PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FECHA DE ELABORACIÓN: 27 de enero de 2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Escuela Tecnológica Instituto Técnico Central, a través de su Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno en Línea (GEL), dicta el 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. Dichos requisitos y lineamientos serán aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación de la Escuela, por tal motivo, deberán ser conocidos y cumplidos por todo el recurso humano (servidores públicos, proveedores y terceros), que accedan a los sistemas de información e instalaciones físicas de la Institución.

2. OBJETIVO

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, se encuentran basados, en el marco de lo establecido, en la norma internacional NTC-ISO-IEC 27001:2013 y las buenas prácticas contenidas en el componente Seguridad y Privacidad de la Información

3. ALCANCE

El plan de seguridad y privacidad 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. TERMINOLOGÍA:

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.

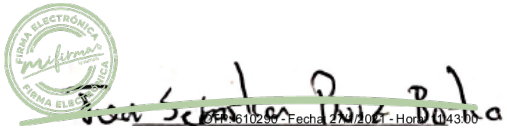
5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Gestión	Actividades	Tareas	Inicio	Terminación
Gestión de riesgos	Sensibilización	Sensibilizar y capacitar a los servidores públicos, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información institucionales.	1/02/2021	30/11/2021
	Monitoreo y revisión	Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.	1/02/2021	30/11/2021
	Identificación de riesgos	Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.	1/02/2021	30/11/2021
	Reportes mediante la herramienta SIEM	Reportes periódicos herramienta SIEM	1/04/2021	30/11/2021
Activos de información	Actualizar el Inventario de Activos de	Inventario de activos de información actualizado, registro de activos de	1/02/2021	30/11/2021

	Información de la ETITC y realizar informe.	información, índice de información clasificada y reservada.		
Seguridad de la información	Gestionar incidentes de seguridad de la información.	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento.	1/02/2021	30/11/2021
	Eventos/ Vulnerabilidades.	Informes periódicos herramienta SIEM y así mismo análisis de vulnerabilidades externos. Informe técnico.	1/04/2021	30/11/2021
	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	1/02/2021	30/11/2021
	Revisar los avances del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información, y actualizar de la documentación respectiva	Actualización de la documentación y avances en el MSPI y SGSI.	1/02/2021	30/11/2021
	Entidades y equipos de respuesta a incidentes(CSIRT,COLCERT) ETC	Socializar boletines informativos de seguridad de la información En la ETITC	1/01/2021	30/11/2021

Gobierno Digital	Gobierno Digital	Actualización del documento autodiagnóstico de la ETITC en la implementación de seguridad y privacidad de la información	1/01/2021	30/11/2021
		Revisar la implementación del plan de seguridad digital en la ETITC	1/01/2021	30/11/2021
Auditorías Internas Y Externas	Interna	Participación en las auditorías internas	1/01/2021	30/11/2021
	Externa	Participación auditoria externa Norma ISO 27001:2013	1/02/2021	28/02/2021
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.	1/01/2021	30/11/2021

Elaboro:



Ing. Juan Sebastian Ruiz Botia
Gestión de Seguridad de la Información
seguridaddigital@itc.edu.co