PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

VERSION 1.0

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ELABORADO POR: CARLOS ANDRÉS GUERRERO
PROFESIONAL ESPECIALIZADO I

GRUPO AREA GESTIÓN DE SISTEMAS

INSTITUTO NACIONAL DE CANCEROLOGÍA E.S.E.

2019

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las tecnologías de información y comunicaciones se han convertido en la herramienta por excelencia para la optimización de los procesos y el funcionamiento eficaz del Instituto Nacional de Cancerología. Con el uso de la tecnología, surgen a su vez amenazas y vulnerabilidades asociadas, que pueden llegar a afectar la disponibilidad, privacidad e integridad de la información que se encuentra disponible en las diferentes plataformas, afectando de esta manera el desempeño normal de la Entidad. Para esto, el Sistema de Gestion de Seguridad de la Información (SGSI) indica pautas específicas para guiar al INC a robustecer sus plataformas y mitigar amenazas que pueden llegar a traer consigo las tecnologías implementadas, sin embargo, un programa robusto de seguridad y privacidad de la información no se basa únicamente en el aseguramiento de plataformas y procesos, sino que también debe involucrar los factores humanos, que en muchos casos, son la principal causa de los incidentes de seguridad dentro de un sistema determinado, esto debido a que no conocen sobre seguridad de la información y su rol dentro de la Entidad. Muchas instituciones no prestan la suficiente atención a su recurso humano, que puede llegar a ser el eslabón más débil en la cadena de la seguridad de la información, por lo que es necesario sensibilizarlos o capacitarlos sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

2. OBJETIVO

El presente documento se enmarca dentro de la política establecida por el Gobierno Nacional que pretende la inclusión social y la competitividad a través de la apropiación y el usos de las Tecnologías de la Información y las Comunicaciones (TIC), tanto en la vida cotidiana como productiva de los ciudadanos, empresas, academia y estado. Su desarrollo se ha enmarcado dentro de la Estrategia de Gobierno en Línea que contribuye a la construcción de un Estado eficiente, transparente, participativo y que preste mejores servicios a los ciudadanos.

El Plan de capacitación y sensibilización en seguridad de la información para el Instituto Nacional de Cancerología ESE (INC) define las estrategias que conducen a la preservación de la confidencialidad, integridad, y disponibilidad de sus activos de información, por medio de la sensibilización capacitación y comunicación de las reglas de comportamiento adecuadas para el uso de los sistemas y de los activos de la información, y de la privacidad y del manejo de datos personales del ciudadano, paciente y cliente interno dentro y fuera del INC

3. OBJETIVOS ESPECIFICOS

- Difundir los valores y principios institucionales en nuestras labores diarias y generar apropiación de cada uno de ellos con el fin de mostrar que el talento humano del INC conoce y aplica nuestra identidad corporativa para el mejoramiento institucional.
- Promover el conocimiento que poseen los pacientes y funcionarios sobre sus derechos y deberes
- Definir los temas para la capacitación en seguridad de la información, de acuerdo con el público objetivo.
- Establecer la metodología que permita evidencias cuales son las necesidades de capacitación para el INC.
- Construir materiales para sensibilización y entrenamiento.
- Evaluar, medir y cuantificar, si el programa implementado genera impacto en el desarrollo de las actividades del INC.

- Identificar las necesidades y requerimientos del INC de educación no formal y educación formal para su personal en seguridad de la información.

4. ALCANCE

Establecimiento de un programa de sensibilización y capacitación de seguridad y privacidad de la información enmarcado dentro del sistema de gestión de seguridad de la información (SGSI) del INC y la metodología MSPI de MINTIC, para ejecución en el año 2019-2020.

5. NORMATIVIDAD

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 Superfinaciera: Por la cual se Imparten instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad.

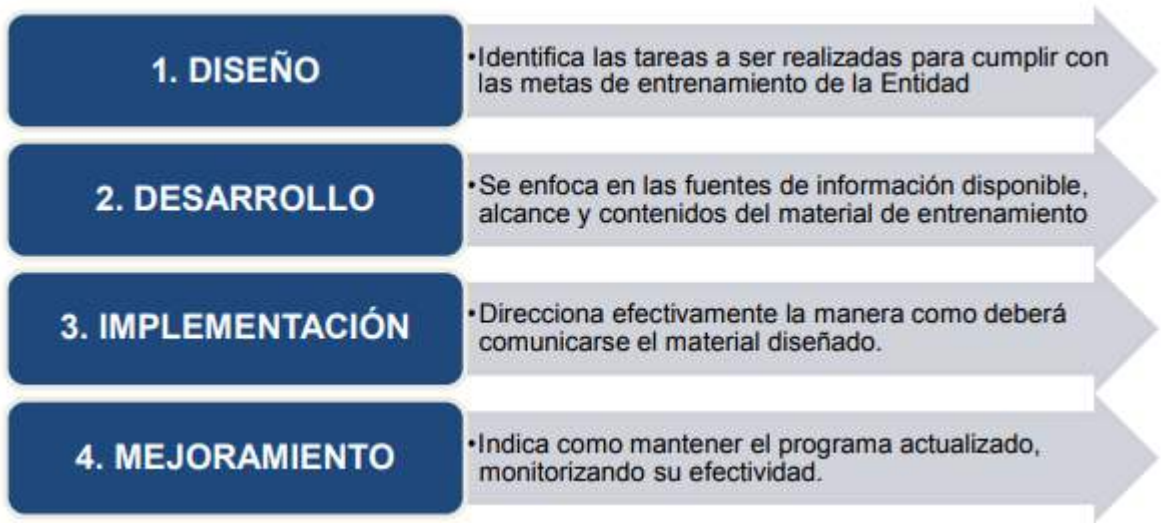
6. DEFINICIONES TÉCNICAS

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.

Cuestionario Encuesta: Se trata de un cuestionario que sirve de encuesta para medir la satisfacción del cliente.
Error Conocido: Es un Problema cuya raíz y solución temporal han sido documentadas. Los Errores Conocidos se crean y se gestionan a lo largo de su ciclo de vida por personal de Gestión de Problemas.
Escalado por Parte del Usuario: Se trata de un escalado relacionada con el procesamiento de un Incidente; se origina luego de que un usuario experimenta retrasos o fallos durante la restauración de un servicio.
Informe de Gestión de Incidentes: Provee información relacionada con Incidentes a los procesos de Gestión de Servicio.
Informe de Nivel de Servicio: Este informe ayuda a entender la habilidad que tiene un proveedor de servicios para lograr la calidad de servicio acordada. A estos efectos, compara los niveles de servicio logrados con los propuestos, y también incluye información sobre el uso de servicios, las medidas de mejoramiento continuo a los servicios y eventos excepcionales.
Plantilla para Solicitudes de Cambio: Es una plantilla usada cuando se solicita formalmente un Cambio.
Política de Seguridad de la información: Establece reglas vinculantes para el uso de servicios y de sistemas con miras a mejorar la seguridad de TI.
Preguntas sobre Estado de Incidentes: Cualquier pregunta sobre el estatus actual de un Incidente, generalmente provienen de un usuario que lo reportó inicialmente.
Preguntas Frecuentes de los Usuarios: Información de autoayuda para los usuarios, provista por la Mesa de Ayuda como parte de las Páginas de Apoyo o de una red interna.
Registro de Evento: Es un cambio de estado significativo para el manejo de algún componente o servicio de Configuración. El término "Evento" también se usa para referirse a las alertas o notificaciones creadas por algún servicio de TI, elemento de Configuración o herramienta de monitorización.
Incidente: Un Incidente se define como una interrupción no planificada o como la reducción de calidad de algún servicio de TI.
Registro de Incidente: Es un conjunto de datos con todos los detalles de un Incidente, que documenta la historia de los mismos desde su registro hasta su resolución.
Registro de Problema: Contiene todos los detalles de un Problema y documenta el historial de ese Problema desde su detección hasta su resolución.
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.
Sistema de Información de Gestión de la Seguridad (SMIS): El Sistema de Información de Gestión de la Seguridad (Information Security Management System, SMIS) es un depósito virtual de todos los datos de Gestión de la Seguridad de TI, generalmente almacenados en varias localidades físicas
Solicitud de Cambio (RFC): La Solicitud de Cambio (Request for Change, RFC) es una requisición formal de Cambio en espera de ser implementada. Incluye detalles del Cambio propuesto, y puede estar en formato electrónico o en papel.
Solicitud de Servicio: Generado por un usuario que busca información o consejo, o que desea solicitar un Cambio menor o que se le conceda acceso a algún servicio de TI. Esta solicitud puede ser de cambio de contraseña, o de que se le provean servicios comunes de TI a otro usuario.

7. DESARROLLO DEL PLAN

El plan de capacitación, sensibilización y comunicación adecuado, se lleva a cabo con base a las siguientes 4 fases:



7.1 Diseño de programa de sensibilización y capacitación

El instituto cuenta con un programa de entrenamiento y sensibilización Centralizado liderado por Talento Humano. En este programa, Talento Humano delega al grupo área gestión de sistemas la definición de estrategia y diseño del plan. El plan luego es distribuido de igual manera a todas las unidades organizacionales, sedes, incluyendo proveedores y terceros para que sea aplicado de manera homogénea en cada una.
El desarrollo de los diseños, materiales para sensibilización y capacitación, y el despliegue se construyen en el Grupo Area sistemas con el apoyo de la Oficina asesora de planeación y sistemas de la información (Oficina de comunicaciones), utilizando las estrategias de comunicación orientadas a cliente externo e interno (ciudadano y paciente) implantadas para tal fin, como los son las que se identifican a continuación

- Correo electrónico (Mailing)
- Sistema Multivisual y Auditorios
- Canal INCformaTV e Vida y Cancer Tv
- Carteleras
- Intranet
- Boletines virtuales
- Lista de difusión
- Papel Tapiz de equipos.

7.2. Identificación de necesidades de capacitación en S.I.

El INC reconoce que la información es uno de los activos más importantes para cumplir las funciones y objetivos que le han sido delegados por el Gobierno Nacional, de ahí la importancia de realizar 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 parte interesadas

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

- La estructura organizacional,
- La verificación de los incidentes de seguridad de la información
- Análisis de eventos de las herramientas y dispositivos de seguridad (Firewall, Antispam, Antivirus)
- Amenazas identificadas para el sector salud en las mesas de trabajo de Ciberseguridad y ciberdefensa del Ministerio de Salud.
- Reporte de las amenazas a la seguridad en Internet (Internet Security Threat Report o ISTR)
- El plan de capacitación y sensibilización ejecutado para el año anterior.
- Informe de Amenazas Cibernéticas INC

7.3. Análisis DOFA (Debilidades, Amenazas, Fortalezas y Oportunidades)

Luego de identificar los roles y necesidades, a continuación, se presenta el análisis DOFA (debilidades, oportunidades, fortalezas y amenazas) identificado por el instituto con relación a la situación actual de capacitación en seguridad de la información.

FACTORES INTERNOS DE LA EMPRESA		FACTORES EXTERNOS A LA EMPRESA	
DEBILIDADES (-)		**AMENAZAS (-)**	
1	La entidad debe fortalecer los programas de divulgación y sensibilización a los Funcionarios y/o Contratistas, proveedores y terceros frente al SGSI.	1	Apropiarse de los cambios normativos y legislativos vigentes que afecten el SGSI.
2	La entidad carece de visibilidad para seguimiento y monitoreo de plan de sensibilización de seguridad para verificar la efectividad y eficacia del mismo.	2	Mantenerse actualizado con las evoluciones tecnológicas en seguridad informática.
3	La entidad debe fortalecer el plan de tratamiento de los riesgos que afecten el SGSI, incluyendo riesgos de seguridad digital, ciberdefensa y ciberseguridad.	3	Dar cumplimiento a los requisitos de los entes de control.
4	Alta rotación del personal operativo responsable de los procesos	4	Dar cumplimiento al Manual del SGSI y a las políticas de seguridad y privacidad de la información
5	El instituto carece de seguimiento a los Funcionarios y/o contratistas, proveedores y terceros frente al cumplimiento del SGSI.	5	Ataques cibernéticos a la infraestructuras criticas del Instituto
6	Rotación del personal operativo responsable de plataformas, debido a cambio de outsourcing y cambio de tecnología de seguridad de la información.	6	
7	Resistencia al cambio y al control	7	

8	Baja penetración de los medios establecidos para la sensibilización, según registros de 2018	8	

FORTALEZAS (+)		OPORTUNIDADES (+)	
1	Personal calificado, rigurosidad técnica y con habilidades de liderazgo.	1	Aprender de los incidentes conocidos ocurridos en otras Entidades y Organizaciones del sector.
2	Programas de sensibilización y transferencia de conocimiento actualizados e implementados.	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	Se cuenta con Sistemas de Gestión Integrados, que permite comunicar varios procesos y hacerlos parte integral del mismo.	3	Lograr que los objetivos de la Entidad se cumplan con un alto nivel de Seguridad en el manejo de la Información.
4	Implementación del SGSI que promueve la confidencialidad, Integridad y Disponibilidad de la información para los clientes internos (Funcionarios y/o Contratistas) y Externos (Entidades, proveedores, etc.).	4	Participar entre las Entidades Públicas que hayan adoptado la metodología MSPI e ISO 27001:2013 mediante la apropiación de una Cultura del SGSI.
5	Adecuaciones de redes y comunicaciones y seguridad para adopción de protocolo IPV6	5	
	Se estableció plan de Adopción de protocolo IPV6		

7.4. Identificación de Roles Involucrados

Se identifican entonces los siguientes roles y necesidades de sensibilización y capacitación en seguridad de la información.

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. • Comprender el liderazgo y compromisos con la seguridad de la información que su rol tiene • Sensibilización sobre manejo de datos personales
RESPONSABLES DE SEGURIDAD DE LA INFORMACION	• Diseñar, estructurar e implementar el plan de sensibilización en seguridad de la información, teniendo	• Actualización en modelos de ciberseguridad y ciberdefensa.

	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 del mismo.	• Conocer funcionamiento y buenas prácticas de seguridad de protocolo IPV6 • Actualización en administración de herramientas de seguridad implantadas por recambio de tecnología con proyecto cambio Outsourcing. • Actualización en las herramientas de seguridad por recambio de arquitectura de redes y SI. • Actualización en las herramientas de seguridad por recambio de arquitectura de redes y SI.
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	• Preparación y actualización a nivel técnico de seguridad (implementación y prácticas de seguridad efectivas) para soportar las operaciones críticas del INC de manera apropiada. • Capacitación avanzada sobre protocolo IPV6 • Conocer y entender su compromiso y el de su grupo con las políticas de

	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.	seguridad de la información y Política de manejo de datos personales • Conocer sus responsabilidades con el SGSI. • Conocimientos avanzados sobre protección y administración de archivos en la nube.
LIDERES DE PROCESOS	• Fomentar la aplicación de las buenas 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.	• 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 • Sensibilización sobre manejo de datos personales • Sensibilización sobre controles de seguridad implantados para proteger la infraestructura que soporta cada proceso. • Sensibilización de riesgos de ciberdefensa y ciberseguridad • 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	• Conocer y entender su compromiso y el de su grupo con las políticas de seguridad de la

	de ingreso y retiro de personal • Incluir al SGSI y la seguridad de la información en los planes de Inducción reinducción del instituto	información y Política de manejo de datos personales • Conocer sus responsabilidades con el SGSI. • Sensibilización sobre manejo de datos personales • 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 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.	• El 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. • Conocer funcionamiento y buenas prácticas de seguridad de 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. • Conocimientos avanzados sobre protección de archivos en la nube.
USUARIOS FINALES	• Participar de todas 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	• 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

	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.	manejo de datos personales e información sensible en el INC. Abarca a los usuarios finales internos del INC, a estudiantes, docentes e investigadores, y al personal de proveedores, externos y tercerizados. • Conocimientos básicos sobre protección de archivos en la nube.
PACIENTE Y CIUDADANO	• Receptor de campañas de sensibilización a través de medios de comunicación del INC. • Ejercer sus derechos en el manejo 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 y darle a conocer los canales de comunicación con el INC.

7.5. Definición de metas del plan

De acuerdo a las debilidades y oportunidades identificadas en la matriz DOFA, se definen a continuación las principales metas para el programa de sensibilización en seguridad de la información para la vigencia 2019-2020:

- Socializar a toda la entidad la existencia del sistema de gestión de seguridad de la información y sus componentes de apoyo.
- Socializar a todo el personal de la Entidad las políticas de seguridad de la información
- Socializar las principales actividades de seguridad de la información, incluyendo proyecto de transición protocolo IPV4 a IPV6
- Fomentar la cultura de la seguridad de la información como herramienta de protección de la información institucional
- Explicar de manera sencilla la regulación que soportan el sistema de gestión de seguridad de la información, y las sanciones que acarrean el incumplimiento de las mismas.
- Divulgar a todos los funcionarios los principales riesgos de seguridad de la información
- Explicar en manera sencilla en qué consisten diversos tipos de ataques informáticos y como controlarlos
- Explicar los mecanismos de control dispuestos por la entidad para evitar ataques informáticos
- Dar a conocer los derechos de los pacientes y ciudadanos sobre el tratamiento de sus datos

personales.
- Dar a conocer los deberes de los trabajadores de Instituto con el manejo de información personal.
- Sensibilizar a contratistas y terceros sobre el manejo de la seguridad de la información en el instituto

7.6 Temáticas del plan

Se identifican las siguientes temáticas que debe cubrir el plan de capacitación y sensibilización en seguridad de la información

Conocimiento general del sistema de gestión de seguridad de la información (SGSI)
- Concepto de seguridad de la información
- Concepto Seguridad Informática
- Qué es un riesgo de seguridad de la información
- Qué la norma ISO27001 de gestión de seguridad de la información
- Cómo está estructurado el sistema de gestión de seguridad de la información
- Quienes son los actores del sistema de gestión de seguridad de la información

Conocimiento de las políticas de seguridad de la información
- Socialización de la política general de la seguridad de la información
- Socialización política de manejo de datos personales y privacidad de la información.
- Descripción de los controles de seguridad de la información con ejemplos de aplicación

Conocimiento de los procedimientos principales del Subsistema de gestión de seguridad
- Explicación del procedimiento de clasificación y etiquetado de información
- Explicación del procedimiento de Acceso a áreas seguras
- Metodología de gestión de riesgos y su anexo para identificación de riesgos de seguridad

Amenazas informáticas
- Phishing y Spear Phishing
- Ramsonware
- Robo de identidad
- Estafas de carnada
- Ataques a dispositivos Móviles
- Ataques a dispositivos de IOT de medicina (IoMT)

Higiene de seguridad básica
- Política de Contraseñas
- Política de Escritorios Limpios
- Bloqueo de sesiones de equipos
- Bloqueo Usb y dispositivos de almacenamiento externo

Tratamiento de Datos Personales
- Derechos de los titulares y deberes de los encargados

- Sanciones
- Procedimientos y medidas de seguridad
- Canales de comunicación de habeas data

7.7 Cursos obligatorios para todo el personal

Se definen como cursos obligatorios para todo el personal los siguientes:

- Conocimiento de las políticas de seguridad de la información
- Amenazas informáticas
- Higiene de seguridad básica
- Tratamiento de datos personales

8. DESARROLLO DE MATERIAL DE SENSIBILIZACION

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

MATERIAL	TEMATICA CUBIERTA	RESPONSBLE DESARROLLO	METODO DE DESPLIEGUE	FRECUENCIA
5 estafas cibernéticas que todos debemos conocer	Amenazas informáticas Higiene de seguridad básica	Oficial de seguridad de la información Oficina Asesora de planeación y sistemas de la información (oficina de comunicaciones)	Correo electrónico Stand feria de acreditación	Semestral
Tapices de Pantalla	Tratamiento de datos personales (Derechos y deberes de pacientes)	Oficial de seguridad de la información Oficina Asesora de planeación y sistemas de la información (oficina de comunicaciones)Administrador de Directorio Activo	Tapiz de pantalla de equipos - Active Directory	Anual
Material para sistemas multivisuales	Tratamiento de datos personales (Derechos y deberes de pacientes)	Oficial de seguridad de la información Oficina Asesora de planeación y sistemas de la información (oficina de comunicaciones) Administrador de Directorio Activo	Video institucional por los canales internos y correo masivo	Anual
Políticas Organizacionales Relacionadas Con Seguridad	Política de Seguridad de la información	Oficial de seguridad de la información	Capacitación presencial en auditorio	Anual

De La Información	Política BYOD Restricciones de Navegación	Oficina Asesora de planeación y sistemas de la información (oficina de comunicaciones)	Página web Videos-papel tapiz-infografías	
Tratamiento de datos personales	Política de manejo de datos personales	Oficial de seguridad de la información Grupo Area Gestion Documental	Papel tapiz Video	Anual
Tips Soy Ciberseguro	Higiene de seguridad básica Manejo de datos Personales	Oficial de seguridad de la información Oficina Asesora de Comunicaciones Mintic	Correo electrónico Infografía	Semestral. Diseñado para aplicar segundo semestre
Gestion de cambio – proyecto Outsourcing	Cambio Controles de seguridad Informática Interiorización de trabajo seguro Seguridad de office 365 Higiene de Seguridad	Colsof Oficial de Seguridad de la información Administrador de seguridad informática Consultores Office 365	Pendones Correo electrónico Sistema Multivisual Capacitaciones Presenciales Material para Carteleras	1 Vez, durante proyecto
Spam y Phishing	Amenazas informáticas	Oficial de Seguridad de la información	Correo electrónico	Anual
Qué hacer ante la pérdida de dispositivos móviles	Amenazas informáticas Higiene de Seguridad	Oficial de Seguridad de la información	Correo electrónico	Anual
Semana de seguridad de la información	Política de Seguridad Amenazas informáticas	Oficial de Seguridad de la información –Grupo Area Sistemas	Stand Correo electrónico	Anual

	Higiene de Seguridad Habeas Data		Sistema Multivisual Capacitaciones Presenciales	

9. IMPLEMENTACIÓN

A continuación se presenta Cronograma de implementación del Plan de Capacitación el cual es generada por Microsoft proyect:

Id	Nombre de tarea	Comienzo	Fin
0	**PLAN DE CAPACITACION Y SENSIBILIZACION EN SEGURIDAD DE LA INFORMACION**	**vie 15/02/19**	**vie 6/12/19**
1	**PLANEACIÓN**	**mar 2/07/19**	**vie 9/08/19**
2	**Identificacion de necesidades de capacitación**	**mar 2/07/19**	**vie 9/08/19**
3	Alineación de metodología con MSPI Minitic	lun 8/07/19	lun 8/07/19
4	Análisis Dofa	vie 12/07/19	vie 12/07/19
5	Definición de Perfiles y Necesidades	lun 15/07/19	vie 19/07/19
6	Definición de metas de capacitación	mar 16/07/19	mié 17/07/19
7	Diseño de la estrategia	lun 22/07/19	vie 26/07/19
8	Definición de Metas	lun 29/07/19	lun 29/07/19
9	Definición de temáticas de capacitación y sensibilización	lun 29/07/19	mar 30/07/19
10	Definición de medios y estrategias de Comunicación	mar 2/07/19	mar 2/07/19
11	Aprobación de la estrategia	mar 30/07/19	mié 31/07/19
12	Elaboración de Cronograma de Implementación	vie 9/08/19	vie 9/08/19
13	Entregable: Estrategia de Implementación	vie 9/08/19	vie 9/08/19
14	**DISEÑO**	**jue 28/02/19**	**mié 14/08/19**
15	**Diseño de Material de Capacitación INC**	**jue 28/02/19**	**vie 2/08/19**
16	Diseño textos de campañas seguridad de la información	jue 28/02/19	dom 31/03/19
17	Creación de Piezas e imágenes	mié 1/05/19	mié 31/07/19
18	Validación de Piezas e imágenes	mié 31/07/19	vie 2/08/19
19	Entregable: Piezas con Imágenes corporativas para despliegue	vie 2/08/19	vie 2/08/19
20	**Creación de Piezas e imágenes Sensibilización Gestión de seguridad Outsourcing**	**mié 24/07/19**	**mié 14/08/19**
21	Diseños Personaje Seguridad Campaña Expectativa	mié 24/07/19	mar 13/08/19
22	Validación de Piezas e imágenes	mié 14/08/19	mié 14/08/19
23	Entregable: Piezas con Imágenes corporativas para despliegue	mié 14/08/19	mié 14/08/19
24	**DESARROLLO**	**vie 15/02/19**	**vie 29/11/19**
25	**Capacitaciones Internas / Transmisión de conocimiento**	**vie 15/02/19**	**jue 29/08/19**

26	**Capacitación IPV6**	**vie 15/02/19**	**lun 25/02/19**
27	Jornada 1 - Capacitación Interna IPV6 -Password	vie 15/02/19	vie 15/02/19
28	Jornada 2 - Capacitación Interna IPV6 -Password	lun 25/02/19	lun 25/02/19
29	Sensibilización proyecto IPV6 para el INC + Phishing	mar 19/02/19	mar 19/02/19
30	**Workshop Fortinet - Fortiguard**	**jue 29/08/19**	**jue 29/08/19**
31	Jornada 1 workshop Fortigate	jue 29/08/19	jue 29/08/19
32	Jornada 2 workshop Fortigate	jue 29/08/19	jue 29/08/19
33	**Capacitación Usuario**	jue 11/04/19	vie 29/11/19
34	**GESTIÓN DEL CAMBIO - PROYECTO OUTSOURCING - CAMBIO PLATAFORMA SEGURIDAD**	**vie 19/07/19**	**vie 1/11/19**
39	Capacitación manejo de datos personales	jue 11/04/19	jue 11/04/19
40	Sensibilización para Dirección -Manejo datos Personales	vie 20/09/19	vie 20/09/19
41	**Despliegue en pantallas Multivisual - Capacitación Seguridad de la Información**	**lun 9/09/19**	**vie 15/11/19**
45	Qué hacer ante la pérdida de dispositivos móviles	mié 12/06/19	vie 14/06/19
46	Capacitación 5 Estafas Cibernéticas que todos deben Conocer en el INC	vie 26/07/19	lun 29/07/19
47	Capacitación en Estándar de Gerencia de la Información	mar 6/08/19	mar 6/08/19
48	**Sensibilizaciones SGSI**	**mar 25/06/19**	**vie 29/11/19**
49	Jornada Sensibilización Seguridad de la información y Riesgo Digital	lun 25/11/19	vie 29/11/19
50	Sensibilización en seguridad Comité Administrativo	lun 15/07/19	vie 26/07/19
51	Sensibilización Nueva politica de Seguridad de la información	vie 4/10/19	vie 11/10/19
52	Sensibilización para Jornada de Acreditación	mar 25/06/19	mié 26/06/19
53	Despliegue de tapices de escritorio	mar 15/10/19	jue 31/10/19
54	**SEGUIMIENTO**	**lun 2/12/19**	**vie 6/12/19**
55	Aplicación Encuesta- Estado de apropiación de seguridad de la información	lun 2/12/19	vie 6/12/19
56	Reevaluacion de Material Creado	mie 15/01/20	vie 30/01/20

10. DOCUMENTACIÓN

El registro de la asistencia a capacitaciones y sensibilizaciones del plan se realiza en formato **GTH-P05-F-08 Registro de asistencia a capacitaciones y entrenamientos**. Toda la documentación, material de capacitación y sensibilización y los registros de la asistencia se encuentran archivados en una ubicación centralizada en el sistema NNAS del INC, en la carpeta \\192.168.0.31\seguridad de la informacion\SGSI\Capacitación y Concienciacion\2019\

11. EVALUACIÓN.

Para la evaluación se elaborará una encuentra a los usuarios sobre del estado de sensibilización de seguridad de la información, utilizando el sistema de encuesta de Office 365 (Microsoft Forms)

- Disponibilidad de recursos y materiales
- Impacto en la organización, dependiendo del rol y cargo
- Conocimiento sobre la política de seguridad de la información
- Interiorización de los contenidos de Seguridad
- Identificación de necesidades de capacitación y/o reinducción
- Identificación de nuevas habilidades de entrenamiento

Con el resultado de esta primera evaluación se debe establecer el estado del plan, y las brechas o falencias que se hayan identificado y que se necesiten corregir para el año 2020,

12. FINANCIAMIENTO DEL PLAN DE CAPACITACIÓN

En 2019 no se cuenta con un presupuesto asignado al plan de capacitación y sensibilización, debido a que el SGSI del INC se encuentra en etapa de implementación. Los recursos y medios que se utilizarán son aquellos con los cuales ya cuenta en el instituto para el diseño y despliegue, y con la sensibilización en Gestión del Cambio en seguridad que se contrató de manera general con el cambio de Outsourcing. Para el año 2020 utilizando los resultados de la encuesta y evaluación del plan, se debe identificar que las áreas deben priorizar este aspecto de formación, para que el programa se desarrolle a plenitud.

Para el año 2020 se identifican unas necesidades básicas de financiamiento las cuales se presenta a continuación, y que deben tenerse en cuenta en la etapa de planeación financiera en 2019. Estas necesidades deben ser completadas con las necesidades que se identifiquen el ejercicio de evaluación de desarrollo del plan de 2019.

Necesidad	Presupuesto Estimado	Implementación
Implementación de curso virtual de seguridad de la información en campus virtual.	$9.000.000 IVA incluido	Primer semestre 2020
Semana de seguridad (Impresos-fichas técnicas cartillas-libretas material POP, Comparsa, obra teatro o Stand UP Comedy, conferencistas)	$ 6.000.000 IIVA Incluido	Segundo semestre 2020
Actualización - Capacitación Formal para los responsables en seguridad de la Información	N/A, Acceso a convenios MINTIC e ICETEX	Primer y segundo semestre de 2020
Material para Avisos de Tratamiento de datos personales	$500.000	Primer semestre 2020

13. CONTROL DE CAMBIOS

ELABORÓ		**REVISÓ**		**APROBÓ**	
Cargo:	Profesional especializado I	Cargo:	Coordinador	Cargo:	MIPG - Comité institucional de gestión y desempeño
Nombre	Carlos Andres Guerrero	Nombre	Luis Eduardo Martínez	Cargo:	Coordinador Grupo Área Sistemas
Dependencia:	Grupo Área Gestión de Sistemas	Dependencia:	Grupo Área Gestión de Sistemas	Dependencia:	Comité institucional de gestión y desempeño
Fecha:	01-08-2019	Fecha:	14-08-2019	Fecha:	23-08-2019

INDICE DE MODIFICACIONES				
Versión	Responsable	Cargo	Fecha	Descripción
1.0	Carlos Andres Guerrero	Profesional especializado I – oficial de seguridad de la información	01/08/2019	Creación del documento
1.0	Luis Martinez	Coordinador Grupo Area Gestión de Sistemas	14/08/2019	Aprobación de documento