie 26/09/25	vie 31/10/25		CISO
Sensibilización en Continuidad de Negocio	26 días	vie 26/09/25	vie 31/10/25		CISO
Simulacion de Phishing con plataforma Microsoft	26 días?	vie 26/09/25	vie 31/10/25		CISO
DESARROLLO DE CAPACITACIONES /SENSIBILIZACIONES	**375 días**	**lun 21/07/25**	**vie 25/12/26**		
Guía de ciberataques: Ataques por contraseñas	5 días	vie 1/08/25	jue 7/08/25		Oficina de Comunicaciones;CISO
Guía de ciberataques: Ataques por ingenieria social	5 días	vie 8/08/25	jue 14/08/25	57	CISO
Guía de ciberataques: Ataques por ingeniería social 2	5 días	vie 15/08/25	jue 21/08/25	58	CISO
Guía de ciberataques: Ataques a las conexiones -1	5 días	vie 22/08/25	jue 28/08/25	59	CISO
Guía de ciberataques: Ataques a las conexiones – 2	5 días	vie 29/08/25	jue 4/09/25	60	CISO
Guía de ciberataques: Ataques por malware 1	5 días	vie 5/09/25	jue 11/09/25	61	CISO
Guía de ciberataques: Ataques por malware 2	5 días	vie 12/09/25	jue 18/09/25	62	CISO
Guía de ciberataques INC - Buenas Prácticas e Higiene de seguridad	5 días	vie 19/09/25	jue 25/09/25	63	CISO
Socialización de Política de riesgo de seguridad digital	5 días	vie 26/09/25	jue 2/10/25	64	Oficina de Comunicaciones;Profesional

					de Riesgo;CISO;Oficna de Comunicaciones
Capacitación sobre el cuidado y buen uso de los equipos tecnológicos,	5 días	vie 3/10/25	jue 9/10/25	65	Coordinadora Grupo Soporte, hardware y redes;Lider Oficina Control Interno disciplinario
Capacitación Activos de Informacion	9 días	vie 10/10/25	mié 22/10/25	66	CISO;Coordinadora Gestion Documental;Epecialista Ofiamtica 365 -Outsourcing
Capacitaciones sobre herramientas de ofimática	15 días	jue 23/10/25	mié 12/11/25	67	Coordinadora Grupo Soporte, hardware y redes;Especialista Microsoft Office365
Código general disciplinario	10 días	mié 11/03/26	mar 24/03/26	68	Lider Oficina Control Interno disciplinario;Oficina de Comunicaciones
Correo electrónico Certificado	10 días	mar 24/03/26	lun 6/04/26	69	Coordinadora Gestion Documental;Especialista Microsoft Office365;Oficina de Comunicaciones
Sensibilización en el manejo de documentos obsoletos	10 días	lun 6/04/26	vie 17/04/26	70	Coordinadora Gestion Documental;Oficina de Comunicaciones
Sensibilización sobre líneas de defensa de riesgos	10 días	vie 17/04/26	jue 30/04/26	71	Lider Oficina Control Interno;Profesional de Riesgo
Sensibilización tratamiento de datos personales en el INC	10 días	jue 30/04/26	mié 13/05/26	72	CISO;Lider Oficina Control Interno;Lider Oficina Juridica
Qué hacer ante la pérdida de dispositivos móviles	10 días	mié 13/05/26	mar 26/05/26	73	CISO
Socializaciones técnicas criptográficas y manual de criptografía	10 días	mar 26/05/26	lun 8/06/26	74	CISO
Socialización manual y gestión de capacidad.	10 días	lun 8/06/26	vie 19/06/26	75	CISO;Coordinadora Grupo Soporte, hardware y redes
Actualización Socialización de Manual de Contraseñas y control de acceso	10 días	vie 19/06/26	jue 2/07/26	76	CISO
Socialización Medidas de Seguridad para redes Sociales	10 días	jue 2/07/26	mié 15/07/26	77	CISO
Socialización actualización documental por cambio de la Norma ISO27001:2022	10 días	mié 15/07/26	mar 28/07/26	78	CISO
Socialización enfoque Zero Trust (Cero Confianza).	10 días	mar 28/07/26	lun 10/08/26	79	CISO;Coordinadora Grupo Soporte, hardware y redes

Curso Tenan Curso Fortinet NSE1(Network Security associate).	10 días	lun 10/08/26	vie 21/08/26	80	CISO
Guía de CiberSeguridad para Niños y Adultos	10 días	vie 21/08/26	jue 3/09/26	81	CISO
Socialización de manual DRP (Continuidad informática)	10 días	jue 3/09/26	mié 16/09/26	82	CISO
Sensibilización Aprendiendo a identificar Fraudes Online	10 días	mié 16/09/26	mar 29/09/26	83	CISO
Sensibilización Curso cibersegruidad OSI con plataforma de Gamificación	10 días	mar 29/09/26	lun 12/10/26	84	CISO
Socialización sobre criptografía	10 días	lun 12/10/26	vie 23/10/26	85	CISO
Sensibilización sobre firmas digitales	10 días	vie 23/10/26	jue 5/11/26	86	CISO
Socializar gestión de telemetría	10 días	jue 5/11/26	mié 18/11/26	87	CISO
Sensibilización de Cibersegruidad	10 días	mié 18/11/26	mar 1/12/26	88	CISO
Sensibilización de seguridad en IA	10 días	mar 1/12/26	lun 14/12/26	89	CISO
Sensibilización de criptografía	10 días	lun 14/12/26	vie 25/12/26	90	CISO
Sensibilización de capacidad y telemetría	10 días	lun 14/12/26	vie 25/12/26		CISO;Coordinadora Grupo Soporte, hardware y redes
Sensibilización en Continuidad de Negocio	63 días	lun 21/07/25	mié 15/10/25		CISO;Lider de Continuidad Operacional;Consultor de continuidad
Simulacion de Phishing con plataforma Microsoft	36 días	lun 3/11/25	lun 22/12/25		CISO;Epecialista Ofiamtica 365 -Outsourcing

Nota: Se aclara que este es plan de capacitación y sensibilización es un plan vivo, y que pueden revisarse y modificarse el cronograma de actividades de acuerdo con las necesidades y cambios en la seguridad de la institución y del sector Salud, en la evolución de amenazas, en los cambios de normatividad, y en las recomendaciones de organismos de gobierno y control.

4.2.3.1 Documentación de asistencia

El registro de asistencia a capacitaciones y sensibilizaciones presenciales se realizará en formato GTH-P05-F-08, o mediante registros de asistencia de eventos de las plataformas utilizadas. Para entrenamientos virtuales, se utilizará el listado de asistencia automática de Microsoft Teams o Microsoft Forms. Para correos y boletines, se mantendrán los registros de entregabilidad, reconociendo la limitación de estadísticas de lectura. Se explorarán herramientas adicionales que permitan medir la interacción con los contenidos digitales y la lectura efectiva.

4.2.4 FASE DE MEJORA

El plan de capacitación y sensibilización en seguridad de la información se somete a una revisión cada dos años. La revisión debe ajustar el plan a los cambios institucionales, tecnológicos o normativos, garantizando que el personal reciba información relevante para proteger los activos institucionales. Los contenidos y metodologías de formación deben mantenerse actualizados con las últimas amenazas y mejores prácticas en ciberseguridad

Para evaluar la efectividad de este plan y el estado de la sensibilización de los usuarios, se implementa una encuesta anual. Esta evaluación se integra estratégicamente dentro de la encuesta de satisfacción, uso y apropiación de TI. La herramienta seleccionada para la aplicación de esta encuesta es el sistema de encuestas de Office 365 (Microsoft Forms), lo que facilita la distribución, recolección y análisis de los datos.

En la Encuesta se tratarán y analizar los siguientes temas mínimos:

- Disponibilidad de recursos y materiales
- Impacto en la organización
- Interiorización de los contenidos de Seguridad, incluyendo conocimientos sobre seguridad de IA y continuidad de negocio.
- Percepción de la efectividad de las capacitaciones virtuales y la facilidad de acceso a los materiales.
- Nivel de confianza en los sistemas de IA del INC.

5 METAS

Meta 1: Aumentar la Apropiación de Seguridad y Continuidad Digital
Lograr un incremento sostenido en el porcentaje de apropiación de la seguridad y continuidad digital por parte de los usuarios, reflejando una mayor conciencia y aplicación de las mejores prácticas.

Meta 2: Garantizar la Ejecución del Plan de Capacitación y Sensibilización
Asegurar un cumplimiento oportuno de todas las actividades programadas en el plan de capacitación y sensibilización en seguridad y continuidad digital.

6 INDICADORES

Se definen los siguientes indicadores de plan de capacitación y sensibilización.

- **Indicador 1 - Porcentaje apropiación de seguridad y continuidad digital**

  Fórmula: {Sumatoria de los promedios de las respuestas (si y no) x tipo de incidente S.I. evaluado}/{Número de tipos de incidentes de S.I. evaluados} * 100
  Unidad: Porcentaje (%)
  Frecuencia: Anual

- **Indicador 2 - Porcentaje de ejecución del plan de capacitación y sensibilización en seguridad y continuidad digital**

  Fórmula: {Número actividades ejecutadas del plan de capacitación y sensibilización en seguridad y

continuidad digital} /{Total actividades programadas del plan de capacitación y sensibilización en seguridad y continuidad digital} * 100
Unidad: Porcentaje (%)
Frecuencia: Semestral

7 CRONOGRAMA

Este **cronograma de dos años**, que se extiende desde el **3 de marzo de 2025 hasta el 25 de diciembre de 2026**, detalla el plan estratégico para fortalecer la seguridad de la información a través de la capacitación y sensibilización del personal.

El cronograma del plan se divide en tres fases principales:

Fase 1: Planeación

- **Duración:** 76 Días
- **Fechas:** 03/03/2025 - 16/06/2025
- **Enfoque:** Establecer las bases del plan.
- **Actividades Clave:**
  - Identificación de necesidades de capacitación.
  - Actualización de análisis DAFO.
  - Definición de perfiles y necesidades.
  - Definición de metas de capacitación.
  - Diseño de estrategia.
  - Definición de temáticas, medios y cronograma.
  - Alineación con metodologías y planes de comunicación.
  - Aprobación y publicación del plan.

Fase 2: Diseño/Actualización de Material de Capacitación

- **Duración:** 89 Días
- **Fechas:** 08/07/2025 - 07/11/2025
- **Enfoque:** Crear y adaptar contenidos.
- **Actividades Clave:**
  - Desarrollo de guías sobre ciberataques (contraseñas, ingeniería social, malware, conexiones, higiene).
  - Creación de material para socialización de políticas (riesgo digital, uso de equipos, activos de información).
  - Preparación de capacitaciones sobre herramientas de ofimática y normativas (código disciplinario, datos personales).
  - Diseño de sensibilizaciones clave (manejo de documentos, líneas de defensa, pérdida de dispositivos, criptografía, Zero Trust).
  - Alistamiento de cursos específicos (Fortinet NSE1, ciberseguridad OSI).
  - Material para sensibilización en continuidad de negocio y simulación de phishing.

Fase 3: Desarrollo de Capacitaciones / Sensibilizaciones

- **Duración:** 375 Días
- **Fechas:** 21/07/2025 - 25/12/2026
- **Enfoque:** Implementación y formación.
- **Actividades Clave:**
  - Ejecución continua de las guías de ciberataques.
  - Realización de socializaciones de políticas y manuales.
  - Impartición de capacitaciones técnicas y de normativas.

- Campañas de sensibilización en temas críticos (fraudes online, IA, firmas digitales, telemetría).
- Desarrollo de cursos especializados.
- Simulaciones de phishing y actividades de concientización.
- Capacitación en continuidad de negocio.

El cronograma de implementación del plan de capacitación y sensibilización se encuentra detallado en el numeral 5.2.2, específicamente dentro de la sección designada como "FASE IMPLEMENTACIÓN (CRONOGRAMA)". Este apartado ofrece una vista completa y estructurada de las actividades planificadas, sus plazos y los responsables para llevar a cabo eficazmente la formación y concientización en seguridad de la información a lo largo del periodo establecido.

8 RECURSOS

No se cuenta con un presupuesto formalmente asignado para la ejecución del plan de capacitación y sensibilización de seguridad de la información, y por lo tanto se debe gestionar con las herramientas institucionales actualmente desplegadas para capacitación, con material de sensibilización desarrollado internamente, material Opensource, y material de proveedores y terceros con licencia de uso para el INC. Los recursos y medios que se utilizarán son aquellos con los cuales ya cuenta el instituto para el diseño y despliegue. Se buscará priorizar la adquisición de recursos y capacitaciones que aborden los nuevos riesgos de ciberseguridad, de continuidad de Negocio, y la implementación de la ISO 42001.

9 APROBACIÓN

El presente plan de capacitación y sensibilización se encuentra aprobado mediante acta institucional No. 05 de 23 de mayo de 2025, por el Comité Institucional de Gestión y Desempeño – MIPG

LÍA MARGARITA ÁLVAREZ P
Subdirección Administrativa y Financiera

Luis Eduardo Martinez Gonzalez
Coordinador Grupo Área Gestión de Sistemas

10 BIBLIOGRAFIA

- INCIBE. (s.f.). *Kit de Concienciación*. Recuperado de https://www.incibe.es/empresas/formacion/kit-concienciacion

- Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Modelo de seguridad y privacidad de la información (MSPI).

  https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150525_G14_Plan_comunicacion_sensibilizacion.pdf

- OSI (Oficina de Seguridad del Internauta). (s.f.). Cyberscouts. Recuperado de https://cyberscouts.osi.es/

.

VERSIÓN	FECHA DE ACTUALIZACIÓN	DESCRIPCIÓN DE ACTUALIZACIÓN	RESPONSABLE OYM
1	30-01-2020	Versión inicial del documento	Paula Andrea Salamanca Medina
2	19-10-2022	Se revisa documento y se actualiza la vigencia en el alcance, se incluyó como canal de información: INCforma, se actualiza los medios de comunicación del plan. Se actualiza el analisis DOFA. se actualiza los roles y perfiles, se actualiza la temática del plan de capacitación y sensibilización y se actualiza la implementación del plan.	Elizabeth Romero Rodriguez
3	28-12-2023	Se realiza actualización del plan, realizando las siguientes modificaciones. Se ajusta el OBJETIVO agregando al mismo, conceptos técnicos que complementan la definición de la finalidad del objetivo. Se definen nuevos OBJETIVOS ESPECIFICOS al plan. Al numeral de la NORMATIVIAD se las agregan las siguientes 2 normas ISO/IEC 27001:2022 y Conpes 3995 de 2020. Se realiza actualización del cronograma de implementación del plan donde se define un alcance de ejecución de 2 años. Este plan fue presentado en el comité de MIPG del día 18-10-2023 y aprobado por acta institucional No 10 18-10-2023 - AI-23-02225.	Diego Andres Paez Gomez
4	20-06-2025	Se revisa el documento y se realizan los siguientes ajustes: Se ajusta la vigencia del plan. 2.Se ajusta la enumeración y estructura del documento. 3. Se ajusta el objetivo general. 4. En el ítem 3.1 NORMATIVIDAD se adiciona normas aplicadas a plan los cuales son: COMPES 4144 - Politica Nacional de Inteligencia Artificial, ISO/IEC 42001:2023, Resolución 500 de 2021 de Mintic. 5. En el ítem 3.2 DEFINICIONES se adiciona las definiciones de: Inteligencia artificial, sistema de gestión de inteligencia Artificial, ciberresilencia, Análisis de impacto de negocio, plan de recuperación ante desastres, plan de continuidad del negocio. 6. En el ítem 4.1.1 FASE DE DISEÑO se ajustan lo medios de comunicación que utilizan como estrategias de divulgación. 7. Se adiciona el ítem FASE DE MEJORA. 8. Se adiciona el ítem de CRONOGRAMA.	Laura Catherin Rodriguez Galan

ELABORÓ		REVISÓ		APROBÓ	
Cargo:	Profesional Universitario	Cargo:	Coordinador Grupo Área Gestión de Tecnologías de Información	Cargo:	Coordinador
Dependencia:	Oficina Asesora de Planeación y Sistemas	Dependencia:	Coordinador Grupo Área Gestión de Tecnologías de Información	Dependencia:	Coordinador Grupo Área Gestión de Tecnologías de Información
Fecha:	13-10-2021	Fecha:	13-10-2021	Fecha:	13-01-2021