El riesgo es inherente a todos los procesos, desarrollemos juntos una buena gestión.

Conoce nuestro Cyber Plan

Ing. Sandra Guerrero

Profesional de Gestión de Seguridad de la Información ETITC

Seguridaddigital

Escuela Tecnológica Instituto Técnico Central

Establecimiento Público de Educación Superior

"Generando conciencia digital en nuestra red ETITC"

PLAN OPERATIVO DE SEGURIDAD DE LA INFORMACIÓN

Vigencia 2022

TABLA DE CONTENIDO

Cll 13 No. 16 - 74. / Teléfono Conmutador +57 (601) 344 3000 / www.etitc.edu.co. / atencionalciudadano@itc.edu.co. Bogotá, D. C. - Colombia

1. INTRODUCCIÓN

La Escuela Tecnológica Instituto Técnico Central (ETITC) considera la información que gestiona, recolecta y custodia, como un elemento indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Institución, razón por la cual es necesario que la misma, establezca un marco, en el cual, se asegure que la información es protegida de manera adecuada, independientemente, de la forma en la que ésta sea manipulada, procesada, transportada o almacenada.

Por lo anterior, el presente plan describe las actividades a desarrollar durante la vigencia 2022 definidas por la ETITC. Para la elaboración del mismo, se toma como referencia la norma ISO 27001:2013 y los lineamientos de la estrategia Gobierno Digital, en especial las guías suministradas para el Modelo de Seguridad y Privacidad de la Información que tienen como objetivo, gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos. Dichos requisitos y lineamientos serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la ETITC.

2. OBJETIVO DEL PLAN OPERATIVO DE SGSI

Establecer actividades contempladas de acuerdo al Modelo de Seguridad y Privacidad de la Información que están alineadas con la NTC/IEC ISO 27001:2013 y con la Política de Seguridad y Privacidad de la Información de la Escuela Tecnológica Instituto Técnico Central.

3. ALCANCE

El plan anual de seguridad de la información aplica a los procesos de la Escuela Tecnológica Instituto Técnico Central, donde se da cumplimiento de los requisitos y lineamientos, que tienen como objetivo, gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos.

4. TERMINOS Y DEFINICIONES

DELITO INFORMÁTICO: Se conoce como delito informático cualquier acción ilícita o criminal que atente a aun sistema informática con el fin de causar un daño que atente a aun programa, sistema de procesamiento de información etc.

CIBERSEGURIDAD: La ciberseguridad se refiere a un conjunto de técnicas utilizadas para proteger la integridad de la arquitectura de seguridad de una organización y proteger sus datos contra ataques, daños o acceso no autorizado

INTEGRIDAD: La integridad se refiere a la cualidad de la información en la cual se debe ser legitima, sin modificación y correcta, esto quiere decir que debe encontrarse en un estado original manteniendo su estructura tal cual como fue generada sin ningún tipo de alteración por parte de terceros.

DISPONIBILIDAD: La disponibilidad se refiere a aquella información que se encuentra disponible y que se puede acceder a través de los medios y los canales adecuados en cualquier momento.

CONFIDENCIALIDAD: La confidencialidad se refiere a la propiedad de la información para ser suministrada únicamente usuarios autorizados a dicha información, por consiguiente, solo resultada accesible con una debida comprobación de los usuarios para ser accedida.

AUTENTICIDAD: La autenticidad se refiere a dicha situación en la cual se hace la verificación de que un documento pertenece o ha sido elaborado por quien dice ser el autor o dueño de un documento. En dicha situación se hace la verificación de la identidad del usuario en la cual se confirma que dicha persona es quien dice ser, por consiguiente, si su identidad es auténtica será esta persona será autorizada.

NO REPUDIO: Es el servicio en el cual se relaciona con la autenticación y la aprobación de la participación de dos o más partes (emisor y receptor) en la comunicación y transmisión de la información. De la anterior, el no repudio puede ser tanto “No Repudio en Origen” y “No repudio en Destino”. Por consiguiente, el no repudio se refiere a que si en un caso el emisor y el recetor niegan haber recibido y enviado información cualesquiera de los dos pueden probar que si se ha efectuado.

5. NORMATIVIDAD

NORMA	DESCRIPCIÓN
Constitución Política de Colombia	Artículo 15.
Ley 527 de 1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000	Por medio de la cual se expide la Ley General de Archivos.
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1221 del 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TICS se crea la agencia Nacional de espectro y se dictan otras disposiciones.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
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 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Ley 1978 de 2019	Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de 2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
Decreto 620 de 2020	Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 2999 del 2008	Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
Resolución 2034 de 2016	Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
Resolución 2306 de 2020	Por la cual se actualiza el Modelo Integrado de Gestión (MIG) del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se deroga la Resolución 911 de 2018
Resolución 1151 de 2019	Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga la Resolución 0002133 del 3 de agosto de 2018
Resolución 924 de 2020	Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo Único de TIC y se deroga la resolución 2007 de 2018.
Resolución 2256 de 2020	Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 1124 de 2020.
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016	Política Nacional de Seguridad digital.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.

Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 331 de 2020	Por la cual se adoptan de los instrumentos de la gestión de la información pública de la ETITC.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Directiva presidencial 03 de 2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

6. PLAN OPERATIVO DE SEGURIDAD DE LA INFORMACION

A continuación se determinan las actividades del plan operativo del Sistema de Gestión de Seguridad de la Información para el periodo comprendido entre el 01 de febrero hasta el 16 de diciembre de 2022.

Gestión	Actividades	Tareas	Fecha de Programación de Tareas	
			Fecha Inicial	Fecha Final
Activos de la Información.	Levantamiento de Activos de Información.	Identificar nuevos activos de información en cada dependencia.	01-Feb-2022	30-Sep-2022
	Publicación de Activos de Información.	Actualizar el Inventario de Activos de registro de activos de información, índice de información clasificada y reservada.	03-Oct-2022	31-Oct-2022
Gestión de Riesgos.	Identificación de Riesgos de Seguridad de la Información.	Identificar, Analizar y Evaluar los riesgos inherentes relacionados con la Seguridad de la Información, Seguridad Digital y Continuidad de los servicios de la ETITC.	01-Feb-2022	30-Jun-2022
	Administrar los Riesgos de Seguridad de la Información.	Verificar y administrar el cumplimiento de los riesgos de seguridad de la información y mantenerlos en niveles aceptables de acuerdo a la guía para la administración del riesgo y el diseño de controles en entidades públicas en su versión No. 5.	01-Feb-2022	16-Dic-2022
	Revisión de Riesgos de acuerdo a los requisitos de la norma NTC ISO 27001:2013.	Revisión de cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y de auditorías internas planificadas a intervalos regulares.	01-Feb-2022	16-Dic-2022
	Monitoreo de Riesgos de Seguridad de la Información con herramientas especializadas del SGSI.	Generación, presentación y reporte de monitoreo al directorio activo y servidor de archivos para evidenciar los riesgos de Seguridad y que brindan cumplimiento a la NTC ISO 27001:2013, a través de la herramienta SIEM.	01-Feb-2022	16-Dic-2022
Gestión de Incidentes de Seguridad de la Información. ⬇	Eventos y Vulnerabilidades.	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI.	01-Feb-2022	16-Dic-2022

Gestión	Actividades	Tareas	Fecha de Programación de Tareas	
			Fecha Inicial	Fecha Final
Gestión de Incidentes de Seguridad de la Información.	Realizar actividades de Hacking Ético y Pentesting Interno y Externo.	Realizar escaneo para encontrar vulnerabilidades y fallos de seguridad, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos.	01-Feb-2022	16-Dic-2022
	Participar en los grupos de respuesta a incidentes (CSIRT).	Socializar boletines informativos de eventos de seguridad de la información a toda la comunidad de la ETITC e integrarlos con las CSIRT de Gobierno.	01-Feb-2022	16-Dic-2022
	Reportes periódicos herramienta SIEM.	Realizar seguimiento a los informes del SIEM asociados a SGSI, de acuerdo a la severidad del incidente notificar a Informática y Comunicaciones para realizar ajustes a Infraestructura de TI.	01-Feb-2022	16-Dic-2022
	Gestionar los incidentes de Seguridad de la Información identificados.	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento.	01-Feb-2022	16-Dic-2022
Gestión de Seguridad de la Información.	Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas en temas relacionados al SGSI.	Correos sospechosos	01-Feb-2022	16-Dic-2022
		Escritorio limpio y sesiones cerradas		
		Políticas de Seguridad y Privacidad de la Información		
		Procedimientos de Seguridad de la Información		
		Contexto actual de Seguridad Informática		
		¿Qué son los Malware?		
		Gestión de contraseñas		
		¿Qué es Ingeniería Social?		
		Hacking Ético		
		¿Qué es Ciberseguridad?		
	Constante entrenamiento para el SGSI.	Recibir capacitaciones en temas identificados como Gestión de Riesgos, Criptografía, Rol de la IA, Hackeo Ético, Mitigación de Riesgo IOT y Pruebas de Penetración.	01-Jun-2022	16-Dic-2022
	Realizar actividades pertinentes para mantener la certificación del Sistema de Gestión de Seguridad de la Información NTC ISO 27001.	Registros de actividades desarrolladas para mantener la certificación del sistema de seguridad de la información NTC ISO 27001:2013	01-Feb-2022	16-Dic-2022
	Actualización los avances del MSPI y respectivamente del SGS.	Actualizar la documentación, espacio web del SGSI y avances en el Modelo de Seguridad y Privacidad de la Información y del Sistema de Gestión de Seguridad de la Información.	01-Feb-2022	16-Dic-2022
	Revisión de los controles del Anexo A. de la norma NTC ISO 27001:2013	Aplicar estrategias para validar el cumplimiento de la Política General de Seguridad y Privacidad de la Información.	01-Feb-2022	16-Dic-2022

Gestión	Actividades	Tareas	Fecha de Programación de Tareas	
			Fecha Inicial	Fecha Final
Acciones correctivas y de mejora al Sistema de Gestión de Seguridad de la Información.	Acompañamiento a Entidades del sector Educación, Gobierno en Línea y Seguridad Digital.	Participar en los talleres de acompañamiento a las entidades adscritas y vinculadas al sector educación en la implementación de políticas de gobierno y seguridad digital.	01-Feb-2022	16-Dic-2022
Planeación del Sistema de Gestión de Seguridad de la Información.	Revisión Manual Políticas de Seguridad de la Información.	Actualizar el Manual Políticas de Seguridad de la Información.	01-Feb-2022	16-Dic-2022
Gobierno Digital.	Modelo de Seguridad y Privacidad de la Información y Seguridad Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	01-Feb-2022	16-Dic-2022
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la normatividad vigente.		
Auditorías Internas y Externas.	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas programadas en el Plan Anual de Auditorías.	01-Feb-2022	16-Dic-2022
		Participar en auditorías externas de la norma ISO 27001:2013	01-Feb-2022	28-Feb-2022
Protección de datos personales.	Revisión de bases de datos.	Socializar y revisar la información recolectada por las diferentes áreas de la ETITC mediante el manual de anonimización.	01-Feb-2022	16-Dic-2022

Cordialmente,

Ing. Sandra J. Guerrero G.
Gestión de Seguridad de la Información
seguridaddigital@itc.edu.co
seguridaddigital