PLAN DE SENSIBILIZACIÓN Y ENTRENAMIENTO

Plan aprobado en Comité Institucional de Gestión y Desempeño bajo acta No. 001 del día 30 de enero del 2025.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Rectoría de la Escuela Tecnológica Instituto Técnico Central para la formulación del PDI se acompañó de una firma con alta experiencia y demostrada idoneidad para adelantar metodológica y técnicamente todo el proceso de formulación del Plan de Desarrollo Institucional 2025 – 2032 con el apoyo de sus Directivos y la Oficina Asesorade Planeación y Desarrollo Institucional. Dentro del PDI se encuentra la misión "Somos una Institución Pública de Educación Superior que ofrece programas y servicios educativos integrales, articulando los niveles: técnico, tecnológico, profesional y posgrado, para personas éticas, emprendedoras, competentes e innovadoras que lideran el desarrollo de Colombia"; el cual inició con las propuestas del Programa de Gobierno 2024-2027 y la articulación con los planes; del orden Nacional, Departamental, Distrital y sectorial. Este se articuló en sus diferentes estrategias con los estamentos de la comunidad educativa de la ETITC y se socializó con el Consejo Académico, los docentes y estudiantes de Educación Superior, con los docentes de Bachillerato y con el personal Administrativo.

En la última década, la Seguridad de la Información, la Ciberseguridad y la Protección de la Privacidad han sido esenciales para la optimización de procesos y el funcionamiento eficiente de las organizaciones. Sin embargo, con la adopción de tecnologías avanzadas, surgen también amenazas y vulnerabilidades que pueden comprometer la disponibilidad, confidencialidad e integridad y la autenticación segura de la información contenida en las diversas plataformas de la Escuela, lo que podría afectar el desempeño normal de la institución. Para mitigar estos riesgos, contamos con certificado actualizado a la norma ISO/IEC 27001:2022 proporcionando un marco de gestión de seguridad de la información para proteger los activos de información.

Este enfoque incluye la implementación de controles tecnológicos y procesos adecuados, la gestión de los aspectos humanos que son los incidentes de seguridad más causados por la falta de conocimiento sobre las buenas prácticas de seguridad de la información y el papel crucial que cada individuo desempeña dentro de la institución. Considerando lo anterior, las actividades de seguridad de la información contempladas en el marco de la ISO 27001:2022 se centrarán en fortalecer la capacitación y sensibilización del recurso humano. Esto tiene como objetivo minimizar el riesgo de que el personal se convierta en el eslabón más débil en la cadena de seguridad. Para lograrlo, se implementará un Plan de Sensibilización y Entrenamiento en Seguridad de la Información, Ciberseguridad y Protección de la Privacidad el cual contribuirá al cumplimiento del objetivo No. 3 del SGSI: "Sensibilizar y capacitar a la comunidad educativa sobre los cambios y actualizaciones en el SGSI, con un enfoque en la prevención y la promoción de una cibercultura, alineada con mecanismos específicos de verificación de identidad."

2. OBJETIVO

Definir las actividades para sensibilizar y entrenar en temas de seguridad de la información a todos los servidores públicos, estudiantes y partes interesadas de la ETITC, logrando con esto, un alto índice de cultura que favorece la preservación de la confidencialidad, integridad, disponibilidad y la autenticación segura como principios esenciales para garantizar la continuidad del servicio.

3. ALCANCE

El Plan de Sensibilización y Entrenamiento está dirigido a todos los servidores públicos, estudiantes, docentes y partes interesadas de la ETITC, que tienen acceso a los recursos informáticos, sistemas de información e instalaciones físicas.

4. ROLES Y RESPONSABILIDADES

Profesional de Seguridad de la Información: Debe elaborar el Plan de Sensibilización y Entrenamiento de la ETITC, de acuerdo con el contexto de la organización y a los aspectos de seguridad de la información, que constituyen falencias en el recurso humano. Dictar las charlas de sensibilización.

Comité Institucional de Gestión y Desempeño: Debe aprobar, mediante Acta, el Plan de Sensibilización y Entrenamiento para funcionarios de la ETITC, así mismo comprometerse a fomentar con nuevos conocimientos en materia de Ciberseguridad para sus funcionarios y realizar observaciones que permitan mejorar su funcionalidad.

Servidores Públicos: Deben participar en las actividades de sensibilización y/o entrenamiento planificadas y leer comunicados emitidos a través de los boletines por medio del correo institucional, redes sociales o de comunicación adaptados para su divulgación.

5. DEFINICIÓN DE TÉRMINOS

ACTIVO DE INFORMACIÓN: Es la información tratada o sistema dentro de la entidad que genera valor para la misma, puede ser de tipo software, servicio, hardware o documental.

AMENAZA: Es una situación perjudicial que al presentarse puede traer consecuencias negativas para los activos de información provocando su indisponibilidad o mal funcionamiento, incluso puede traer pérdida directa del valor que genera.

ADWARE: Se trata de un tipo de software que, de modo automático, exhibe al usuario anuncios publicitarios. De este modo, el fabricante del software obtiene ganancias a partir de estas publicidades.

ANTIVIRUS: Es un software diseñado para detectar, bloquear y eliminar un código malicioso y de esta forma proteger los equipos de otros peligros o malware.

ANÁLISIS DE RIESGOS: Es un procedimiento que permite identificar amenazas y vulnerabilidades de los activos de información, así como medir el impacto de estos. Su objetivo es determinar controles adecuados para tratar el riesgo.

APT - ADVANCED PERSISTENT THREATS: Es un tipo de ataque dirigido a una empresa u organización que se infiltra para el robo o pérdida de información confidencial durante un período de tiempo determinado.

ATAQUE MAN IN THE MIDDLE – ATAQUE DE INTERMEDIARIO: Es un tipo de ataque donde el hacker es capaz de observar e interceptar mensajes entre sus víctimas y que ninguna de ellas se dé cuenta que han sido violada la información.

AUTENTICACIÓN: Es un procedimiento que nos permite comprobar que alguien es quién dice ser cuando accede a un servicio online y su principal funcionalidad es lograr una comunicación segura.

BACKUP: Es una copia de seguridad que se realiza sobre toda la información contenida y su finalidad consiste en recuperar los datos en el caso de que los sistemas sufran daños o pérdidas accidentales de los datos almacenados.

BAITING: Es un tipo de ataque de ingeniería social conocido también como gancho o cebo. Este ataque consiste en dejar anclado un dispositivo de almacenamiento extraíble como usb, cd, dvd, o móvil, infectado con un software malicioso en algún lugar visible para tentar a la víctima a cogerlo y ver el contenido del mismo. Una vez se ejecuta en el computador, este malware hará todo su trabajo automáticamente.

BIA – BUSINESS IMPACT ANALYSIS: Es un informe que muestra el costo por interrupción de procesos críticos de negocio y define objetivos de impacto y recuperación de cada uno de ellos.

BIOMETRÍA: Este es un método de reconocimiento de personas basado en características fisiológicas del cuerpo humano como huellas dactilares, retinas, iris o rostro.

BOTS: El término viene de la palabra "robot", es un software que realiza tareas repetitivas, predefinidas e incluso automatizadas. Actualmente existen bots informáticos y bots de internet y ambos actúan para engañar y robar información.

BOTNET: Es un conjunto de computadoras denominadas bots, son controlados remotamente por un atacante y suelen ser utilizados para realizar actividades maliciosas como el envío de spam, ataques de DDoS (Denegación de Servicio).

CERTIFICADO SSL – SECURE SOCKET LAYER: Es un protocolo de seguridad que sirve para brindar seguridad al visitante de una página web e informa a los mismos de que la web es real, auténtica y confiable para ingresar datos personales o realizar transacciones.

CSIRT: Es el Centro de Respuesta a Incidentes de Seguridad Informática y su objetivo principal es el de detectar, prevenir y mitigar ataques a los sistemas de información.

CIBERSEGURIDAD: Es un conjunto de prácticas diseñadas para defender los sistemas de información, redes de datos, computadoras, dispositivos móviles y prevenir ataques maliciosos.

CORTAFUEGOS (FIREWALL): Es un sistema de seguridad de software o hardware que su objetivo se centra en la denegación de tráfico de internet de acuerdo con las normas y políticas de seguridad y privacidad de la información.

CRIPTOGRAFÍA: Es una técnica usada especialmente para cifrar un mensaje convirtiéndolo en un mensaje cifrado o criptograma.

DECEPTION AD: Técnica de seguridad cibernética que consiste en crear anuncios falsos o engañosos para desviar su atención de los sistemas reales.
DEEP FAKES – FALSEDADES PROFUNDAS: Son archivos de imagen, video o de voz que se manipulan mediante un software de inteligencia artificial para aparecer originales, auténticos y reales.

DEEP WEB: Son páginas web que no están indexadas en ninguno de los buscadores conocidos. Solo expertos pueden ingresar de forma transparente para compartir información acerca de vulnerabilidades de los sistemas de información, expandir botnets, adquirir amenazas dirigidas, herramientas para crear ransomware, phishing, etc.

DDOS (DENEGACIÓN DE SERVICIO): Es un tipo de ataque informático en el que consiste en saturar con peticiones de servicio al servidor y provocar su colapso.

EXPLOIT: Es una secuencia de comandos para aprovecharse de un fallo o una vulnerabilidad en un sistema y provocar un comportamiento no deseado.

ENTRENAMIENTO: Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas a su cargo.

FILTRACIÓN: Este término es el más utilizado por los ciberdelincuentes y su objetivo se enfoca en romper los filtros de seguridad informática para llevar a cabo el objetivo de su ataque.

FUGA DE DATOS: Es la pérdida de información privada o confidencial de una persona o empresa y que termina siendo visible o accesible para otros usuarios.

GUSANO: Es un software malicioso o malware que tiene un alto grado de propagación.

HACKING ÉTICO: Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión

maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

HARDENING: Es el proceso de reforzar la seguridad de un sistema, red o dispositivo reduciendo sus vulnerabilidades y configurándolo para minimizar los riesgos de ser atacado.

INGENIERÍA SOCIAL: Es la práctica de obtener información confidencial, a través de la manipulación de usuarios legítimos.

INYECCIÓN SQL: Es un ataque que se aprovecha de las vulnerabilidades en una validación de contenidos introducidos en un formulario web y permite la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web como por ejemplo las credenciales de acceso.

LOGS: Es el registro o datos de quién, qué, cuándo, dónde y porqué un evento ocurre para un sistema en particular o un dispositivo.

MALWARE: Software malicioso, software dañino o software malintencionado. Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información, sin el consentimiento de su propietario.

OAuth - OAuth2: Son protocolos diseñados para permitir el acceso autorizado a recursos sin compartir credenciales sensibles, siendo OAuth2 la versión más moderna y ampliamente utilizada por su flexibilidad y capacidad para adaptarse a diferentes necesidades de autorización.

P2P PEER TO PEER: Es un modelo de comunicaciones entres sistemas o servicios en el cuál todos los nodos extremos son iguales, contienen las mismas capacidades y cualquiera de ellas puede iniciar una comunicación.

PARCHE DE SEGURIDAD: Es un conjunto de cambios que se aplican a un software con el fin de corregir errores de seguridad en programas o sistemas operativos.

PENTESTING: Son pruebas de penetración con ataques hacia los sistemas informáticos con la intención de encontrar sus debilidades o vulnerabilidades. Este tipo de pruebas aclaran los peligros que corren los sistemas y da una visión detallada de las defensas informáticas.

PHARMING: Es una de las variantes del Phishing, consiste en hacer creer al usuario que visita una página web que está es un sitio oficial y seguro, pero en realidad el usuario navega dentro de la web del hacker con la finalidad de obtener credenciales o apropiarse de identidad de alguien.

PHISHING: Es un tipo de estafa a través de medios remotos, correos y el estafador intenta conseguir de usuarios legítimos, información confidencial y sensible como contraseñas o datos bancarios entre otros.

PLAN DE CONTINGENCIA: Es una estrategia planificada en fases y se encuentra constituida por un conjunto de recursos de respaldo ante una emergencia, encaminados a conseguir el restablecimiento ordenado, progresivo y seguro de los sistemas de información que soportan los procesos de negocio considerados críticos y hacen parte del plan de continuidad de la institución.

PLAN DE CONTINUIDAD: Es un conjunto de planes de actuación, de emergencia, de comunicaciones y planes de contingencia destinados a mitigar el impacto provocado por los riesgos sobre la información y sus procesos de negocio de una institución.

POLÍTICA: Declaraciones de alto nivel que expresan los objetivos a cumplir de la entidad respecto a algún tema en particular.

POLÍTICA DE SEGURIDAD: Son medidas de seguridad donde la empresa toma decisiones en base a la seguridad de la información para evaluar el valor de sus activos y los riesgos a los que están expuestos.

RANSOMWARE: Es una técnica utilizada por los ciberdelincuentes donde toman control del equipo infectado, secuestrando la información y de esta forma pedir rescate económico para la recuperación de la información.

ROGUE: Es un software malicioso cuyo objetivo es la de hacer creer que una computadora está infectada por algún virus haciendo pagar una suma de dinero por el usuario.

ROOTKIT: Permite un acceso de privilegio continuo a una computadora, pero que mantiene su presencia activamente oculta al control de los administradores, al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones.

SENSIBILIZACIÓN: Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

SCAREWARE: Es un software malicioso que engaña al usuario para que visiten sitios infestados de malware, estos también pueden darse en forma de ventanas emergentes.

SMISHING: Es una de las técnicas de ingeniería social que se envían a través de mensajes SMS o de texto y hacerle creer a su víctima publicidad engañosa; donde el hacker busca obtener credenciales a sus cuentas bancarias o datos personales relevantes.

SNIFFER: Es un software que monitorea la información que circula por la red con el objetivo de capturarla. El tráfico de información que no esté cifrada podrá ser escuchado de forma íntegra.

SPEAR PHISHING: Es una de las variantes del phishing, donde el estafador envía mensajes a su víctima haciéndose pasar de que lo conoce, y su objetivo se centra en la búsqueda de datos confidenciales que pueden utilizar para explotar o vender en el mercado negro.

SPAM: Son mensajes no solicitados, no deseados o de remitente desconocido, enviados en grandes cantidades (incluso masivas), que perjudican de alguna o varias maneras al receptor.

SPYWARE: El spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa, sin el conocimiento o el consentimiento del propietario del ordenador.

TRASHING O DUMPSTER DIVING: Práctica de buscar datos sensibles o información personal en documentos tirados por las empresas o individuos, con el fin de obtener acceso a sistemas o realizar fraudes.

VIRUS INFORMÁTICO: Es un tipo de malware diseñado para propagarse de un host a otro y tiene habilidad de replicarse. Tiene como objetivo el de alterar el correcto funcionamiento de un dispositivo, infectando los ficheros de un computador mediante código maligno.

VISHING: Es un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima. Este intento de estafa busca obtener datos personales y bancarios a través de la recepción de llamadas telefónicas. En algunos casos te manifiestan ofertas económicas, seguros de vida, etc.

VULNERABILIDAD: Son las debilidades, huecos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la institución (amenazas), las cuales se constituyen en fuentes de riesgo.

WHALING: Es un tipo de estafa. Su objetivo se centra en enviar un mensaje para hacerse pasar como una autoridad, jefe o ejecutivo de una institución, creando una historia con contenido muy realista para pedirle a su víctima la transferencia de dinero o fondos a la cuenta del estafador.

WHISHING: Es una de las variantes del phishing, pero en este caso se utiliza la aplicación de whatsaap para el envío de mensajes para ofrecer promociones de marcas reconocidas o incluso difundiendo que se ha ganado un premio.

ZERO-DAY: Es un tipo de vulnerabilidad en un software que es conocida por determinados atacantes y que son desconocidas por los fabricantes y los usuarios. En ellos no existe un parche de seguridad para solucionarlas y

pueden ser explotadas sin que el usuario sea consciente de que es vulnerable.

ZOMBIE: Este es el nombre que los ciberdelincuentes utilizan para controlar los computadores de manera remota. Actualmente se utilizan las computadoras zombie para desarrollar actividades ilícitas a través de internet como el envió de mensajes no deseados o la propagación de malware.

6. TEMAS DE SENSIBILIZACIÓN IDENTIFICADOS

a. Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad
b. Activos de información
c. Inducción IBTI, PES, Docentes, Servidores Públicos y partes interesadas
d. Inducción y Reinducción a Servidores Públicos
e. Phishing e Ingeniería Social
f. Protección de Datos durante el Trabajo en Casa
g. El Bullying y Ciberacoso
h. Cibercultura para padres de familia
i. Gestión de contraseñas
j. Desintoxicación digital
k. Ciberhigiene y Tips de Seguridad Digital

7. CRONOGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN

ACTIVIDADES	FECHA	RESPONSABLE
Inducción a estudiantes de IBTI, PES, Docentes, Servidores públicos y partes interesadas.	Enero y Febrero 2025	Profesional de SGSI
Infografía acerca de Cibercultura para padres de familia por aplicativo de Gnosoft	Febrero 2025	
Guía de Gestión de Contraseñas divulgación por correo institucional y aplicativos académicos	Febrero 2025	
Mesas de Trabajo con los veinte (20) líderes de los procesos para diligenciamiento correcto de matriz de activos de información	Febrero y Marzo de 2025	
Crear aula virtual con intensidad de ocho (8) horas para abarcar temas de sensibilización identificados para servidores públicos	Marzo 2025	
Desintoxicación digital, Ciberhigiene y Tips de Seguridad Digital	Julio 2025	
El Bullying y Ciberacoso	Septiembre 2025	
Protección de Datos durante el Trabajo en Casa	Primer día de Trabajo en Casa	
Divulgación de alertas de Seguridad de la Información	Durante la vigencia	
Phishing e Ingeniería Social	Durante la vigencia	

8. ENTRENAMIENTO IDENTIFICADO

1. Hardening y Ethical Hacking
2. Mitigación de Riesgo IOT e Inteligencia de Artificial
3. Simulaciones y Ejercicios Técnicos de Ciberseguridad
4. Aseguramiento de evidencias digitales, Análisis Forense Digital e Inteligencia de Amenazas.

9. CRONOGRAMA DE ENTRENAMIENTO

TEMA	FECHA	RESPONSABLE
Hardening y Ethical Hacking Mitigación de Riesgo IOT e Inteligencia de Artificial Simulaciones y Ejercicios Técnicos de Ciberseguridad Aseguramiento de evidencias digitales, Análisis Forense Digital e Inteligencia de Amenazas.	Durante la vigencia 2025	Departamento Administrativo de la Función Pública Ministerio de Tecnologías de la Información y Comunicaciones de Colombia Vicerrectoría Administrativa y Financiera Rectoría – Planeación Gestión de Talento Humano

10. MÉTRICAS

Para medir la efectividad de las acciones de toma de conciencia y comunicación en el plan de capacitación y sensibilización, se definen métricas claras que evalúan el conocimiento adquirido y el impacto en el comportamiento de los participantes. A continuación, presento algunas métricas clave para el cumplimiento de este:

- Asegurar una tasa de participación del 90% o más.
- Obtener un aumento del 30% en el conocimiento de los participantes tras la capacitación.
- Al menos un 75% de los participantes debe demostrar la aplicación práctica de las mejores prácticas de seguridad.
- Lograr al menos un 80% de respuestas correctas en los simulacros.

- Reducir los incidentes en un 30% en el periodo posterior a la capacitación.

11. BIBLIOGRAFÍA CONSULTADA

- Guía No. 14 Plan de Capacitación, Sensibilización y Comunicación de la Seguridad de la Información - MINTIC.
- NIST (National Institute Of Standards And Technology) Special Publication 800-50. Building an Information Technology Security Awareness and Training Program.
- ISO/IEC 27035, Information Technology. Security Techniques. Information Security Incident Management
- ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary and Requirements.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas – DAFP.

12. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
01/03/2017	1	Adopción del Documento.
09/04/2018	2	Adición de la sección para etiquetar el documento. Actualización de la sección Roles y Responsabilidades. Actualización de la sección Temas de Sensibilización Identificados. Actualización de la sección Cronograma de Sensibilización. Actualización de la sección Temas de Entrenamiento Identificados. Actualización de la sección Cronograma de Entrenamiento. Ingreso al sistema de gestión integrado.
01/04/2019	3	Redacción del documento. Actualización de la sección Definición de términos. Actualización de la sección Roles y responsabilidades. Actualización de la sección Temas de Sensibilización Identificados. Actualización de la sección Cronograma de Sensibilización.

		Actualización de la sección Temas de entrenamiento identificados. Actualización de la sección Cronograma de Entrenamiento.
16/10/2019	4	Actualización de la sección Roles y responsabilidades.
21/01/2022	5	Redacción del documento. Actualización de la sección Roles y responsabilidades. Actualización de la sección Definición de términos. Actualización de la sección Temas de Sensibilización Identificados. Actualización de la sección Cronograma de Sensibilización y Capacitación. Actualización de la sección Entrenamiento identificado. Actualización de la sección Cronograma de Entrenamiento.
18/01/2023	6	Actualización de la sección Temas de Sensibilización Identificados. Actualización de la sección Cronograma de Entrenamiento.
26/01/2024	7	Actualización de las secciones de Temas de Sensibilización, Entrenamiento identificado y Cronograma de Entrenamiento.
27/01/2025	8	Actualización del Plan de Sensibilización y Entrenamiento de acuerdo con los nuevos lineamientos del Plan de Desarrollo Institucional 2025-2032 en su Meta Estratégica "Alcanzar el 92% en el Índice de Desempeño Institucional del FURAG." – Cronograma – Entrenamiento y Métricas.

ELABORÓ	REVISÓ	APROBÓ
Ing. SANDRA J. GUERRERO G. Líder de Gestión de Seguridad de la Información	**ANAY PINTO** Administrador de la Documentación	**COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO**