MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ETITC

TABLA DE CONTENIDO

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 tal motivo, el presente manual describe las políticas de seguridad de la información definidas por la ETITC. Para la elaboración de este, se toma como base el Anexo A, incluido en la norma ISO 27001:2013 y los lineamientos de la estrategia Gobierno Digital, en especial las guías suministradas para el MSPI.

Las políticas de seguridad de la información incluidas en este manual constituyen una parte fundamental del SGSI y MSPI de Gobierno Digital, estas se convierten en la base para la implementación de los controles, procedimientos y estándares definidos.

La preservación de la confidencialidad, integridad y disponibilidad de la información para la ETITC constituye una prioridad y, por tanto, es responsabilidad de todos hacer el respectivo cumplimiento de las políticas contenidas en este manual.

2. OBJETIVO

Establecer las políticas de seguridad de la información para la ETITC, con el fin de cumplir con los requisitos de seguridad, definidos en el SGSI y el MSPI de Gobierno Digital, que ayudarán, mediante su implementación, a preservar la confidencialidad, integridad y disponibilidad de la información en la ETITC.

3. ALCANCE

Todas las políticas de seguridad de la información, contenidas en este manual, serán aplicadas a los procesos estratégicos, misionales, de apoyo y de evaluación de la ETITC, por tal motivo, deberán ser conocidas y cumplidas por todos los Servidores Públicos, Proveedores y demás partes interesadas, que accedan a los sistemas de información, repositorios e instalaciones físicas de la ETITC.

4. TÉRMINOS Y DEFINICIONES

Activo de información: Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la ETITC y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento, en los que los servidores públicos de la ETITC, manifiestan su voluntad de mantener la confidencialidad de la información de la ETITC, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan

acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: Es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la ETITC para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio de la información: Son los líderes de las áreas definidas para la ETITC.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Directriz: Es una norma o una instrucción que se tiene en cuenta para realizar una tarea. También se trata de aquello que fija cómo se producirá algo. Las directrices, por lo tanto, sientan las bases para el desarrollo de una actividad o de un proyecto.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

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.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Es la protección de la exactitud y estado completo de los activos. Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al Instituto.

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información, a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: Son los líderes de procesos de la ETITC.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre

otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la ETITC.

Registros de Auditoría: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la ETITC. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la ETITC o de origen externo, ya sea adquirido por el Instituto como un producto estándar de mercado o desarrollado para las necesidades de éste.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Teletrabajo suplementario: Trabajadores con contrato laboral que alternan sus tareas en distintos días de la semana entre la institución y un lugar fijo fuera de ella. Se entiende que teletrabajan al menos dos días a la semana.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la ETITC.

Vulnerabilidades: Son las debilidades, hoyos de seguridad o falencias inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el Instituto (amenazas), las cuales se constituyen en fuentes de riesgo

5. POLÍTICA GENERAL DE SISTEMA DE GESTIÓN INTEGRADO

La Escuela Tecnológica Instituto Técnico Central (ETITC), es un Establecimiento Público de Educación Superior, de carácter académico, de orden Nacional, con personería jurídica, autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional. La ETITC consciente de la importancia que la seguridad de la información, la seguridad y salud en el trabajo, la gestión ambiental y gestión de calidad del servicio tienen para el desarrollo y buen funcionamiento de sus procesos internos, ha decidido implementar un Sistema de Gestión Integrado, basado en las normas internacionales NTC-ISO-IEC 27001:2013, NTC-ISO-45001:2018, NTC-ISO-14001:2015 y NTC-ISO-9001:2015, el Modelo de Seguridad y Privacidad de

la Información de Gobierno Digital, el Modelo Integrado de Planeación y Gestión y los requisitos legales y de otra índole vigentes que le sean aplicables.
La ETITC establece, define y revisa unos objetivos dentro del Sistema de Gestión Integrado, garantizando la preservación de la confidencialidad, integridad y disponibilidad de los activos de información; la protección y prevención de accidentes y enfermedades laborales, promocionando la calidad de vida laboral; la protección del medio ambiente, la prevención de impactos ambientales, el uso sostenible de recursos y la satisfacción del cliente, incrementando los niveles de confianza en los servidores públicos, estudiantes, acudientes y otras partes interesadas.

El diseño, implementación y mantenimiento del Sistema de Gestión Integrado, se apoya en los resultados de un proceso continuo de identificación, análisis y valoración de riesgos, del que se derivan las actuaciones a desarrollar; guardando una estrecha relación con la declaración de aplicabilidad vigente para el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.

La Alta Dirección de la ETITC establece los criterios de aceptación del riesgo, de manera que todos aquellos escenarios, que impiden un nivel de riesgo aceptable, sean tratados adecuadamente y mantenidos bajo control; así mismo, desarrolla, implementa y mantiene actualizado un Plan de Contingencia, Recuperación y Retorno a la Normalidad, acorde a las necesidades de la ETITC y dimensionado a los riesgos que le afectan.

La Alta Dirección de la ETITC se compromete a la implementación, mantenimiento y mejora del Sistema de Gestión Integrado, dotándolos de aquellos medios y recursos que sean necesarios e instando a todos los Servidores Públicos, Proveedores y demás partes interesadas, para que asuman este compromiso. Para ello, la ETITC implementa las medidas requeridas para sensibilizar y concientizar a los Servidores Públicos, Proveedores y demás partes interesadas. A su vez, cuando exista una violación de las políticas del Sistema de Gestión Integrado, aprobadas por la Alta Dirección, la ETITC se reserva el derecho de aplicar las medidas disciplinarias, acorde a los compromisos laborales de los Servidores Públicos, Proveedores y demás partes interesadas, dentro del marco legal vigente aplicable y dimensionado al impacto que tengan sobre la ETITC.

La responsabilidad general del Sistema de Gestión Integrado en la ETITC recae sobre la Alta Dirección. Por otro lado, todos los Servidores Públicos, Proveedores y demás partes interesadas, tienen la obligación de reportar los incidentes de Seguridad de la Información, Seguridad y Salud en el Trabajo y Gestión Ambiental, haciendo uso de las directrices establecidas por la ETITC. Para el Sistema de Gestión de Calidad se debe hacer el reporte de las salidas no conformes que se presenten.

Todo lo definido en la Política del Sistema de Gestión Integrado se implementa, mediante las buenas prácticas establecidas en el habilitador transversal Seguridad de la Información de Gobierno Digital, el Modelo Integrado de Planeación y Gestión, los planes de sensibilización y

capacitación, las políticas y procedimientos específicos del Sistema de Gestión Integrado, compartiendo aquellos recursos en pro de la optimización y fomentando los procesos de revisiones por la Alta Dirección y auditorias integrales, para impulsar, de una manera satisfactoria, la mejora continua de la eficacia y eficiencia, en la gestión de los procesos misionales, estratégicos, de apoyo y evaluación, mediante las acciones correctivas que permitan eliminar la causa de las no conformidades identificadas.

La presente Política del Sistema de Gestión Integrado, es aplicada por todos los Servidores Públicos, Proveedores y demás partes interesadas que gestionan los procesos misionales, estratégicos, de apoyo y evaluación; debe ser socializada al interior de la ETITC y publicada en el sitio web Institucional.

6. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de la ETITC aprueba el Manual de Políticas de Seguridad de la Información, como muestra de su compromiso y apoyo al proceso de evaluación que se lleva a cabo en la Institución, mediante el SGSI y el MSPI de Gobierno Digital.

La Alta Dirección de la ETITC demuestran su compromiso de apoyo a través de:

1- La revisión y aprobación del Manual de Políticas de Seguridad de la Información para la Institución.

2- La promoción activa de una cultura de seguridad de la información en los Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a los sistemas de información, repositorios e instalaciones físicas de la ETITC.

3- Facilitar la divulgación de este manual a todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

4- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información, contenidas en el manual.

5- La verificación del cumplimiento de las políticas aquí mencionadas.

7. SANCIONES

Las Políticas de Seguridad de la Información contenidas en este manual, pretenden generar un compromiso, en todo el recurso humano de la Institución, que permita garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información institucional, lográndose de esta manera, altos estándares de cultura, en temas de ciberseguridad.

Por tal motivo, las violaciones de las Políticas de Seguridad de la Información serán objeto de análisis y sanción, aplicando de esta manera, medidas correctivas, mediante la Secretaría General, la cual implementará el **GCD-PC-01 Procedimiento Responsabilidad Disciplinaria**, tomando como base el Código General Disciplinario (Ley 1952 de 2019, Artículo 55, Numeral 1), para de esta manera, impartir las respectivas correcciones, ante la violación presentada.

8. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.

La política de Administración del Riesgo es aprobada por el Comité Institucional de Gestión y Desempeño y se encuentra versionada dentro de los documentos del proceso de Direccionamiento Institucional y se identifica como **DIE-DO-18 Política de Administración del Riesgo**.

Para esta las actividades correspondientes a la administración de riesgos en la ETITC se hará uso del procedimiento **GDC-PC-06 Administración del riesgo** en donde se definen los criterios y métodos para la identificación, análisis, evaluación mitigación y control de posibles eventos de riesgos que puedan afectar el cumplimiento de la misión, visión y objetivos institucionales.

9. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

9.1- Política de Estructura Organizacional de Seguridad de la Información.

Objetivo:

Garantizar la implementación de una estructura organizacional de seguridad de la información que define roles y responsabilidades alineada con la Política de Gobierno Digital conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Alcance:

La Política de Estructura Organizacional de Seguridad de la Información será aplicada por la Alta Dirección, Comité Institucional de Gestión y Desempeño, además por el Profesional de Seguridad de la Información.

Directrices:

La asignación de recurso humano para apoyar las actividades de gestión de la seguridad de la información constituye un elemento indispensable para lograr el cumplimiento de requisitos, metas y entregables, contemplados en el SGSI y el MSPI de Gobierno Digital.

La definición y aprobación de roles y responsabilidades dentro de la Institución, permite estructurar el modelo organizacional interno que, a su vez, gestionará el cumplimiento de las tareas aprobadas. Por otro lado, cada rol asumirá un grupo de responsabilidades que permiten identificar

las funciones de cada área, organización o personal comprometido con el rol.

La definición de roles y responsabilidades son propios de cada organismo o institución. Cada entidad posee necesidades diferentes, una estructura organizacional diferente, procesos diferentes y condiciones tecnológicas diferentes.

Por otro lado, el compromiso de la Alta Dirección, en apoyar las actividades de seguridad de la información programadas, es fundamental para que toda la estructura organizacional definida funcione efectivamente y alcance las expectativas trazadas. Para ello, se hace necesario la elaboración, revisión y aprobación de la carta de compromiso de la Alta Dirección.

Una de las actividades más significativas dentro de la estructura organizacional interna, para la gestión de la seguridad de la información, son las actividades dirigidas a crear una cultura de seguridad elevada en los Servidores Públicos, Proveedores y demás partes interesadas, que tienen acceso a los sistemas de información, repositorios y áreas físicas de la ETITC. Para lograr un eficiente resultado en esta tarea, se requiere del total apoyo de la Alta Dirección.

La estructura organizacional definida por roles y responsabilidades en la Institución permitirá gestionar con mayor rapidez y asertividad los incidentes de seguridad detectados. En estos casos se debe hacer uso del Procedimiento **GSI-PC-05 Gestión de Incidentes de la Seguridad de la Información**.

Por otro lado, para fortalecer la organización interna de seguridad de la información en la ETITC, se requiere la orientación del Comité Institucional de Gestión y Desempeño.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Alta Dirección:

- La Alta Dirección de la ETITC debe aprobar los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

- La Alta Dirección debe elaborar y aprobar la carta de compromiso donde manifieste su total apoyo a las actividades relacionadas con la seguridad de la información.

- La Alta Dirección debe definir y establecer el Procedimiento de Contacto con las Autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

- La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este manual.

- La Alta Dirección debe promover activamente una cultura de seguridad de la información en la Institución.

- La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la

Información a todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

- La Alta Dirección de la ETITC debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la Institución.

Comité Institucional de Gestión y Desempeño:

- El Comité Institucional de Gestión y Desempeño debe revisar, periódicamente, las Políticas de Seguridad de la Información contenidas en el manual, planes y procedimientos, según lo considere pertinente.

- El Comité Institucional de Gestión y Desempeño debe analizar los incidentes de seguridad que le son escalados y activar el Procedimiento de Contacto con las Autoridades, cuando lo estime necesario.

- El Comité Institucional de Gestión y Desempeño debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe liderar la generación de lineamientos para gestionar la seguridad de la información de la ETITC y el establecimiento de controles técnicos, físicos y administrativos, derivados del análisis de riesgos de seguridad realizado.

- El Profesional de Seguridad de la Información debe validar y monitorear, de manera periódica, la implementación de los controles de seguridad establecidos.

- El Profesional de Seguridad de la Información debe definir los roles y responsabilidades de la ETITC, así como socializarlos ante el Comité Institucional de Gestión y Desempeño de la ETITC, para su aprobación.

Oficina de Control Interno:

- La Oficina de Control Interno debe planear y ejecutar las auditorías internas al SGSI y al MSPI de la ETITC, a fin de determinar si las políticas, procedimientos y controles establecidos están conformes con los requerimientos institucionales, de seguridad y regulaciones aplicables.

- La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del SGSI y el MSPI, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

- La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

9.2- Política para Uso de Dispositivos Móviles.

Objetivo:

Proveer las condiciones para el manejo de los dispositivos móviles institucionales y personales (teléfonos inteligentes y tabletas, entre otros), que hagan uso de los servicios de la ETITC, garantizando con esto, que los Servidores Públicos, Proveedores y demás partes interesadas utilicen responsablemente los servicios y equipos proporcionados por la Institución.

Alcance:

La Política para Uso de Dispositivos Móviles será aplicada por el área de Informática y Comunicaciones, adicional todos los Servidores Públicos, Proveedores y demás partes interesadas que utilicen dispositivos móviles para tener acceso a los servicios ofrecidos por la ETITC.

Directrices:

Para el cumplimiento de la Política para Uso de Dispositivos Móviles se hace necesario que el área de Informática y Comunicaciones garantice el inventario de dispositivos móviles de la ETITC y adicional, identifique al usuario que se conecta a través de cada dispositivo.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe investigar y aprobar las opciones de protección de los dispositivos móviles institucionales y personales, que hagan uso de los servicios provistos por la Institución.

- El área de Informática y Comunicaciones debe establecer las configuraciones aceptables, para los dispositivos móviles institucionales o personales, que hagan uso de los servicios provistos por la ETITC.

- El área de Informática y Comunicaciones debe establecer un método de bloqueo para los dispositivos móviles institucionales, que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

- El área de Informática y Comunicaciones debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales, haciendo imposible la copia o extracción de datos, si no se conoce el método de desbloqueo.

- El área de Informática y Comunicaciones debe configurar la opción de borrado remoto de información, en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.
- El área de Informática y Comunicaciones debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de la ETITC; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.
- El área de Informática y Comunicaciones debe instalar un software de antivirus en los dispositivos móviles institucionales.
- El área de Informática y Comunicaciones debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales, antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Servidores Públicos, Proveedores y demás partes interesadas:

- Servidores Públicos, Proveedores y demás partes interesadas deben evitar usar los dispositivos móviles institucionales, en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Servidores Públicos, Proveedores y demás partes interesadas no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Servidores Públicos, Proveedores y demás partes interesadas deben evitar la instalación de programas, desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Servidores Públicos, Proveedores y demás partes interesadas deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.
- Servidores Públicos, Proveedores y demás partes interesadas deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.
- Servidores Públicos, Proveedores y demás partes interesadas deben evitar conectar los dispositivos móviles institucionales asignados, por puerto USB, a cualquier computador público, de hoteles o cafés internet, entre otros.
- Servidores Públicos, Proveedores y demás partes interesadas no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

9.3- Política para uso de Conexiones Remotas.

Objetivo:

Garantizar que los métodos de conexión remota, dentro de la LAN de la ETITC y desde fuera de ella, sean los idóneos, garantizando con esto los niveles óptimos de seguridad durante la ejecución de las actividades remotas.

Alcance:

La Política para Uso de Conexiones Remotas será aplicada por el área de Informática y Comunicaciones, oficina de Control Interno, Profesional de Seguridad de la Información y todos los Servidores Públicos, Proveedores y demás partes interesadas, que utilicen el servicio de conexiones remotas para darle cumplimiento a alguna de sus funciones.

Directrices:

Se deben revisar los métodos de conexión remota existentes, con el objetivo de definir cuál de ellos son los más convenientes a utilizar en la LAN de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información de la ETITC, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Institución.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe implantar los métodos y controles de seguridad para establecer conexiones remotas, hacia la plataforma tecnológica de la ETITC.

- El área de Informática y Comunicaciones debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

- El área de Informática y Comunicaciones debe verificar la efectividad de los controles aplicados sobre las conexiones remotas, a los recursos de la plataforma tecnológica de la ETITC, de manera permanente.

Oficina de Control Interno:

- La Oficina de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados, para las conexiones remotas, a la plataforma tecnológica de la ETITC.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas que realicen conexiones remotas, hacia la LAN de la ETITC, deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica y deben acatar las condiciones de uso establecidas para dichas conexiones remotas.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas que realicen conexiones remotas, hacia la LAN de la ETITC, deben establecer dichas conexiones en computadores previamente identificados y, bajo ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

10. POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS.

10.1- Política Antes de Asumir el Empleo.

Objetivo:

Garantizar que los Acuerdos y/o Cláusulas de Confidencialidad y Aceptación de Políticas de Seguridad de la Información, sean incluidos en los contratos o cualquier otra forma de vinculación laboral, de Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas y sistemas de información de la ETITC.

Alcance:

La Política Antes de Asumir el Empleo será aplicada por las áreas de Talento Humano, Contratación, adicional, los Supervisores de Contratos o Líderes de Áreas y todos los Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas y sistemas de información de la ETITC.

Directrices:

Es importante tener en cuenta que el área de Contratación de la ETITC trabaja formatos de contratación variados. La estructura de dichos formatos depende, en su medida, del contenido del documento Estudios Previos, que elaboran los supervisores de contrato o líderes de áreas. Por tal motivo los Acuerdos y/o Cláusulas de Confidencialidad y Aceptación de Políticas de Seguridad de la Información deben ser incluidos en el documento de Estudios Previos.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Talento Humano:

- El área de Talento Humano debe realizar las verificaciones necesarias, para confirmar la veracidad de la información suministrada por el candidato, aspirante a una posición laboral en la ETITC, antes de su vinculación definitiva.

Supervisores de Contratos o Líderes de Áreas:

- Cada Supervisor de Contrato o Líder de Área debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de Aceptación de Políticas de Seguridad de la Información, en los contratos o vinculaciones laborales del personal que trabaja para la ETITC, antes de otorgar acceso a los sistemas de información de la ETITC.

Área de Contratación:

- El área de Contratación de la ETITC debe incluir los Acuerdos y/o Cláusulas de Confidencialidad y de Aceptación de Políticas de Seguridad de la Información, en los contratos o vinculaciones laborales de los servidores públicos o partes interesadas.

Servidores Públicos, Proveedores y demás partes interesadas:

- Los Servidores Públicos, Proveedores y demás partes interesadas deben firmar el Acuerdo y/o Cláusula de Confidencialidad y de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las Instalaciones y a los sistemas de información de la ETITC.

- Los Servidores Públicos, Proveedores y demás partes interesadas deben cumplir con el Acuerdo y/o Cláusula de Confidencialidad y de Aceptación de Políticas de Seguridad de la Información, incluidas en el contrato o forma de vinculación laboral con la ETITC.

10.2- Política Durante la Ejecución del Empleo.

Objetivo:

Garantizar que todos los Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas y sistemas de información de la ETITC, reciban charlas o capacitaciones en temas de seguridad de la información, así como aplicar un proceso disciplinario que permita brindarle un tratamiento a las violaciones de las políticas de seguridad de la información, acuerdos/cláusulas de confidencialidad y de aceptación de las políticas de seguridad de la información, así como cualquier otro tipo de violación, que ponga en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información.

Alcance:

La Política Durante la Ejecución del Empleo será aplicada por la Alta Dirección, Control Interno Disciplinario, así como, el Profesional de Seguridad de la Información y todos los Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas y sistemas de seguridad de la información de la ETITC.

Directrices:

Es importante la definición y puesta en marcha de un proceso disciplinario, que permita brindarle un tratamiento a las violaciones de las políticas de seguridad de la información, los acuerdos o cláusulas de confidencialidad, acuerdos o cláusulas de aceptación de políticas de seguridad de la información o cualquier otro tipo de incidente de seguridad, que ponga en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información de la ETITC.

Es importante la elaboración y puesta en marcha de un programa de capacitación en temas de seguridad de la información.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Alta Dirección:

- La Alta Dirección debe demostrar su compromiso con la seguridad de la información, por medio de la aprobación del Manual de Políticas de Seguridad de la Información, normas y demás lineamientos que desee establecer la Institución.

- La Alta Dirección debe promover la importancia de la seguridad de la información entre los Servidores Públicos, Proveedores y demás partes interesadas que acceden a las instalaciones físicas y sistemas de información de la ETITC, así como motivar el entendimiento, toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares establecidos para la seguridad de la información.

- La Alta Dirección debe definir y establecer el proceso disciplinario, para el tratamiento de las violaciones a las políticas de seguridad de la información, acuerdos o cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información, o cualquier otro tipo de incidente de seguridad que ponga en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe diseñar y ejecutar de manera permanente, un plan de sensibilización en seguridad de la información, con el objetivo de apoyar la protección adecuada de los sistemas de información y áreas físicas de la ETITC.

- El Profesional de Seguridad de la Información debe capacitar y entrenar a los Servidores

Públicos, Proveedores y demás partes interesadas que trabajan para la ETITC, en el plan de sensibilización en seguridad de la información, para evitar posibles riesgos de seguridad de esta.

- El Profesional de Seguridad de la Información debe controlar la asistencia a las charlas y/o eventos de seguridad de la información que se programen, para todos los Servidores Públicos, Proveedores y demás partes interesadas que trabajan para la ETITC.

Control Interno Disciplinario:

- La oficina de Control Interno Disciplinario debe aplicar el proceso disciplinario, definido y aprobado por la Alta Dirección, cuando se identifiquen incumplimientos de las políticas de seguridad de la información, acuerdos de confidencialidad y aceptación de las políticas de seguridad de la información, así como cualquier otra violación de seguridad que ponga en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información de la ETITC.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben dar cumplimiento a las políticas de seguridad de la información, normas, procedimientos, acuerdos/cláusulas de confidencialidad, acuerdos/cláusulas de aceptación de las políticas de seguridad de la información, así como asistir a las charlas y/o capacitaciones que sean referentes a la seguridad de la información.

10.3- Política de Terminación y Cambio de Empleo.

Objetivo:

Garantizar que para todos los servidores públicos que se desvinculen, tomen licencia o vacaciones, de la ETITC, sea inhabilitado su acceso en el sistema de control de acceso de la ETITC, además, todo servidor público que cambie de posición laboral obtenga los privilegios adecuados de acceso a los sistemas de información de la ETITC.

Alcance:

La Política de Terminación y Cambio de Empleo será aplicada por el área de Talento Humano, Informática y Comunicaciones, Audiovisuales y adicional por los Supervisores de Contratos o Líderes de Áreas, servidores públicos que tengan acceso a las instalaciones físicas y sistemas de información de la ETITC.

Directrices:

Es importante tener en cuenta que el sistema de control de acceso de la ETITC, es el encargado de otorgar, de manera electrónica, a un servidor públicos, estudiante, proveedor y parte interesada, acceso a las instalaciones físicas de la ETITC.

Adicional, en caso de que el servidor público, efectúe un cambio de posición laboral, dentro de la ETITC, se debe revisar el manual de funciones para el nuevo cargo y modificar o mantener los privilegios de acceso a los sistemas de información de la ETITC, del servidor público en mención.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Supervisores de Contratos o Líderes de Áreas:

- Cada Supervisor de Contrato o Líder de Área debe monitorear y reportar, de manera inmediata, la desvinculación, licencia, vacaciones o cambio de posición laboral, de los servidores públicos al área de Talento Humano.

Talento Humano:

- El área de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de posición laboral de los servidores públicos que trabajen para la Institución, generando el respectivo Paz y Salvo.

Informática y Comunicaciones:

- Cuando recibe el Paz y Salvo debe firmarlo y comenzar con los respectivos procedimientos de cancelación de cuenta de usuario, en todos los entornos informáticos a su cargo (correo electrónico, controlador de dominio, control de acceso)

- El área de Informática y Comunicaciones, cuando el servidor público, es desvinculado o toma licencia o vacaciones, debe inhabilitar el acceso del servidor público, en el sistema de control de accesos de la ETITC.

- El área de Informática y Comunicaciones, cuando el servidor público, cambia de posición laboral, dentro de la ETITC, debe revisar las nuevas funciones del cargo y en base a ellas, modificar o mantener los permisos y privilegios de acceso a los sistemas de información de la ETITC.

Servidor Público:

- Debe entregar el Paz y Salvo al líder del área de Informática y Comunicaciones.

- Toda vez que el área de Informática y Comunicaciones firme el Paz y Salvo y comience a ejecutar las actividades de cancelación de acceso a los sistemas de información y control de entrada a las instalaciones físicas de la ETITC, el servidor público debe evitar su ingreso a las instalaciones físicas y/o acceso a los sistemas de información de la ETITC, mediante otra identidad no autorizada para su uso.

11. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN.

11.1- Política de Responsabilidad por los Activos.

Objetivo:

Garantizar que todos los activos de información de la ETITC, posean un propietario y/o custodio, que garanticen la preservación de la confidencialidad, integridad y disponibilidad de la información, en cada una de las áreas de la ETITC.

Alcance:

La Política de Responsabilidad por los Activos será aplicada por el área de Informática y Comunicaciones, Alta Dirección, además, los Propietarios de los Activos, Custodio de los Activos, Profesional de Seguridad de la Información y Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas y sistemas de información de la ETITC.

Directrices:

Los Propietarios de los Activos serán todos los líderes de los procesos, definidos y aprobados por la Alta Dirección de la ETITC.

Los Custodios de los Activos serán los líderes de áreas.

Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos, son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Propietarios de los Activos:

- Los Propietarios de los Activos deben monitorear periódicamente la validez de los usuarios

y sus perfiles de acceso a la información.

- Los Propietarios de los Activos deben determinar los criterios y niveles de acceso a la información.

- Los Propietarios de los Activos deben ser conscientes que los recursos de procesamiento de información de la ETITC, se encuentran sujetos a auditorías, por parte de la Oficina de Control Interno y a revisiones de cumplimiento, por parte del Profesional de Seguridad de la Información de la ETITC.

- Los Propietarios de los Activos deben autorizar a sus Servidores Públicos, Proveedores y demás partes interesadas, el uso de los recursos tecnológicos, previamente preparados por el área de Informática y Comunicaciones.

- Los Propietarios de los Activos deben recibir los recursos tecnológicos asignados a sus Servidores Públicos, Proveedores y demás partes interesadas, cuando estos se retiran de la ETITC o son trasladados de a otra área.

Custodio de los Activos:

- Los Custodios de los Activos deben verificar que los niveles de acceso a la información, definidos y aprobados por el propietario, se cumplan.

- Los Custodios de los Activos deben verificar que los accesos a archivos físicos, magnéticos u ópticos de información sean los adecuados y aprobados por el propietario de la información.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe establecer una configuración de acceso a la información adecuada, para cada uno de los Servidores Públicos, Proveedores y demás partes interesadas, que requieran ingresar los sistemas de información y recursos informáticos de la ETITC.

- El área de Informática y Comunicaciones, deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la ETITC.

- El área de Informática y Comunicaciones debe preparar las estaciones de trabajo fijas y/o portátiles de los servidores públicos y hacer entrega de estas a su propietario o custodio.

- El área de Informática y Comunicaciones debe recibir los equipos de trabajo, fijo y/o portátil, para su reasignación o disposición final, y generar copias de seguridad de la información de los servidores públicos que se retiran o cambian de labores, cuando les es formalmente solicitado.

Profesional de Seguridad de la Información / Propietarios de los Activos / Custodios de los Activos:

- El Profesional de Seguridad de la Información, de conjunto con los Propietarios de los Activos y Custodios de los Activos deben garantizar la identificación de los activos de información de la ETITC, generando con esto, el inventario correspondiente.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe evaluar las brechas de seguridad de los activos de información identificados a través de GSI-FO-03 Matriz de inventario general de activos de la ETITC.

- El Profesional de Seguridad de la Información debe definir las condiciones de uso y protección de los activos de información, tanto físicos, como digital.

- El Profesional de Seguridad de la Información debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la ETITC.

Servidores Públicos, Proveedores y demás partes interesadas:

- Los Servidores Públicos, Proveedores y demás partes interesadas deben utilizar de forma ética y en cumplimiento de las leyes y reglamentos vigentes, los recursos tecnológicos de la ETITC, con el fin de evitar daños o pérdidas sobre las operaciones o la imagen de la ETITC.

- Los Servidores Públicos, Proveedores y demás partes interesadas deben utilizar los recursos tecnológicos de la ETITC, con el fin de llevar a cabo las labores de la ETITC; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

- Los Servidores Públicos, Proveedores y demás partes interesadas no deben utilizar sus equipos de cómputo y dispositivos móviles personales, para desempeñar las actividades laborales.

- Los Servidores Públicos, Proveedores y demás partes interesadas no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la ETITC.

- En el momento de desvinculación, licencia, vacaciones o cambio de labores, los Servidores Públicos, Proveedores y demás partes interesadas, deben realizar la entrega de su puesto de trabajo al Propietario de los Activos o Custodio de los Activos; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación laboral.

11.2- Política de Clasificación y Etiquetado de la Información

Objetivo:

Garantizar que la información reciba una clasificación y etiquetado adecuada, para con esto, proporcionar un nivel de protección óptimo a la misma.

Alcance

La Política de Clasificación y Etiquetado de la Información será aplicada por el área de Informática y Comunicaciones, Alta Dirección y, además, por el Profesional de Seguridad de la Información, Propietarios de la Información, Custodios de la Información y Servidores Públicos, Proveedores y demás partes interesadas que tengan acceso a las instalaciones físicas y sistemas de información de la ETITC.

Directrices

Para la clasificación y etiquetado de la información de la ETITC, se debe tener en cuenta el **Procedimiento de Clasificación y Etiquetado de la Información**, revisado y aprobado por la Alta Dirección.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información de la ETITC debe definir los niveles de clasificación y etiquetado de la información y posteriormente, elaborar el Procedimiento de Clasificación y Etiquetado de la Información.

- El Profesional de Seguridad de la Información de la ETITC debe socializar y divulgar la Política de Clasificación y Etiquetado de la Información y el Procedimiento de Clasificación y Etiquetado de la Información, a los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

- El Profesional de Seguridad de la Información de la ETITC debe acompañar a los propietarios y custodios de la información, durante la actividad de clasificación y etiquetado de la misma.

Alta Dirección:

- La Alta Dirección debe revisar y aprobar la Política de Clasificación y Etiquetado de la Información y el Procedimiento de Clasificación y Etiquetado de la Información, para la ETITC.
-

Propietario de la Información:

- Los Propietarios de la Información deben clasificar la misma, de acuerdo con el Procedimiento de Clasificación y Etiquetado de la Información, establecido en la ETITC.

- Los Propietarios de la Información son responsables de monitorear periódicamente la clasificación y etiquetado de la misma y de ser necesario, realizar su reclasificación y re-etiquetado.

Custodios de la Información:

- Los Custodios de la Información deben colaborar en la actividad de clasificación y etiquetado de la información, liderada por los propietarios de la misma, haciendo uso del Procedimiento de Clasificación y Etiquetado de la Información.

- Los Custodios de la Información deben velar que los Servidores Públicos, Proveedores y demás partes interesadas, respeten los niveles de clasificación y etiquetado asignados a la documentación de la ETITC.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben respetar los niveles de clasificación y etiquetado de la información, definidos por el propietario y custodio de esta.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben asegurarse de que no queden documentos físicos en impresoras, escáneres, fotocopiadoras y máquinas de fax, para evitar su divulgación no autorizada.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben asegurarse de que, en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, los mismos deben contar con las protecciones de seguridad adecuada, de acuerdo con su nivel de clasificación y etiquetado.

11.3- Política de Manejo de Medios.

Objetivo:

Garantizar que todos los Servidores Públicos, Proveedores y demás partes interesadas, que requieran usar periféricos o medio de almacenamiento, para el cumplimiento de sus funciones, lo hagan cumpliendo con los lineamientos de seguridad de la ETITC.

Alcance

La Política de Manejo de Medios será aplicada por el área de Informática y Comunicaciones, Profesional de Seguridad de la Información y adicional, todos los Servidores Públicos, Proveedores y demás partes interesadas que requieran usar un periférico o medio de almacenamiento, para darle cumplimiento a sus funciones.

Directrices

Se hace necesario regular el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la ETITC, para minimizar la posibilidad que un usuario avanzado utilice alguna herramienta, que permita iniciar el PC mediante un segundo sistema operativo. Además, muchas veces los usuarios guardan programas de monitoreo de redes, hackeo, etc., que utilizan para detectar vulnerabilidades y obtener algún beneficio de ellas.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información de la ETITC, deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la ETITC.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe implementar los controles, que regulen el uso de periféricos y medios de almacenamiento, en la plataforma tecnológica de la ETITC, de acuerdo con los lineamientos y condiciones establecidas.

- El área de Informática y Comunicaciones debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la ETITC, ya sea cuando son dados de baja o reasignados a un nuevo servidor público, proveedor y parte interesada.

- El área de Informática y Comunicaciones debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la ETITC, de acuerdo con el perfil del cargo del servidor público, proveedor y parte interesada.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben acogerse a las condiciones de uso de los periféricos y medios de almacenamiento, establecidos por el área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información de la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben modificar la configuración de periféricos y medios de almacenamiento, establecida por el área de Informática y Comunicaciones.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas son responsables por la custodia de los medios de almacenamientos institucionales asignados.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben utilizar medios de almacenamientos personales, en la plataforma tecnológica de la ETITC.

12. POLÍTICA DE CONTROL DE ACCESO.

12.1- Política de Acceso a Redes y Recursos de Red.

Objetivo:

Garantizar que todo servidor público, proveedor y parte interesada, que tenga necesidad de acceder las redes instituciones o recursos de red de la ETITC, realicen la actividad siguiendo una serie de lineamientos de seguridad, que contribuyen a preservar la confidencialidad, integridad y disponibilidad de la información de la ETITC.

Alcance

La Política de Acceso a Redes y Recursos de Red será aplicada por el área de Informática y Comunicaciones, Talento Humano, Contratación, Registro y Control, adicional por el Profesional de Seguridad de la Información, Supervisores de Contrato o Líderes de Área y Servidores Públicos, Proveedores y demás partes interesadas, que necesiten acceder a las redes institucionales y recursos informáticos de la ETITC.

Directrices

Todos los equipos de usuario final, que se conecten o deseen conectarse, a las redes de datos de la ETITC, deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Es importante contar con un Procedimiento de Autorización de Acceso a la Red Institucional, revisado y aprobado por la Alta Dirección de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información, deben establecer un Procedimiento de Autorización de Acceso a la Red Institucional, para proteger el acceso a las redes de datos y los recursos informáticos de la ETITC.

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información, deben velar por el cumplimiento del Procedimiento de Autorización de Acceso a la Red Institucional.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe asegurar que las redes inalámbricas de la ETITC, cuenten con métodos de autenticación, que evite accesos no autorizados.

- El área de Informática y Comunicaciones debe establecer controles, para la identificación y autenticación de los usuarios, provistos por proveedores y partes interesadas, en las redes o recursos de red de la ETITC, así como velar por la aceptación de las responsabilidades de dichos proveedores y terceros.

- El área de Informática y Comunicaciones debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe verificar periódicamente los controles de acceso, para los usuarios provistos por proveedores y partes interesadas, con el fin de revisar que dichos usuarios tengan acceso permitido, únicamente, a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas, antes de tener acceso, por primera vez, a la red de datos de la ETITC, deben seguir las indicaciones del área de Informática y Comunicaciones.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben conocer y cumplir el Procedimiento de Autorización de Acceso a la Red Institucional.

Supervisor de Contrato o Líder de Área:

- El Supervisor de Contrato o Líder de Área debe conocer y cumplir con el Procedimiento de Autorización de Acceso a la Red Institucional.

Talento Humano:

- El área de Talento Humano debe conocer y cumplir con el Procedimiento de Autorización de Acceso a la Red Institucional.

Registro y Control:

- El área de Registro y Control debe conocer y cumplir con el Procedimiento de Autorización de Acceso a la Red Institucional.

Contratación:

- El área de Contratación debe conocer y cumplir con el Procedimiento de Autorización de Acceso a la Red Institucional.

12.2- Política de Administración de Acceso de Usuarios.

Objetivo:

Garantizar que las áreas respectivas efectúen una administración óptima y adecuada, de los usurarios autenticados, en los diferentes recursos informáticos y sistemas de información de la ETITC.

Alcance

La Política de Administración de Acceso de Usuarios será aplicada por el área de Informática y Comunicaciones, adicional por el Profesional de Seguridad de la Información, Propietarios de la Información y Custodios de la Información.

Directrices

Para el cumplimiento de la Política de Administración de Acceso de Usuarios, se debe tener en cuenta el Procedimiento de Autorización de Acceso a la Red Institucional, revisado y aprobado por la Alta Dirección.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe garantizar la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la ETITC, contemplando la creación, modificación, bloqueo o eliminación de las cuentas de usuarios.

- El área de Informática y Comunicaciones debe conocer y cumplir con el Procedimiento de Autorización de Acceso a la Red Institucional, revisado y aprobado por la Alta Dirección de la ETITC.

- El área de Informática y Comunicaciones debe asegurarse que los usuarios o perfiles de usuario, que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

- El área de Informática y Comunicaciones debe autorizar la creación, modificación o cancelación de las cuentas de acceso de los usuarios, toda vez que Talento Humano, Registro y Control notifiquen al área sobre alguna novedad al respecto.

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información, deben definir lineamientos, para la configuración de contraseñas de acceso a la plataforma tecnológica y/o sistemas de información de la ETITC (cuentas de usuarios en el controlador de dominio, correo electrónico y sistemas de información). Dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico,

control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso.

Propietarios de la Información / Custodios de la Información:

- Los Propietarios de la Información, de conjunto con los Custodios de la Información, deben definir los perfiles de sus usuarios y en base a eso, solicitarle al área de Informática y Comunicaciones el acceso a sus recursos tecnológicos y/o sistemas de información.

- Los Propietarios de la Información, de conjunto con los Custodios de la Información, deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

12.3- Política de Responsabilidades de Acceso de los Usuarios.

Objetivo:

Garantizar que todos los Servidores Públicos, Proveedores y demás partes interesadas, que requieran ingresar a las instalaciones físicas, plataforma tecnológica y sistemas de información de la ETITC, se responsabilicen por hacer un uso adecuado y correcto de los usuarios y contraseñas definidos en la red institucional, para el desarrollo de sus funciones.

Alcance

La Política de Responsabilidades de Acceso de los Usuarios será aplicada por todos los Servidores Públicos, Proveedores y demás partes interesadas que requieran ingresar a las instalaciones físicas, plataforma tecnológica y sistemas de información de la ETITC.

Directrices

Es importante realizar una labor de concienciación en todo el personal de la ETITC, para de esta forma fortalecer una conciencia de seguridad de la información, que preserve la confidencialidad de usuarios y contraseñas configurados en la plataforma tecnológica y sistemas de información de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben hacerse responsables de las acciones realizadas sobre la plataforma tecnológica y sistemas de información de la ETITC, así como del usuario y contraseña asignados para el acceso a los recursos informáticos y de información de la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben compartir sus cuentas de usuarios y contraseñas con terceras personas. Las cuentas de usuarios y contraseñas son intransferibles y solo pueden ser usadas por la persona autorizada y para fines institucionales.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben acogerse a los lineamientos, establecidos por el área de Informática y Comunicaciones, para la configuración de contraseñas de acceso a la plataforma tecnológica y sistemas de información de la ETITC.

12.4- Política de Uso de Altos Privilegios y Utilitarios de Administración.

Objetivo:

Garantizar que todo privilegio administrativo, otorgado a los perfiles de administración de los recursos informáticos y sistemas de información de la ETITC, obtengan los niveles de acceso adecuados para cumplir con la actividad de administración, siempre en función de los intereses institucionales.

Alcance

La Política de Uso de Altos Privilegios y Utilitarios de Administración será aplicada por el área de Informática y Comunicaciones y Profesional de Seguridad de la Información de la ETITC.

Directrices

El análisis de privilegios administrativos para los perfiles que así lo requieran, deben ser tenidos en cuenta de manera cuidadosa, para evitar pasar por alto el hecho de que un usuario administrativo deje de poseer algún privilegio requerido o posea privilegios por encima de los necesitados para desempeñar la labor de administración de un recurso informático y/o sistema de información.

Se debe revisar todos los utilitarios que sirven para otorgar privilegios de accesos, adicionales a los asignados, y elaborar una lista con los mismos, para mantener un control de su posible existencia en la plataforma tecnológica de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe otorgar los privilegios para la administración de los recursos tecnológicos, servicios de red y sistemas de información, sólo a aquellos Servidores Públicos, Proveedores y demás partes interesadas designados para dichas funciones.

- El área de Informática y Comunicaciones debe establecer cuentas personalizadas, con altos privilegios, para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información de la ETITC.

- El área de Informática y Comunicaciones debe restringir las conexiones remotas a los recursos informáticos; servicios de red y sistemas de información de la ETITC. Únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

- El área de Informática y Comunicaciones debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos y las bases de datos sean suspendidos o modificados y que las contraseñas, que traen por defecto dichos usuarios o perfiles, sean modificadas.

- El área de Informática y Comunicaciones debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información, no tengan instalados en sus equipos de cómputo utilitarios, que permitan accesos privilegiados a dichos recursos, servicios o sistemas de la ETITC.

- El área de Informática y Comunicaciones no debe hacer uso de los utilitarios que permiten acceso privilegiado a los sistemas informáticos y/o sistemas de información de la ETITC.

- El área de Informática y Comunicaciones debe deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos y/o sistemas de información. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

- El área de Informática y Comunicaciones debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos informático y sistemas de información de la ETITC.

- El área de Informática y Comunicaciones debe validar que los lineamientos para contraseñas, establecidos para la plataforma tecnológica de la ETITC, se aplican a los usuarios administrativos en su totalidad.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe revisar, periódicamente, la actividad de los usuarios administrativos de la plataforma tecnológica y los sistemas de información de la ETITC.

12.5- Política de Control de Acceso a Sistemas y Aplicaciones.

Objetivo:

Garantizar que los accesos autorizados a los sistemas de información de la ETITC, se realicen cumpliendo con lineamientos de seguridad, que permiten garantizar la preservación de la confidencialidad, integridad y disponibilidad de la información de la ETITC.

Alcance

La Política de Control de Acceso a Sistemas y Aplicaciones será aplicada por el área de Informática y Comunicaciones, además por los Propietarios de Activos de Información, Custodios de Activos de Información, Profesional de Seguridad de la Información y Desarrolladores Internos o Externos.

Directrices

Para el cumplimiento de la Política de Control de Acceso a Sistemas y Aplicaciones, es necesario la elaboración y aprobación de un Procedimiento para la Asignación de Accesos a los Sistemas de Información de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Propietarios de Activos de Información / Custodios de Activos de Información:

- Los Propietarios de Activos de Información y Custodios de Activos de Información deben autorizar los accesos a sistemas de información del área, de acuerdo con los perfiles establecidos y las necesidades de uso.

- Los Propietarios de Activos de Información y Custodios de Activos de Información deben monitorear, periódicamente, los perfiles definidos en los sistemas de información de la ETITC.

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información, deben establecer un Procedimiento para la Asignación de Accesos a los Sistemas de Información de la ETITC.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe establecer ambientes de desarrollo, pruebas y producción totalmente separados, para evitar que las actividades de desarrollo y pruebas pongan en riesgo la integridad de la información del ambiente de producción.

- El área de Informática y Comunicaciones debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

- El área de Informática y Comunicaciones debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

- El área de Informática y Comunicaciones debe proporcionar repositorios de archivos fuentes, de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios.

Desarrolladores Internos o Externos:

- Los Desarrolladores Internos o Externos deben asegurar que los sistemas de información construidos requieran autenticación para todos los usuarios y además que exista un nivel de privilegios de acceso a los recursos del aplicativo.

- Los Desarrolladores Internos o Externos deben garantizar la confiabilidad de los controles de autenticación.

- Los Desarrolladores Internos o Externos deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

- Los Desarrolladores Internos o Externos deben establecer los controles de autenticación, de tal manera, que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

- Los Desarrolladores Internos o Externos deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

- Los Desarrolladores Internos o Externos deben garantizar que se inhabiliten las cuentas de usuarios, luego de un número establecido de intentos fallidos de ingreso a los sistemas de información desarrollados para la ETITC.

- Los Desarrolladores Internos o Externos deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales, a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar al cambio de las contraseñas temporales después de su utilización.

- Los Desarrolladores Internos o Externos deben asegurar la re-autenticación de los usuarios, antes de la realización de operaciones críticas en los sistemas de información de la ETITC.

13. POLÍTICAS DE CRIPTOGRAFÍA.

13.1- Política de Controles Criptográficos.

Objetivo:

Garantizar que todos los sistemas de información de la ETITC, posean un certificado digital, permitiendo, de esta manera, que toda la información que viaja de origen a destino, lo haga de manera cifrada, preservando, a su vez, la confidencialidad e integridad de la información.

Alcance

La Política de Controles Criptográficos será aplicada por el área de Informática y Comunicaciones.

Directrices

Para el cumplimiento de la Política de Controles Criptográficos, es necesario garantiza que todos los sistemas de información de la ETITC, sean visitados mediante nombre de dominio y no mediante la IP.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe garantizar que todos los sistemas de información de la ETITC, sean visitados mediante un nombre de dominio y no por la IP.

- El área de Informática y Comunicaciones debe gestionar la adquisición de certificados digitales para los sistemas de información de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe validar de manera periódica, el cumplimiento los certificados digitales y llaves criptográficas a través del siguiente manual GSI-MA-03 Manual Operativo del SGSI (documento interno privado).

14. POLÍTICAS DE SEGURIDAD FISICA Y DEL ENTORNO.

14.1- Política de Áreas Seguras.

Objetivo:

Garantizar que todo Servidores Públicos, Proveedores y demás partes interesadas, que necesite utilizar las instalaciones físicas de la ETITC, realice su ingreso y salida cumpliendo con los lineamientos de seguridad física adecuados y aprobados por la Alta Dirección de la Institución.

Alcance

La Política de Áreas Seguras será aplicada por el área de Informática y Comunicaciones, Alta Dirección, Infraestructura Física, además por todos los Servidores Públicos, Proveedores y demás partes interesadas que necesiten hacer uso de las instalaciones físicas de la ETITC.

Directrices

Para el cumplimiento de la Política de Áreas Seguras se hace necesaria la puesta en marcha de un sistema de control de acceso, que permita registrar el ingreso y salida de todos Servidores Públicos, Proveedores y demás partes interesadas que hagan uso de las instalaciones físicas de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe autorizar las solicitudes de acceso al Data Center, Centros de Cableado y/o Cuarto de Servidores, adicional, los visitantes, proveedores y/o terceros, siempre deberán estar acompañados de un servidor público del área, durante su visita a dichas instalaciones.
- El área de Informática y Comunicaciones debe registrar el ingreso de los visitantes, proveedores y/o terceros al Data Center, Centros de Cableado y/o Cuarto de Servidores, que están bajo su custodia.

- El área de Informática y Comunicaciones debe deshabilitar o modificar de manera inmediata, los privilegios de acceso físico al Data Center, Centros de Cableado y/o Cuarto de Servidores, que están bajo su custodia, en los eventos de desvinculación, licencia, vacaciones o cambio en las labores de un servidor público autorizado a ingresar.

- El área de Informática y Comunicaciones debe proveer las condiciones físicas y medioambientales necesarias, para certificar la protección y correcta operación de los recursos de la plataforma tecnológica, ubicados en el Data Center, Centros de Cableado y/o Cuarto de Servidores; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

- El área de Informática y Comunicaciones debe velar porque los recursos de la plataforma tecnológica de la ETITC, ubicados en el Data Center, Centros de Cableado y/o Cuarto de Servidores, se encuentran protegidos contra fallas o interrupciones eléctricas.

- El área de Informática y Comunicaciones debe garantizar que el Data Center, Centros de Cableado y/o Cuarto de Servidores, que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.

- El área de Informática y Comunicaciones debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente, autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

- El área de Informática y Comunicaciones debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones físicas de la ETITC.

- El área de Informática y Comunicaciones debe verificar la efectividad de los mecanismos de seguridad física y control de acceso al Data Center, Centros de Cableado, Cuarto de Servidores, y demás áreas de procesamiento de información de la ETITC.

- El área de Informática y Comunicaciones debe controlar el ingreso de los visitantes, proveedores y/o terceros al Data Center, Centros de Cableado, Cuarto de Servidores, que están bajo su custodia.

-

Alta Dirección:

- La Alta Dirección debe controlar el acceso físico, del personal que labora en las áreas, a la ETITC. Dicho control puede ejecutarlo mediante el monitoreo del aplicativo de control de acceso y las cámaras de seguridad.

- La Alta Dirección debe velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas, solo sean utilizados por los servidores públicos autorizados y, salvo situaciones de emergencia u otro tipo de eventos, que por su naturaleza lo requieran, estos no sean transferidos a otros servidores públicos de la ETITC.

Infraestructura Física:

- El área de Infraestructura debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles de seguridad física, implementados en las instalaciones de la ETITC.

- El área de Infraestructura Física debe proponer mejoras a los mecanismos de seguridad física implementados y, de ser necesario, debe implementar nuevas estrategias que permitan mejorarlos, con el fin de perfeccionar la actividad de seguridad física de las instalaciones de la ETITC.

- El área de Infraestructura Física debe cerciorarse de que el Data Center, Centros de Cableado y/o Cuarto de Servidores, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- El área de Infraestructura debe asegurar que todo el cableado eléctrico y de datos, que está instalado en las áreas físicas de la ETITC, se encuentren en las respectivas canaletas y/o bandejas porta cables.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos y demás partes interesadas, deben hacer uso del sistema de control de acceso, para ingresar y salir de las instalaciones físicas haciendo uso de su carné digital que lo acredita como miembro de la ETITC.

- En el caso de Proveedores y demás partes interesadas, deben portar el stiker generado desde la recepción que los identifica como visitantes. El mismo debe estar en un lugar visible, mientras se encuentren en las instalaciones físicas de la Institución.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas, que ingresen a las instalaciones físicas de la ETITC, no deben intentar ingresar a áreas a las cuales no tengan autorización.

14.2- Política de Seguridad para los Equipos Institucionales.

Objetivo:

Garantizar que los recursos tecnológicos de la ETITC reciban una protección óptima, durante las operaciones internas que realizan en la red institucional, permitiendo con esto la preservación de la confidencialidad, integridad y disponibilidad de la información que soporta.

Alcance

La Política de Seguridad para los Equipos Institucionales será aplicada por el área de Informática y Comunicaciones, Control Interno, además por el Personal de Seguridad Perimetral, Profesional de Seguridad de la Información, Servidores Públicos, Proveedores y demás partes interesadas.

Directrices

Para el cumplimiento de la Política de Seguridad para los Equipos Institucionales, es necesario que el inventario de activos tipo hardware se encuentre elaborado, actualizado y aprobado por la Alta Dirección de la ETITC. Adicional, en dicha matriz de inventario debe figurar el propietario de cada activo y su ubicación.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe proveer los mecanismos y estrategias necesarios, para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la ETITC.

- El área de Informática y Comunicaciones debe realizar mantenimientos preventivos y correctivos, a los recursos tecnológicos de la ETITC.

- El área de Informática y Comunicaciones debe garantizar la configuración segura, para los equipos de cómputo de los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

- El área de Informática y Comunicaciones debe establecer las condiciones, que tienen que cumplir los equipos de cómputo del personal provisto por terceros, que requieran conectarse a la red de datos de la Institución y verificar el cumplimiento de dichas

condiciones antes de conceder a estos equipos acceso a los servicios de red institucionales.

- El área de Informática y Comunicaciones debe aislar los equipos servidores, cualquiera que sea el servicio que brinde sobre la red institucional, garantizando un espacio único para ellos, manteniéndolos fuera del alcance del personal no autorizado a manipularlos.

- El área de Informática y Comunicaciones debe generar y aplicar, lineamientos para la disposición segura de los equipos de cómputo de los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC, ya sea cuando son dados de baja o cambian de propietario.

- El área de Informática y Comunicaciones debe revisar los accesos físicos de personal, en horas no hábiles, a las áreas donde se procesa información.

- El área de Informática y Comunicaciones debe restringir el acceso físico de personal, a los equipos de cómputo de las áreas donde se procesa información sensible.

- El área de Informática y Comunicaciones debe asegurarse de que los equipos que se encuentren sujetos a traslados físicos fuera de la Institución se encuentren incluidos en la póliza de seguro de la ETITC.

- El área de Informática y Comunicaciones es la única autorizada a realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, está prohibida la disposición que pueda hacer los Servidores Públicos, Proveedores y demás partes interesadas de los recursos tecnológicos de la ETITC.

Personal de Seguridad Perimetral:

- El Personal de Seguridad Perimetral debe velar por la salida y entrada de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales, los mismos deben contar con la respectiva autorización documentada y aprobada por los propietarios de los activos de información de cada área y el Profesional de bienes muebles.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe validar periódicamente el inventario de activos tipo hardware, al área de Informática y Comunicaciones, con el objetivo de identificar posibles riesgos de seguridad.

Servidores Públicos, Proveedores y demás partes interesadas:

- Los Servidores Públicos, Proveedores y demás partes interesadas deben acogerse a las instrucciones técnicas que proporcione el área de Informática y Comunicaciones

relacionadas con las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos.

- Cuando se presente una falla, problema de hardware o software en una estación de trabajo u otro recurso tecnológico, propiedad de la ETITC, el servidor público, proveedor, parte interesada, debe informar a la Mesa de Ayuda, donde se atenderá o escalará el caso, con el fin de realizar una asistencia adecuada. El servidor público, proveedor, parte interesada, no debe intentar solucionar el problema.

- La instalación, reparación o retiro de cualquier componente de hardware o software, de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la ETITC, solo puede ser realizado por los servidores públicos del área de Informática y Comunicaciones.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben bloquear el computador asignado, en el momento de abandonar su puesto de trabajo.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos, en horario no laboral.

- Los equipos de cómputo, bajo ninguna circunstancia, deben ser desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, para garantizar su integridad física.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a golpes ni fuertes campos electromagnéticos.

- En caso de pérdida o robo, de un equipo de cómputo o recurso tecnológico de la ETITC, se debe informar de forma inmediata al propietario y custodio de los activos de información del área, reportar el incidente a la mesa de ayuda para que se inicie el trámite de investigación interna y, en caso necesario, denunciar ante las autoridades competentes el caso.

14.3- Política de Seguridad para el Ingreso de Equipos Externos.

Objetivo:

Garantizar que los recursos tecnológicos externos que ingresan a la ETITC sean identificados para brindar una conexión óptima y segura, durante las operaciones internas que realicen haciendo uso adecuado de la conectividad en la red institucional.

Alcance

La Política de Seguridad para el ingreso de Equipos Externos será aplicada por el área o proceso asignado por la Alta Dirección, Profesional de Informática y Comunicaciones, Personal de Seguridad Perimetral, Profesional de Seguridad de la Información, Servidores Públicos, Proveedores y demás partes interesadas.

Directrices

Para el cumplimiento de la Política de Seguridad para el ingreso de Equipos Externos, es necesario registrar una única vez el activo tipo hardware (Laptop, Tablets) a través del siguiente link: https://forms.office.com/r/Birqgy3jfZ luego dirigirse al Salón E102 (Laboratorio Festo), para la adición del stiker QR único para (Laptop, Tablets). Adicional, debe figurar el propietario de cada activo con sus datos de identificación en este caso cédula de ciudadanía, serial del equipo, color y marca.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Área o Proceso Asignado:

- Debe proveer los mecanismos y estrategias necesarios, para el registro de recursos tecnológicos externos que ingresan dentro de las instalaciones de la ETITC.

- Debe realizar copias de seguridad y actualización de base de datos en el sistema TOIOTEM de la ETITC.

Profesional de Informática y Comunicaciones:

- Profesional de Informática y Comunicaciones debe garantizar la conectividad segura de los Equipos Externos, para los activos tipo hardware (Laptops, Tablets) de los Servidores Públicos, Proveedores y demás partes interesadas.

Personal de Seguridad Perimetral:

- El Personal de Seguridad Perimetral debe velar por el registro de ingreso y salida de los recursos tecnológicos externos, los mismos deben figurar el propietario de cada activo con sus datos de identificación en este caso cédula de ciudadanía, serial del equipo, color y marca.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe validar periódicamente los registros, copias de seguridad y actualizaciones del sistema TOIOTEM de la ETITC., con el objetivo de identificar posibles riesgos de seguridad.

Servidores Públicos, Proveedores y demás partes interesadas:

- Servidores Públicos, Proveedores y demás partes interesadas deben acogerse a las instrucciones técnicas que proporcione el área o proceso asignado por la Alta Dirección para el ingreso de los recursos tecnológicos externos.

- Cuando se presente deterioro del stiker o cambio de equipo deben dirigirse al Salón E102 (Laboratorio Festo), para el cambio y/o adición del stiker QR único para (Laptops, Tablets).

14.4- Política de Escritorio Limpio y Pantalla Limpia.

Objetivo:

Garantizar que los servidores públicos de la ETITC, proveedores y partes interesadas, que tengan acceso a las instalaciones físicas, sistemas de información y equipos de cómputo, mantengan sus escritorios libres de documentos o dispositivos de almacenamiento, guardándolos en sitios seguros, durante la jornada laboral y después de la misma, a su vez, mantengan el escritorio de los equipos de cómputo libres de documentación sensible y accesos directos.

Alcance

La Política de Escritorio Limpio y Pantalla Limpia será aplicada por todos los Servidores Públicos, Proveedores y demás partes interesadas, que tengan acceso a las instalaciones físicas, sistemas de información y equipos de cómputo de la ETITC.

Directrices

Para el cumplimiento de la Política de Escritorio Limpio y Pantalla Limpia, es necesario que todos los equipos de cómputo de la ETITC, se encuentren ingresados al dominio institucional.

Además, el inventario de activos de información tipo hardware debe actualizarse de manera periódica.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- Mantener actualizado el inventario de activos tipo hardware.
- Garantizar que todos los equipos de cómputo se encuentren ingresados al dominio institucional.
- Establecer, a nivel de controlador de dominio, un bloqueo de sesión de usuario, cuando transcurra cierto y determinado tiempo de inactividad.
- Garantizar que todos los equipos de cómputo sean instalados en el puesto de trabajo, de manera que la pantalla del monitor, no pueda ser visualizada por personal no autorizado.
- Garantizar que la autenticación de usuario sea requerida, cada vez que el equipo de cómputo se encienda, reinicie o bloquee.

Infraestructura y Planta Física:

- Garantizar que todos los puestos de trabajo y áreas, cuenten con suficientes cajones y/o archivadores, con sus respectivas chapas de seguridad, para almacenar toda la documentación física, que requiera protegerse.

Servidores Públicos, Proveedores y demás partes interesadas:

- No deben ingerir alimentos o bebidas cerca de equipos de cómputo, documentación física y medios magnéticos, así como, evitar manipular líquidos en su cercanía.
- Bloquear la sesión de usuario, cuando se ausente del puesto de trabajo y/o deje los equipos desatendidos, para proteger el acceso a la documentación digital, aplicaciones y servicios de la ETITC.
- Guardar toda la documentación física y/o medio magnético en cajones, archivadores o sitios seguros, durante su ausencia del puesto de trabajo, manteniendo el mismo, libre de documentación física y medios magnéticos.
- Cerrar correctamente la sesión de usuario y apagar el equipo de cómputo y periféricos, cuando finalice la jornada laboral, garantizando con esto, una desconexión satisfactoria de la red institucional.
- Evitar colocar documentos sensibles o accesos directos a los mismos, en el escritorio del equipo de cómputo, manteniendo el mismo, limpio y seguro.
- Retirar de las impresoras, escáner y fax, toda documentación física, evitando de esta manera la exposición de la información a personal no autorizado.

15. POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES.

15.1- Política de Asignación de Responsabilidades Operativas.

Objetivo:

Garantizar que se elabore, revise y apruebe toda la documentación operativa y administrativa de la plataforma tecnológica de la ETITC, favoreciendo con esto, el cumplimiento de las responsabilidades operativas asignadas a cada servidor público del área de Informática y Comunicaciones.

Alcance

La Política de Asignación de Responsabilidades Operativas será aplicada por el área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información de la ETITC.

Directrices

Para el cumplimiento de la Política de Asignación de Responsabilidades Operativas es necesario la existencia de instructivos, manuales o guías sobre todos los recursos y servicios tecnológicos de la ETITC. Por citar algunos ejemplos, instructivos de backups, actualización de servidores, administración de servicios (Directorio Activos, DNS, Firewall, etc.).

Adicional, toda la documentación relacionada con operación y administración de la plataforma tecnológica de la ETITC debe ser etiquetada como Reservada y almacenada en un espacio que ofrezca unas condiciones de seguridad óptima.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe elaborar, revisar y aprobar, a través de sus servidores públicos, la documentación y/o procedimientos, relacionados con la operación y administración de la plataforma tecnológica de la ETITC.

- El área de Informática y Comunicaciones debe proporcionar, a sus servidores públicos, manuales o instructivos de configuración y/o operación de los sistemas operativos para servidores, actualización de servidores, servicios de red, backups, y sistemas de información que conforman la plataforma tecnológica de la ETITC.

- El área de Informática y Comunicaciones debe proveer los recursos necesarios que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en

cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- El área de Informática y Comunicaciones, a través de sus servidores públicos, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos tecnológicos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica de la ETITC. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

- El área de Informática y Comunicaciones debe clasificar toda la documentación de operación y administración de la plataforma tecnológica de la ETITC, como Pública Reservada y etiquetada como Reservada.

- El área de Informática y Comunicaciones debe garantizar un espacio seguro para toda la documentación de operación y administración de la plataforma tecnológica de la ETITC, evitando en todo momento, que personal no autorizado tenga acceso a dicha documentación y la use con fines mal intencionados.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe emitir conceptos y generar recomendaciones, acerca de las soluciones de seguridad, propuestas por el área de Informática y Comunicaciones, para la plataforma tecnológica de la ETITC.

- El Profesional de Seguridad de la Información debe monitorear periódicamente el cumplimiento de la actividad de clasificación y etiquetado, de la documentación de operación y administración de la plataforma tecnológica de la ETITC.

- El Profesional de Seguridad de la Información debe monitorear periódicamente, las condiciones de seguridad de los espacios destinados para el almacenamiento de la documentación de operación y administración, de la plataforma tecnológica de la ETITC.

15.2- Política de Protección contra Códigos Maliciosos.

Objetivo:

Garantizar que todos los equipos informáticos de la ETITC, posean software antivirus, antimalware, antispam y antispyware instalados y configurados, para de esta forma, evitar la infección de software maliciosos en la red institucional, que pongan en riesgo la preservación de la confidencialidad, integridad y disponibilidad de la información, generada, procesada y custodiada por la ETITC.

Alcance

La Política de Protección contra Códigos Maliciosos será aplicada por el área de Informática y Comunicaciones, además todos los Servidores Públicos, Proveedores y demás partes interesadas que utilicen equipos informáticos de la Institución.

Directrices

Para el cumplimiento de la Política de Protección contra Códigos Maliciosos es necesario que la ETITC cuente con software antivirus, antimalware, antispam y antispyware, debidamente licenciados, instalados y configurados en cada uno de los equipos informáticos de la plataforma tecnológica de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de infección de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la ETITC y los servicios que se prestan en la misma.
- El área de Informática y Comunicaciones debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualizaciones periódica de las últimas bases de datos de firmas del proveedor del servicio.

- El área de Informática y Comunicaciones debe certificar que la información almacenada en la plataforma tecnológica de la ETITC, sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- El área de Informática y Comunicaciones, mediante sus servidores públicos, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware instalados en los equipos institucionales.
- El área de Informática y Comunicaciones debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe monitorear periódicamente el cumplimiento de la actividad contra Códigos Maliciosos es necesario que la ETITC cuente con software antivirus, antimalware, antispam y antispyware, debidamente licenciados, instalados y configurados en cada uno de los equipos informáticos de la plataforma tecnológica de la ETITC.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam, definida por el área de Informática y Comunicaciones; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios de almacenamiento.
- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben asegurarse de que los archivos adjuntos, provenientes de correos electrónicos o copiados de cualquier medio de almacenamiento externo, provienen de fuentes conocidas y seguras, para evitar la infección de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos de la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas que sospechen o detecten alguna infección por software malicioso, deben notificar a la Mesa de Ayuda de la ETITC para que, a través de ella, el área de Informática y Comunicaciones tome las medidas de control correspondientes.

15.3- Política de Copias de Respaldo de la Información.

Objetivo:

Garantizar que la información generada, procesada y custodiada por la ETITC, se encuentre respaldada, mediante copias de seguridad, que preservarán la disponibilidad de los datos institucionales que, en adición, serán sometidos a pruebas de restauración que verificarán el grado de integridad de estos.

Directrices

Para el cumplimiento de la Política de Copias de Respaldo de la Información es necesario la elaboración y aprobación del procedimiento de Copia de Respaldo a través de GIC-PC-05 Procedimiento de Copia de Respaldo de la Información, así mismo el procedimiento de Restauración GIC-PC-17 Restauración de la Información.

Adicional la ETITC debe contar con suficiente tecnología de almacenamiento, para soportar por periodos prolongados, las copias de seguridad de la información generadas donde se define en el formato GSI-FO-03 Matriz de inventario general de activos de la ETITC los criterios de este:

Periocidad del backup: Mensual – Diario – Trimestral – Semestral y/o Anual
Tipo de backup: Completo y/o Incremental
Lugar de almacenamiento: Virtual – Físico o en los dos casos Virtual/Físico

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información deben elaborar los procedimientos para la ejecución y restauración de las copias de respaldo de la información institucional.

Informática y Comunicaciones:

- El área Informática y Comunicaciones deben garantizar la ejecución periódica de los Procedimientos de Copia de Respaldo y Restauración de la Información de la ETITC.

- El área de Informática y Comunicaciones debe disponer de los recursos tecnológicos necesarios, para permitir la identificación y disposición de los medios de almacenamiento, que soportarán las copias de seguridad de la información institucional.

- El área de Informática y Comunicaciones debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información de la ETITC, que son almacenadas externamente.

- El área de Informática y Comunicaciones debe definir la estructura organizacional de directorios de respaldo y estrategia de retención y rotación, de las copias de respaldo de la información institucional.

- El área de Informática y Comunicaciones debe definir y aprobar los tiempos en que se efectuarán las actividades de copia de respaldo y restauración de la información de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe monitorear periódicamente, el cumplimiento de las actividades de generación de copias de respaldo de la información institucional y el ejercicio de restauración de esta, para verificar el estado en que se encuentra.

15.4- Política de Registro de Eventos y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información.

Objetivo:

Garantizar que todos los recursos tecnológicos y sistemas de información de la ETITC, cuenten con un sistema de monitoreo periódico, de los registros de eventos generados y almacenados, en la plataforma tecnológica de la ETITC.

Alcance

La Política de Registro de Eventos y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información, será aplicada por el área de Informática y Comunicaciones y el Profesional de Seguridad de la Información.

Directrices

Para el cumplimiento de la Política de Registro de Eventos y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información de la ETITC, es necesario identificar los recursos y sistemas que requieren un monitoreo periódico de los registros de eventos generados.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe determinar los eventos, que generarán registros, en los recursos tecnológicos y los sistemas de información de la ETITC.
- El área de Informática y Comunicaciones debe definir qué tipo de monitoreo efectuará a los registros, especialmente sobre aquellos registros que provengan de los sistemas de información o recursos tecnológicos que gestionan procesos misionales.
- El área de Informática y Comunicaciones debe garantizar la integridad y disponibilidad de los registros generados en la plataforma tecnológica de la ETITC.
- El área de Informática y Comunicaciones debe garantizar, que los registros generados, sean revisados solo el personal autorizado.
- El área de Informática y Comunicaciones debe efectuar un monitoreo, mediante aplicativo, sobre los recursos tecnológicos de la ETITC, que permitan evidenciar registros de eventos, tales como reinicio de equipos, equipos fuera de servicio, información sobre el rendimiento de trabajo de los equipos, intermitencias, etc.
- El área de Informática y Comunicaciones debe definir los periodos de retención, de los registros generados y almacenados, en la plataforma tecnológica de la ETITC.
- El área de Informática y Comunicaciones deben generar registros de las actividades realizadas por los usuarios finales y administradores, en los sistemas de información de la ETITC.
- El área de Informática y Comunicaciones deben registrar, en los registros de eventos, fallas de: validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros.
- El área de Informática y Comunicaciones deben evitar almacenar datos innecesarios, en los sistemas de información de la ETITC y en los registros de eventos.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe revisar periódicamente los registros generados de los recursos tecnológicos y los sistemas de información de la ETITC, con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

15.5- Política de Control de Software Operacional.

Objetivo:

Garantizar que todo el software operacional, que está instalado en la plataforma tecnológica de la ETITC, se encuentre operando en los niveles óptimos de seguridad.

Alcance

La Política de Control de Software Operacional, será aplicada por el área de Informática y Comunicaciones.

Directrices

Para el cumplimiento de la Política de Control de Software Operacional, es necesario que el área de Informática y Comunicaciones, identifique el software operativo que está instalado en la plataforma tecnológica de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe asegurarse que el software operativo, instalado en la plataforma tecnológica de la ETITC, cuente con el soporte de los proveedores, en caso de que así lo requiera.

- El área de Informática y Comunicaciones debe conceder, accesos temporales y controlados, a los proveedores que realizan actualizaciones del software operativo, en los casos que lo requiera.

- El área de Informática y Comunicaciones debe validar los riesgos, que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica, cuando el software operativo es actualizado.

- El área de Informática y Comunicaciones debe establecer las restricciones y limitaciones, para la instalación de software operativo, en los equipos de cómputo de la ETITC.

15.6- Política de Gestión de la Vulnerabilidad Técnica.

Objetivo:

Garantizar que las vulnerabilidades identificadas, mediante la aplicación de una Metodología de Pruebas de Efectividad, reciban un tratamiento óptimo para lograr mitigarlas.

Alcance

La Política de Gestión de la Vulnerabilidad Técnica, será aplicada por el área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información de la ETITC.

Directrices

Para el cumplimiento de la Política de Gestión de la Vulnerabilidad Técnica se requiere la elaboración de una Metodología de Pruebas de Efectividad.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe elaborar la Metodología de Pruebas de Efectividad para la ETITC.
- El Profesional de Seguridad de la Información debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades detectadas, a raíz de la aplicación de las pruebas de efectividad.
- El Profesional de Seguridad de la Información debe monitorear, periódicamente, el cumplimiento de los planes de acción, elaborados y ejecutados por el área de Informática y Comunicaciones de la ETITC.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe revisar, periódicamente, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información de la ETITC.
- El área de Informática y Comunicaciones debe elaborar y ejecutar planes de acción, para mitigar las vulnerabilidades técnicas, detectadas en la plataforma tecnológica y sistemas de información de la ETITC.

- El área de Informática y Comunicaciones debe garantizar los recursos tecnológicos y profesionales para la planificación y ejecución de las pruebas de efectividad.

16. POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES.

16.1- Política de Gestión de la Seguridad de las Redes.

Objetivo:

Garantizar que los accesos a las redes de datos institucionales cuenten con lineamientos y controles de seguridad, que impidan que personal, no autorizado, conecten equipos en la LAN de la ETITC para fines no esclarecidos.

Alcance

La Política de Gestión de la Seguridad de las Redes, será aplicada por el área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información de la ETITC.

Directrices

Para el cumplimiento de la Política de Gestión de la Seguridad de las Redes, se requiere identificar los recursos tecnológicos y servicios de la red institucional de la ETITC.

Adicional la ETITC debe disponer de un servicio de protección perimetral, configurado en alta disponibilidad.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe adoptar medidas para asegurar la disponibilidad de los recursos tecnológicos y servicios de red de la ETITC.

- El área de Informática y Comunicaciones debe implantar controles, para minimizar los riesgos de seguridad de la información, transportada por medio de las redes de datos de la ETITC.

- El área de Informática y Comunicaciones debe mantener, las redes de datos, segmentadas por dominios, grupos de servicios, grupos de usuarios, áreas, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Institución.

- El área de Informática y Comunicaciones debe garantizar la configuración óptima, de los dispositivos de seguridad perimetral de la red institucional.

- El área de Informática y Comunicaciones debe identificar, justificar y documentar los servicios, protocolos y puertos de comunicación, autorizados por la ETITC, en las redes de datos institucionales e inhabilitar o eliminar el resto de servicios, protocolos y puertos que no se utilicen o que constituyan un riesgo en su operación.

- El área de Informática y Comunicaciones debe definir mecanismos de protección entre las redes internas de la ETITC y cualquier red externa, que esté fuera de la capacidad de control y administración de la Institución.

- El área de Informática y Comunicaciones debe preservar la confidencialidad de la información relacionada con el direccionamiento IP y enrutamiento de paquetes, desde la LAN de la ETITC, hacia y desde el exterior.

- El área de Informática y Comunicaciones debe garantizar una configuración de seguridad en los dispositivos activos, de la red institucional de la ETITC.

- El área de Informática y Comunicaciones debe garantizar una solución, que permita autenticar usuarios en un sistema, para después facilitarles el servicio de internet vía WIFI, mediante la plataforma tecnológica de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe monitorear, frecuentemente, los controles de seguridad, definidos por el área de Informática y Comunicaciones, para las redes de datos de la ETITC.

16.2- Política de Uso del Correo Electrónico Institucional.

Objetivo:

Garantizar que el servicio de correo electrónico institucional se encuentre al alcance de todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC cumpliendo, además,

con todos los lineamientos de seguridad que contribuyan a la preservación de la confidencialidad y buenas prácticas en su uso.

Alcance

La Política de Uso del Correo Electrónico Institucional, será aplicada por el área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información y todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

Directrices

Para el cumplimiento de la Política de Uso del Correo Electrónico Institucional se debe definir y aprobar el Procedimiento para la Creación de Cuentas de Correo Electrónico Institucional.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones

- El área de Informática y Comunicaciones debe elaborar y aprobar un Procedimiento para la Creación de Cuentas de Correo Electrónico Institucional.

- El área de Informática y Comunicaciones debe definir los lineamientos para el uso del servicio de correo electrónico institucional.

- El área de Informática y Comunicaciones debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico institucional.

- El área de Informática y Comunicaciones debe garantizar la protección de la plataforma de correo electrónico institucional, contra código malicioso que pudiera ser transmitido a través de los mensajes enviados y recibidos.

- El área de Informática y Comunicaciones debe definir y aprobar, el mensaje legal corporativo de confidencialidad para la ETITC, en el correo electrónico institucional.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben ser conscientes que la cuenta de correo electrónico institucional asignada, es de carácter

individual; por consiguiente, nadie, en ninguna circunstancia, debe utilizar una cuenta de correo diferente a la asignada y aprobada para el desempeño de sus funciones en la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben hacer uso del correo electrónico institucional, solo para cumplir con el desempeño de sus funciones, evitando utilizarlo para usos personales y ajenos a los intereses de la Institución.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben conocer y aceptar que todos los mensajes e información, contenida en los buzones de correo electrónico institucional, son propiedad de la ETITC y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben enviar cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones, que degraden la condición humana y resulten ofensivas para los servidores públicos, estudiantes de la Institución y el personal provisto por terceras partes.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben utilizar el correo electrónico institucional para el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben respetar, en todos los casos, el mensaje legal corporativo de confidencialidad para la ETITC, incluido en el formato de mensaje para el correo institucional.

16.3- Política de Uso Adecuado de Internet.

Objetivo:

Garantizar que todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC, utilicen adecuadamente el servicio de internet institucional, evitando servirse de él para fines personales o que vayan en contra de los objetivos misionales de la Institución.

Alcance

La Política de Uso Adecuado de Internet, será aplicada por el área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información y todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

Directrices

Para el cumplimiento de la Política de Uso Adecuado de Internet se requiere, como mínimo, la adquisición de un canal de internet en operación.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe proporcionar los recursos tecnológicos y humanos, necesarios para la implementación, administración y mantenimiento, requeridos para la prestación segura del servicio de Internet institucional, y cuando aplique, bajo las restricciones de los perfiles de acceso de usuarios establecidos.

- El área de Informática y Comunicaciones debe diseñar e implementar, mecanismos que permitan la continuidad o restablecimiento, del servicio de Internet, en caso de una afectación interna y/o externa.

- El área de Informática y Comunicaciones debe monitorear continuamente el canal o canales del servicio de Internet adquiridos.

- El área de Informática y Comunicaciones debe definir e implementar controles, para evitar la descarga de software no autorizado y/o código malicioso, proveniente de Internet y evitar el acceso a sitios catalogados como restringidos o no gratos para la ETITC.

- El área de Informática y Comunicaciones debe generar registros de la navegación y los accesos de los usuarios a Internet, así como definir e implementar controles de monitoreo sobre la utilización del servicio de Internet institucional.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben evitar la descarga de software desde el internet institucional, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben acceder a páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking y/o cualquier otra página web que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este manual para la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben descargar, usar, intercambiar y/o instalar juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de los autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica y sistemas de información de la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben intercambiar información institucional, de manera no autorizada, con terceros.

16.4- Política de Transferencia de Información.

Objetivo:

Garantizar que la información de la ETITC sea transferida, hacia terceros que la requieran, cumpliendo con una serie de lineamientos, controles y procedimientos, para de esta manera, garantizar la preservación de la confidencialidad e integridad de los datos institucionales.

Alcance

La Política de Transferencia de Información será aplicada por el área de Contratación, Informática y Comunicaciones, además por Líder de Área o Supervisor de Contrato, Profesional de Seguridad de la Información, Propietarios de la Información, Archivo y Correspondencia, servidores públicos, partes interesadas, con quienes se intercambia información de la ETITC.

Directrices

Para el cumplimiento de la Política de Transferencia de Información debe elaborarse y aprobarse un Procedimiento de Intercambio de Información Física y un Procedimiento de Intercambio de Información Digital para la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Área de Contratación:

- El Área de Contratación debe definir el modelo de Acuerdo y/o Cláusula de Confidencialidad para los contratistas de la ETITC, incluyendo los compromisos adquiridos y las penalidades para el incumplimiento de dicho acuerdo.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe elaborar el Procedimiento de Intercambio de Información Física y el Procedimiento de Intercambio de Información Digital para la ETITC.

Propietarios de la Información:

- Los Propietarios de la Información deben velar porque la información de la ETITC, sea protegida de divulgación no autorizada, por parte de los terceros, a quienes se entrega esta información, verificando el cumplimiento de la Cláusula y/o Acuerdo de Confidencialidad.
- Los Propietarios de la Información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregados a terceros, previo consentimiento de los titulares de estos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los Propietarios de la Información deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

Servidor Público de Correspondencia:

- El servidor público de correspondencia debe hacer uso del Procedimiento de Intercambio de Información Física con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- El servidor público de correspondencia debe certificar que todo envío de información física a terceros (documento o medio magnético), utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la ETITC, y que estos permitan ejecutar rastreo de las entregas.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del Procedimiento para el Intercambio de Información Digital, con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Terceros con quienes se intercambia información:

- Los Terceros con quienes se intercambia información de la ETITC deben darle un manejo adecuado a la información recibida, en cumplimiento de las Políticas de Seguridad de la Institución, de las condiciones contractuales establecidas y de los Procedimientos de Intercambio de Información Física y Digital, definidos y aprobados por la ETITC.

Servidores Públicos, Proveedores y demás partes interesadas:

- Los Servidores Públicos, Proveedores y demás partes interesadas no deben intercambiar información sensible de la ETITC, vía telefónica.

17. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

17.1- Política de Requisitos de Seguridad de los Sistemas de Información.

Objetivo:

Garantizar que todos los sistemas de información desarrollados o adquiridos por la ETITC, cumplan con lineamientos y controles de seguridad, que garanticen la preservación de la confidencialidad, integridad y disponibilidad de la información institucional.

Alcance

La Política de Requisitos de Seguridad de los Sistemas de Información será aplicada por el área de Informática y Comunicaciones y Desarrolladores Internos y/o Externos.

Directrices

Para el cumplimiento de la Política de Requisitos de Seguridad de los Sistemas de Información de la ETITC, es necesario que se elabore y apruebe una metodología para el desarrollo de software.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Custodios de los Sistemas de Información / Profesional de Seguridad de la Información:

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe definir los custodios de los sistemas de información de la ETITC, bajo su responsabilidad.
- El área de Informática y Comunicaciones debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las

buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

- El área de Informática y Comunicaciones debe definir los protocolos para el desarrollo de los sistemas de información de la ETITC.

Informática y Comunicaciones / Seguridad de la Información:

- El área Informática y Comunicaciones en conjunto con el área de Seguridad de la Información, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

Desarrolladores Internos y/o Externos:

- Los Desarrolladores Internos y/o Externos deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles definidos.

- Los Desarrolladores Internos y/o Externos deben garantizar que todo sistema de información adquirido o desarrollado, para la ETITC, utilicen herramientas de desarrollo licenciadas y reconocidas en el mercado.

- Los Desarrolladores Internos y/o Externos deben deshabilitar las funcionalidades de completar automáticamente, en formularios de solicitud de datos, que requieran información sensible.

- Los Desarrolladores Internos y/o Externos deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

- Los Desarrolladores Internos y/o Externos deben asegurar que no se permitan conexiones recurrentes, a los sistemas de información de la ETITC, construidos con el mismo usuario.

- Los Desarrolladores Internos y/o Externos deben utilizar, los protocolos sugeridos por el área de Informática y Comunicaciones, para el desarrollo de los sistemas de información de la ETITC.

- Los Desarrolladores Internos y/o Externos deben garantizar la seguridad de la transmisión de la información, relacionada con pagos o transacciones en línea, a los operadores encargados, por medio de canales seguros.

17.2- Política de Seguridad en los Procesos de Desarrollo y Soporte de los Sistemas de Información.

Objetivo:

Garantizar que todos los sistemas de información de la ETITC cumplan con lineamientos de seguridad y soporte, que garanticen la preservación de la confidencialidad, integridad y disponibilidad de los datos institucionales, soportados en los aplicativos de la ETITC.

Alcance

La Política de Seguridad en los Procesos de Desarrollo y Soporte de los Sistemas de Información será aplicada por el área de Informática / Comunicaciones, Desarrolladores Internos y/o Externos y el Profesional de Seguridad de la Información de la ETITC.

Directrices

Para el cumplimiento de la Política de Seguridad en los Procesos de Desarrollo y Soporte de los Sistemas de Información se debe elaborar y aprobar una metodología de transición de ambientes y una metodología de pruebas del software, desarrollado para la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones, es responsable de realizar las pruebas pertinentes, para asegurar que los aplicativos institucionales cumplen con los requerimientos de seguridad establecidos, antes de pasar a la fase de producción.

- El área de Informática y Comunicaciones, debe elaborar y utilizar una metodología de transición de ambientes, documentando las pruebas de transición realizadas.

- El área de Informática y Comunicaciones, debe realizar pruebas de eficiencia, a los sistemas de información de la ETITC, cuando se efectúen y aprueben modificaciones o ajustes en la funcionalidad de los aplicativos o cuando se efectúen cambios en los recursos tecnológicos que soporta la operación de los aplicativos institucionales.

- El área de Informática y Comunicaciones, debe elaborar una metodología de pruebas para el software desarrollado.

- El área de Informática y Comunicaciones debe implantar, los controles necesarios, para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas por los líderes de las áreas correspondientes.

- El área de Informática y Comunicaciones debe controlar las versiones de los sistemas de información de la ETITC, para de esta manera, garantizar buenas prácticas en la administración de los cambios propuestos y aprobados.

- El área de Informática y Comunicaciones debe asegurase, que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- El área de Informática y Comunicaciones debe garantizar que los recursos tecnológicos, las herramientas de desarrollo y los componentes, de cada sistema de información, estén actualizados con todos los parches disponibles, para las versiones en uso y que estén ejecutando la última versión aprobada.

Desarrolladores Internos y/o Externos:

- Todos los Desarrolladores Internos y/o Externos deben considerar las buenas prácticas y lineamientos de desarrollo seguro, durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- Todos los Desarrolladores Internos y/o Externos deben proporcionar un nivel adecuado de soporte, para solucionar los problemas que se presenten en el software desarrollado para la ETITC; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Todos los Desarrolladores Internos y/o Externos deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Todos los Desarrolladores Internos y/o Externos deben asegurar que los sistemas de información de la ETITC, validen la información suministrada por los usuarios, antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos, caracteres de alteración de rutas, entre otros.

- Todos los Desarrolladores Internos y/o Externos deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout), que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

- Todos los Desarrolladores Internos y/o Externos deben asegurar el manejo de operaciones sensibles o críticas, en los aplicativos desarrollados para la ETITC, permitiendo el uso de opciones de seguridad adicionales, como tokens o el ingreso de parámetros adicionales de verificación de autenticidad en caso que se requiera.

- Todos los Desarrolladores Internos y/o Externos deben asegurar que los aplicativos de la ETITC, proporcionen la mínima información de la sesión establecida y almacenada en cookies.

- Todos los Desarrolladores Internos y/o Externos deben garantizar que no se divulgue información sensible de la ETITC en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de errores genéricos.

- Todos los Desarrolladores Internos y/o Externos deben remover todas las funcionalidades y archivos, que no sean necesarios para los aplicativos de la ETITC, previo a la puesta en producción.

- Todos los Desarrolladores Internos y/o Externos no deben divulgar la estructura de directorios, construidos para los sistemas de información de la ETITC.

- Todos los Desarrolladores Internos y/o Externos deben remover información innecesaria, en los encabezados de respuesta, que se refieran a los sistemas operativos y versiones del software institucional utilizado.

- Todos los Desarrolladores Internos y/o Externos deben evitar incluir las cadenas de conexión a las bases de datos, en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

- Todos los Desarrolladores Internos y/o Externos deben garantizar el cierre de la conexión a las bases de datos, desde los aplicativos, tan pronto como estas no sean requeridas.

- Todos los Desarrolladores Internos y/o Externos deben desarrollar los controles necesarios, para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios, destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

- Todos los Desarrolladores Internos y/o Externos deben proteger el código fuente de los aplicativos construidos, de tal forma, que no pueda ser descargado ni modificado por los usuarios.

- Todos los Desarrolladores Internos y/o Externos deben asegurar que no se permite que los aplicativos desarrollados para la ETITC, ejecuten comandos directamente en el sistema operativo.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe monitorear el cumplimiento de la ejecución de las pruebas de requerimientos de seguridad, pruebas de eficiencia, adicional, la metodología de transición de ambientes y la metodología de pruebas para el software desarrollado.

17.3- Política de Protección de los Datos de Prueba.

Objetivo:

Garantizar que los datos institucionales, suministrados a los desarrolladores y/o administradores de los sistemas de información de la ETITC, para la operación de los ambientes de prueba, se realice acorde al Procedimiento de Selección y Uso de Datos de Prueba, aprobado por el Sistema de Gestión de Calidad de la ETITC.

Alcance

La Política de Protección de los Datos de Prueba será aplicada por el área de Informática y Comunicaciones.

Directrices

Para el cumplimiento de la Política de Protección de los Datos de Prueba se requiere tener elaborado y aprobado un Procedimiento de Selección y Uso de Datos de Prueba.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe elaborar el Procedimiento de Selección y Uso de Datos de Prueba.

- El área de Informática y Comunicaciones debe implementar el Procedimiento de Selección y Uso de Datos de Prueba, cuando se requiera tomar información de los ambientes de producción, para los ambientes de prueba.

- El área de Informática y Comunicaciones debe garantizar la eliminación de la información, en los ambientes de prueba, una vez estos hayan concluido su operación.

- El área de Informática y Comunicaciones debe revisar a intervalos planificados el Procedimiento de Selección y Uso de Datos de Prueba, para efectuar los ajustes pertinentes cuando sea requerido.

18. POLÍTICAS DE RELACIONES CON LOS PROVEEDORES.

18.1- Política de Seguridad de la Información en las Relaciones con los Proveedores.

Objetivo:

Garantizar que las relaciones laborales de la ETITC, con los proveedores o terceros, se efectúen mediante el cumplimiento de lineamientos de seguridad de la información, para que, de esta manera, se preserve la confidencialidad, integridad y disponibilidad de los datos institucionales.

Alcance

La Política de Seguridad de la Información en las Relaciones con los Proveedores será aplicada por el área de Contratación, Informática y Comunicaciones, además por el Líder de Área o Supervisor de Contrato y el Profesional de Seguridad de la Información.

Directrices

Para el cumplimiento de la Política de Seguridad de la Información en las Relaciones con los Proveedores, se debe elaborar y aprobar la Cláusula y/o Acuerdo de Confidencialidad y la Cláusula y/o Acuerdo de Aceptación de las Políticas de Seguridad de la Información para la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Líder de Área o Supervisor de Contrato:

- El Líder de Área o Supervisor de Contrato debe divulgar las políticas y procedimientos de seguridad de la información para la ETITC, a todos los proveedores y/o terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de esta se realice de manera segura.

Área de Contratación:

- El área de Contratación debe incluir, de manera permanente, en los formatos de contratación los Acuerdos y/o Cláusulas de Confidencialidad y Aceptación de las Políticas de Seguridad de la Información para la ETITC.
- El área de Contratación debe incluir las Obligaciones del Contratista, definidas en el formato GAD-FO-05 Estudios Previos las directrices desde los Sistemas de Gestión Integrados.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe establecer las condiciones de conexión adecuada, para los equipos de cómputo y dispositivos móviles de los proveedores o terceros, en la red de datos de la Institución.

- El área de Informática y Comunicaciones debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros o proveedores de servicios.

- El área de Informática y Comunicaciones debe mitigar los riesgos relacionados con terceras partes o proveedores, que tengan acceso a los sistemas de información y los recursos tecnológicos de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe identificar y monitorear los riesgos relacionados con proveedores y terceras partes o los servicios provistos por ellas.

18.2- Política de Gestión de la Prestación de Servicios de Proveedores.

Objetivo:

Garantizar que toda prestación de servicios, por parte de proveedores o terceros, cumpla con una serie de lineamientos de seguridad, que preserven la confidencialidad, integridad y disponibilidad de la información institucional.

Alcance

La Política de Gestión de la Prestación de Servicios de Proveedores será aplicada por el área de Informática y Comunicaciones, además por el Líder de Área o Supervisor de Contrato de la ETITC.

Directrices

Para el cumplimiento de la Política de Gestión de la Prestación de Servicios de Proveedores debe elaborarse y aprobarse el Acuerdo y/o Cláusula de Confidencialidad y el Acuerdo y/o Cláusula de Aceptación de las Políticas de Seguridad de la Información de la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe estar presente, en el momento de la conexión a las redes de datos de la ETITC, de un equipo o dispositivo móvil, perteneciente a un proveedor o tercero, para verificar el cumplimiento de las condiciones de conexión a la red de datos institucional, para equipos o dispositivos móviles propiedad de proveedores o terceros.

- El área de Informática y Comunicaciones debe verificar las condiciones de comunicación segura, cifrado y transmisión de información, desde y hacia los terceros o proveedores de servicios que requieran acceso a información sensible.

Líder de Área o Supervisor de Contrato:

- El Líder de Área o Supervisor de Contrato debe monitorear periódicamente, el cumplimiento de las Obligaciones del Contratista, el Acuerdo y/o Cláusula de Confidencialidad y el Acuerdo y/o Cláusula de Aceptación de las Políticas de Seguridad de la Información de la ETITC, incluidas en el formato del contrato.

- El Líder de Área o Supervisor de Contrato debe administrar los cambios en el suministro de servicios, por parte de los proveedores o terceros, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

19. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

19.1- Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información.

Objetivo:

Garantizar una gestión de incidentes de seguridad óptima y adecuada, para de esta forma, mitigar los riesgos identificados y reportados, que afectan la preservación de la confidencialidad, integridad y disponibilidad de la información institucional.

Alcance

La Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información será aplicada por el área de Informática y Comunicaciones, además por el Propietarios de la Información, Custodios de la Información y Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

Directrices

Para el cumplimiento de la Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información, se debe tener una administración óptima de los incidentes de seguridad identificados y reportados, para ello se recomienda la documentación de los sucesos y el tratamiento realizado.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Propietarios de la Información / Custodios de la Información:

- Los Propietarios y Custodios de la Información deben informar a la mesa de ayuda, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe garantizar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información identificados y reportados.

- El área de Informática y Comunicaciones debe evaluar todos los incidentes de seguridad identificados y reportados, de acuerdo con sus circunstancias particulares e informar al Profesional de Seguridad de la Información sobre el tema.

- El área de Informática y Comunicaciones debe designar personal calificado, para investigar adecuadamente, los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su aparición nuevamente.

- El área de Informática y Comunicaciones debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos de la ETITC, con la mayor brevedad posible.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas, en caso de identificar la pérdida o divulgación, no autorizada, de la información clasificada y etiquetada como Clasificada y Reservada para la ETITC, deben notificarlo

inmediatamente, al Líder del Área o Supervisor de Contrato, para que se registre y se le dé el tratamiento adecuado al caso.

20. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO.

20.1- Política de Continuidad de Seguridad de la Información.

Objetivo:

Garantizar que la ETITC identifique los eventos, que constituyan una emergencia o desastre, elaborando con esto, un plan o planes de contingencia que permitirán mitigar los efectos adversos de la situación y le darán una continuidad al negocio exitosa, disminuyendo así, los riesgos de afectación de las operaciones institucionales, que afectan considerablemente el cumplimiento de la misión de la ETITC.

Alcance

La Política de Continuidad de Seguridad de la Información será aplicada por la Alta Dirección, área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información de la ETITC.

Directrices

Para el cumplimiento de la Política de Continuidad de Seguridad de la Información, se deben elaborar y aprobar los Plan de Contingencia, Recuperación y Retorno a la Normalidad.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Alta Dirección / Informática y Comunicaciones / Profesional de Seguridad de la Información:

- La Alta Dirección, el Profesional de Seguridad de la Información, el área de Informática y Comunicaciones, deben identificar las situaciones que serán concebidas como emergencia o desastre para la ETITC, los procesos y/o las áreas que la componen, la infraestructura tecnológica en general y definir cómo se debe actuar ante la presencia de dichos desastres.

- La Alta Dirección, el Profesional de Seguridad de la Información, el área de Informática y Comunicaciones, deben liderar los temas relacionados con la continuidad del negocio y la recuperación ante cualquier tipo de desastre.

- La Alta Dirección, el Profesional de Seguridad de la Información, el área de Informática y Comunicaciones, deben definir las estrategias de recuperación más convenientes para la ETITC.

- La Alta Dirección, el Profesional de Seguridad de la Información, el área de Informática y Comunicaciones, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y documentando el resultado de dichas pruebas.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación, en caso de activarse el plan de contingencia o continuidad del negocio, con las consideraciones de seguridad de la información a que sean pertinentes tener en cuenta.

- El Profesional de Seguridad de la Información debe garantizar que los Procedimientos de Contingencia, Recuperación y Retorno a la Normalidad, incluyan las consideraciones de seguridad de la información necesaria y requerida, para el cumplimiento de los objetivos trazados.

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información de la ETITC, deben elaborar un plan de recuperación ante desastres, para el Centro de Datos de la Institución y un conjunto de Procedimientos de Contingencia, Recuperación y Retorno a la Normalidad para cada uno de los servicios, sistemas operativos y recurso informático existente.

- El área de Informática / Comunicaciones y el Profesional de Seguridad de la Información de la ETITC, deben participar activamente en las pruebas de recuperación ante desastres planificadas y efectuadas, notificando los resultados obtenidos a la Alta Dirección.

20.2- Política de Redundancias.

Objetivo:

Garantizar que todos los sistemas de información, servicios y recursos tecnológicos de la ETITC, clasificados como críticos, cuenten con una solución redundante en su operación, para favorecer la preservación de la disponibilidad en su funcionamiento.

Alcance

La Política de Redundancias será aplicada por el área de Informática y Comunicaciones, además por el Profesional de Seguridad de la Información de la ETITC.

Directrices

Para el cumplimiento de la Política de Redundancias, la ETITC debe identificar los sistemas de información, servicios y recursos tecnológicos que contribuyen, en gran medida, al cumplimiento de los objetivos y misión institucional.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones / Profesional de Seguridad de la Información:

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información de la ETITC, debe analizar, identificar y definir los requerimientos de redundancia para los sistemas de información, servicios y recursos tecnológicos de la ETITC, clasificados como críticos.

- El área de Informática y Comunicaciones, de conjunto con el Profesional de Seguridad de la Información de la ETITC, debe evaluar, definir y aprobar, soluciones de redundancia para los sistemas de información, servicios y recursos tecnológicos de la ETITC, clasificados como críticos.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe administrar las soluciones de redundancia tecnológica de la ETITC y, además, realizar pruebas periódicas a dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de los sistemas de información, servicios y recursos tecnológicos institucionales, clasificados como críticos.

20.3- Política de Uso de Herramientas Institucionales en Teletrabajo

Objetivo:

Garantizar la confidencialidad, integridad y disponibilidad de la información haciendo el uso adecuado de las herramientas institucionales en situaciones que comprometan la continuidad de la operación.

Alcance

La Política de Uso de Herramientas Institucionales en Teletrabajo, será aplicada en el momento en que un servidor público deba realizar el cumplimiento de sus funciones fuera de las instalaciones de la ETITC.

Directrices

Para el cumplimiento de la política de Uso de Herramientas Institucionales en Teletrabajo, la ETITC, a través de la resolución 224 del 12 de mayo de 2023 “Por medio del cual se confiere la modalidad de teletrabajo suplementario a algunos servidores públicos de la ETITC” se definen en su artículo 7. CONDICIONES DE SERVICIO Y MEDIOS TECNOLÓGIGOS. El teletrabajador dispondrá de sus propias herramientas para el desarrollo del teletrabajo y así mismo se dictan las recomendaciones desde el SGSI, en su artículo 11. SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS:

El acceso a los diferentes entornos y sistemas informáticos de la entidad será efectuado siempre y en todo momento bajo el control y responsabilidad del teletrabajador, siguiendo los procedimientos establecidos por la entidad. El teletrabajador se compromete a respetar la legislación en materia de protección de datos y de la Política de Seguridad y Privacidad de la información, que la entidad ha implementado, como también a:

- Utilizar los datos de carácter personal a los que tenga acceso única y exclusivamente para cumplir con sus obligaciones para con la entidad.
- Cumplir con las medidas de seguridad que la entidad haya implementado para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso.
- No ceder en ningún caso a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación

Responsabilidades de áreas, organizaciones y personal de la ETITC

Informática y Comunicaciones:

- El proceso de Informática y Comunicaciones debe garantizar que las herramientas tecnológicas oficiales de la ETITC en Teletrabajo, entendiéndose como el paquete de Office 365 (Outlook, Word, Excel, Power Point, OneDrive, SharePoint, Teams, Forms, Stream, Sway), Campus Virtual y Sistemas de Información, estén disponibles para dar continuidad a la operación desde un espacio diferente a las instalaciones de la ETITC.

Profesional de Seguridad de la Información:

- El Profesional de Seguridad de la Información verifica los controles aplicables a través de GSI-FO-08 Inspección técnica de seguridad de la información periódicamente, en conjunto con el área de Talento Humano.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben hacer uso adecuado de las herramientas institucionales para dar cumplimiento a sus funciones.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben evitar el uso de herramientas diferentes a las autorizadas por la ETITC, para garantizar la confidencialidad, integridad y disponibilidad de la información.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben notificar al proceso de Informática y Comunicaciones cualquier novedad con respecto al funcionamiento de las herramientas tecnológicas institucionales.

21. POLÍTICAS DE CUMPLIMIENTO.

21.1- Política de Cumplimiento de Requisitos Legales y Contractuales.

Objetivo:

Garantizar que los requisitos legales, reglamentarios o contractuales, aplicables a la ETITC, se revisen periódicamente y se actualicen, respetándose con esto, el derecho de autor del software licenciados y en uso por parte de la Institucional, para el desarrollo de las funciones del colectivo laboral de la ETITC y el cumplimiento de la misión y objetivos institucionales.

Alcance

La Política de Cumplimiento de Requisitos Legales y Contractuales será aplicada por las dependencias de Vicerrectoría Administrativa/Financiera y Secretaria General, el área de Informática y Comunicaciones, además por todos los Servidores Públicos, Proveedores y demás partes interesadas de la ETITC.

Directrices

Para el cumplimiento de la Política de Cumplimiento de Requisitos Legales y Contractuales se debe elaborar y documentar los requisitos legales, reglamentarios o contractuales aplicables a la ETITC.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Vicerrectoría Administrativa y Financiera / Secretaria General:

- La Vicerrectoría Administrativa / Financiera y Secretaria General, mediante las áreas subordinadas a ellas (Oficina Asesora Jurídica, Contratación, Contabilidad, entre otras), deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables la Institución y relacionados con seguridad de la información.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe garantizar que todo software en operación en la plataforma tecnológica de la ETITC, esté protegido por derechos de autor y requiera licencia de uso o, en su lugar, sea software de libre distribución y uso.
- El área de Informática y Comunicaciones debe establecer un inventario con el software y sistemas de información, autorizados a operar en las estaciones de trabajo o equipos móviles de la ETITC, necesarios en el desarrollo de las actividades laborales, docentes y de investigación, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al autorizado.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas no deben instalar software o sistemas de información en las estaciones de trabajo o equipos móviles suministrados por la ETITC para el desarrollo de sus funciones.
- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación, sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

21.2- Política de Privacidad y Protección de Datos Personales.

Objetivo:

Garantizar que los datos personales almacenados, en los sistemas de información, repositorios y recursos informáticos de la ETITC, reciban una protección óptima, para preservar la confidencialidad, integridad y disponibilidad de estos.

Alcance

La Política de Privacidad y Protección de Datos Personales será aplicada por todas las áreas que recolecten, procesen y custodien datos personales de titulares.

Directrices

Para el cumplimiento de la Política de Privacidad y Protección de Datos Personales, la ETITC debe identificar los sistemas de información, repositorios y recursos informáticos que almacenan, recolectan y procesan datos personales, para fines institucionales.

Adicional se debe revisar la Ley 1581 de 2012 o Ley de Protección de Datos Personales.

Responsabilidades de áreas, organizaciones y personal de la ETITC

Áreas que Procesan Datos Personales:

- Todas las áreas que recolecten procesen y custodien datos personales de Servidores Públicos, Proveedores y demás partes interesadas, deben obtener la autorización, para el tratamiento de estos datos, con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir, dichos datos personales en el desarrollo de las funciones propias de la Institución.

- Todas las áreas que recolecten procesen y custodien datos personales de Servidores Públicos, Proveedores y demás partes interesadas, deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima, de acuerdo con sus funciones y responsabilidades, puedan tener acceso a dichos datos.

- Todas las áreas que recolecten procesen y custodien datos personales de Servidores Públicos, Proveedores y demás partes interesadas, deben establecer condiciones contractuales y de seguridad, a las entidades vinculadas, para el tratamiento de dichos datos personales.

- Todas las áreas que recolecten procesen y custodien datos personales de Servidores Públicos, Proveedores y demás partes interesadas, deben cumplir con las directrices técnicas establecidas, para enviar contenido institucional a los propietarios, mediante el correo electrónico y/o mensajes de texto.

Informática y Comunicaciones:

- El área de Informática y Comunicaciones debe establecer los controles respectivos, para el tratamiento y protección de los datos personales de los Servidores Públicos, Proveedores y demás partes interesadas, contenidos en los sistemas de información o repositorios, bajo su propiedad.

Servidores Públicos, Proveedores y demás partes interesadas:

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben guardar la discreción correspondiente, o la reserva absoluta, con respecto a la información de la Institución o del personal, el cual, teniendo en cuenta sus funciones, tiene acceso a los datos personales almacenados en la plataforma tecnológica de la ETITC.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben verificar la identidad de todas aquellas personas, a quienes se les entrega datos personales por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben asumir la responsabilidad individual, sobre las claves de acceso a sistemas de información, repositorios y recursos informáticos de la ETITC, que almacenen datos personales.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas deben aceptar el suministro de datos personales, que pueda hacer la ETITC, a terceros, para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.

- Todos los Servidores Públicos, Proveedores y demás partes interesadas o de cualquier persona con la cual la escuela tecnológica instituto técnico central tuviera establecida o estableciere una relación ocasional o permanente, el tratamiento de datos serán sometidos con fines institucionales. En todo caso, los datos personales podrán ser recolectados y tratados para:

- Dar cumplimiento a todos los compromisos contractuales.

- Realizar envió de información institucional al correo electrónico y/o mensajes de texto al teléfono móvil de acuerdo con los términos autorizados firmados en los siguientes

documentos: Contrato, Matricula Estudiantil IBTI, Matricula Educación Superior, entre otros que hagan parte de la vinculación con la ETITC.

- Mantener contacto con egresados en las diferentes profesiones o intereses a fines.

22. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
30/09/2016	1	Adopción del Documento.
19/04/2017	2	Inclusión del etiquetado del documento. Modificación de la Política General de Seguridad de la Información.
09/04/2018	3	Actualización del capítulo 7. Sanciones. Actualización de las políticas relacionadas con sistemas de información. Actualización de la Política de Protección de los Datos de Prueba. Actualización de la Política de Controles Criptográficos.
30/04/2019	4	Eliminación del Comité de Seguridad de la Información e inclusión del Comité Institucional de Gestión y desempeño. Inclusión de la Política General de Seguridad de la Información dentro del marco de la Política del Sistema de Gestión Integrado. Cambios en la redacción del documento. Adopción de los lineamientos de la estrategia de Gobierno Digital en el Manual.
30/04/2020	5	Cambios en la redacción del documento. Actualización de la sección términos y definiciones. Actualización 9.1- Política de Estructura Organizacional de Seguridad de la Información Inclusión de la 20.3- Política de Uso de Herramientas Institucionales en Teletrabajo

26/02/2021	6	Cambios en la redacción del documento Adopción lineamientos protección de datos personales
19/10/2022	7	Cambios en la redacción del documento Cambio de frases “Servidores públicos, Proveedores, Estudiantes, Ciudadanos y/o Visitantes”; y “Servidores públicos, Estudiantes, Proveedores y Partes Interesadas” por Servidores Públicos, Proveedores y demás partes interesadas. Actualización sección 14. POLÍTICAS DE SEGURIDAD FISICA Y DEL ENTORNO. Adopción lineamientos de carné digital en la 14.1- Política de Áreas Seguras, Sección- Servidores Públicos, Proveedores y demás partes interesadas. Inclusión de nueva Política 14.3- Política de Seguridad para el Ingreso de Equipos Externos. Asignación de numeral 14.3- al numeral 14.4- Política de Escritorio Limpio y Pantalla Limpia.
11/09/2023	8	Se realizan las siguientes mejoras al manual de políticas de seguridad de la información: Actualización sección 4. Términos y Definiciones el concepto de Teletrabajo suplementario. Actualización Sección 7. Sanciones: Tomando como base la derogatoria del Código Único Disciplinario (Ley 734 de 2022, Artículo 48 #43) por cambio al Código General Disciplinario (Ley 1952 de 2019. Artículo 55 #1). Inclusión de la periocidad y tipo de backup y lugar de almacenamiento en la sección 15.3- Política de Copias de Respaldo de la Información Inclusión del rol y la responsabilidad del líder del SGSI en la sección 15.4- Política de Registro de Eventos y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información. Inclusión del rol y la responsabilidad del Líder del SGSI, ante la política 13. POLÍTICAS DE CRIPTOGRAFÍA. Inclusión del rol y responsabilidad del área de Contratación donde incluya las Obligaciones del Contratista, definidas en el formato GAD-

		FO-05 Estudios Previos las directrices desde el Sistema de Gestión Integrado en la sección 18.1- Política de Seguridad de la Información en las Relaciones con los Proveedores. Inclusión del rol y la responsabilidad del Líder del SGSI, ante la política 15.2- Política de Protección contra Códigos Maliciosos. Actualización de directrices e inclusión de la resolución 224 del 12 de mayo de 2023, inclusión de roles y responsabilidades del líder del SGSI en la política 20.3- Política de Uso de Herramientas Institucionales en Teletrabajo.

ELABORÓ	REVISÓ	APROBÓ
Ing. SANDRA J. GUERRERO G. Líder de Gestión de Seguridad de la Información	**ANAY PINTO** Administrador de la Documentación	**DORA AMANDA MESA C.** Representante de la Dirección