

POLÍTICAS DE SEGURIDAD DIGITAL

“SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN”

Tecnológico de Antioquia
Institución Universitaria

Coordinación TIC

Contenido

CONTROL DE CAMBIOS	3
OBJETIVO	4
ALCANCE	4
DEFINICIONES.....	4
ETAPAS DE CONSTRUCCIÓN DE LAS POLÍTICAS DE SEGURIDAD DIGITAL ..	6
MARCO NORMATIVO	7
POLÍTICAS DE SEGURIDAD DIGITAL	9
POLÍTICA DE LA ORGANIZACIÓN.....	9
POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS.....	9
POLÍTICA DE CONTINUIDAD.....	10
POLÍTICA DE USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS	11
POLÍTICA DE GESTIÓN DE ACTIVOS DE TECNOLOGÍA Y DE INFORMACIÓN	13
POLÍTICA DE CONTROL DE ACCESO.....	13
POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE CONTRASEÑAS	14
POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO	15
POLÍTICA DE SEGURIDAD DE LAS OPERACIONES Y COMUNICACIONES	16
POLÍTICAS DE SEGURIDAD PARA LA RELACIÓN CON LOS PROVEEDORES DE SERVICIOS TECNOLÓGICOS	17
POLÍTICA DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	19
POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20

CONTROL DE CAMBIOS

Versión	Fecha de aprobación	Descripción del cambio
1.0	Marzo 2023	Creación del documento: Políticas de seguridad digital "Seguridad y privacidad de la información"

OBJETIVO

Establecer los lineamientos de seguridad digital que permitan garantizar la seguridad de los activos de información y de tecnología, garantizando la disponibilidad, integridad y confiabilidad de la información para el Tecnológico de Antioquia – Institución Universitaria (TdeA).

ALCANCE

Las Políticas de Seguridad Digital – “Seguridad y Privacidad de la Información” son aplicables a todos los empleados, docentes, contratistas, estudiantes (comunidad educativa), visitantes y proveedores que tiene acceso a los activos de información y de tecnología del Tecnológico de Antioquia, Institución Universitaria, incluidas las operaciones de recopilación, análisis, procesamiento, disponibilidad, custodia, conservación y recuperación de información.

DEFINICIONES

Activos Críticos de información: Sistema Administrativo y Financiero, Sistema Académico y sistema educación virtual (Moodle).

Activos críticos de tecnología: Centro de Datos institucional.

Activos de información: cualquier componente (Información Física, Información Digital, Software, y Servicios) que soporta uno o más procesos del Tecnológico de Antioquia, Institución Universitaria (Tecnológico de Antioquia, Institución Universitaria).

Activos de tecnología: Computadores de escritorio, portátiles, servidores y todo equipo que soporte la infraestructura tecnológica institucional (Firewall, Router, Switch, etc.).

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

Ciber amenaza o amenaza cibernética: aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

Ciberataque o ataque cibernético: acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de esta o donde el ciberespacio es fuente o herramienta de comisión de un crimen.

Ciberespacio: entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.

Ciberseguridad: Es el desarrollo de capacidades para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la Entidad.

Comunidad Educativa: Empleados, egresados, docentes, contratistas, estudiantes.

Confidencialidad: es la garantía de que la información no es divulgada a personas, Entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, 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.

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, incluyendo el uso o desarrollo de software.

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.

Evento de seguridad: ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

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 intención 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: ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Entidad.

integridad de los datos: se refiere a la información almacenada en cualquier tipo de base de datos que sea precisa, completa, consistente y confiable, sin importar cuánto tiempo se almacene o con qué frecuencia se acceda a ella.

Mesa de Servicio: Es el principal punto de contacto entre los usuarios y la Coordinación TIC para informar los incidentes relacionados con TI. Registra y monitorea el avance de la solución al incidente informado.

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.

LOG (Registro): es el registro de auditoría de las acciones y de los acontecimientos que ocurren en un sistema computacional cuando un usuario o proceso está activo y sucede un evento que está configurado para reportar. Rastro de lo que se está ejecutando sobre la plataforma tecnológica.

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.

Sistema de respaldo eléctrico: Unidad de potencia ininterrumpida (UPS), Planta de energía.

VPNs institucionales: Conexión remota desde el exterior de la institución a cualquier "activo de información" ubicado en las instalaciones del Tecnológico de Antioquia, Institución Universitaria.

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

ETAPAS DE CONSTRUCCIÓN DE LAS POLÍTICAS DE SEGURIDAD DIGITAL

Etapa	Actividad	Meta	Responsable
Etapa 1 - Planear	Conformar equipo de trabajo para la construcción de las Políticas	Equipo conformado: Seguridad TIC, Infraestructura TIC, apoyo grupo primario TIC.	Coordinador TIC
	Analizar el entorno y la normatividad vigente	Definición de factores externos políticos, económicos, sociales, tecnológicos y normatividad vigente que afecta la entidad.	Grupo Primario TIC
	Definir del alcance de las Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Definición del alcance de las Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Grupo Primario TIC
Etapa 2 - Hacer	Construir documento de Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Documento de Políticas de Seguridad Digital "Seguridad y Privacidad de la Información".	Seguridad TIC Infraestructura TIC
	Presentar el documento de Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Documento aprobado: Políticas de Seguridad Digital "Seguridad y Privacidad de la Información".	Coordinador TIC Comité de Informática
	Publicar las Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Políticas publicadas en la página WEB Institucional	Coordinador TIC Coordinador de Comunicaciones
	Socializar las Políticas de Seguridad Digital "Seguridad y Privacidad de la Información"	Políticas Socializadas	Seguridad TIC
	Definir Tratamiento de riesgos de seguridad de la información.	Documento Final del Plan de tratamiento de riesgos de seguridad y privacidad de la información (PRSI)	Seguridad TIC Infraestructura TIC
Etapa 3 - Verificar	Realizar auditorías internas	Hacer auditorías internas de políticas, controles y procedimientos establecidos en el Plan de Seguridad Digital "Seguridad y Privacidad de la Información"	Seguridad TIC
	Medir implementación del Plan de Seguridad Digital "Seguridad y Privacidad de la Información".	Definición de indicadores para medir el avance en de implementación del Plan de Seguridad Digital "Seguridad y Privacidad de la Información"	Seguridad TIC Infraestructura TIC
Etapa 4 - Actuar	Aplicación de acciones correctivas y de mejora.	Aplicar acciones correctivas y de mejora de la implementación del Plan de Seguridad Digital "Seguridad y Privacidad de la Información"	Coordinador TIC Seguridad TIC

MARCO NORMATIVO

El Tecnológico de Antioquia referencia las siguientes normas y modelos para la gestión de la seguridad y privacidad de la información, en la institución:

Norma	Año	Descripción
Políticas de Seguridad Digital - Seguridad y Privacidad de la Información v2	2023	Establece los lineamientos de seguridad digital que permitan garantizar la seguridad de los activos de información y de tecnología, garantizando la disponibilidad, integridad y confiabilidad de la información para el Tecnológico de Antioquia – Institución Universitaria.
PRSI - Plan de Tratamiento de Riesgos y Seguridad de la Información_Ver_2_2023	2022	Define una metodología para la implementación del Plan de Tratamiento del Riesgo de Seguridad y privacidad de la Información del Tecnológico de Antioquia, institución Universitaria, de ahora en adelante PRSI.
PETI 2022_2026_V3	2022	Optimiza los procesos Institucionales mediante la transformación digital, orientada al cumplimiento de los objetivos estratégicos del Tecnológico de Antioquia – Institución Universitaria, de acuerdo con los lineamientos del MIN TIC.
Plan de Desarrollo del Tecnológico de Antioquia 2022-2026 "Ser, Hacer, Trascender".	2022	Documento que provee los lineamientos estratégicos; objetivos de corto, mediano y largo plazo y las estrategias del Tecnológico de Antioquia Institución Universitaria, para el periodo 2022-2026, permitiendo de esta manera evaluar su gestión.
ISO 27001	2022	Estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información.
Decreto 767	2022	Por el cual se actualiza la Política Colombiana de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 746	2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No.500 de 2021 ("por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".).
CONPES 3975	2019	Formula una política nacional para la transformación digital e inteligencia artificial. Esta política tiene como objetivo potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y el sector privado, para impulsar la productividad y favorecer el bienestar de los ciudadanos, así como generar los habilitadores transversales para la transformación digital sectorial, de manera que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la Cuarta Revolución Industrial (4RI).
Manual de Gobierno Digital	2018	En este documento se desarrolla el proceso de implementación de la Política de Gobierno Digital a través de los siguientes cuatro (4) momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política; cada uno de ellos incorpora las acciones que permitirán desarrollar la Política en las entidades públicas de nivel nacional y territorial.
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 20del Decreto 1078 de 2015, Decreto Único Reglamentario del

Norma	Año	Descripción
		sector de Tecnologías de la Información y las Comunicaciones.
Ley 1915	1918	Sobre Derechos de Autor. Modifica la ley 23de 1982
Decreto 415	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
CONPES 3854	2016	Política Nacional de Seguridad Digital.
Modelo de Gestión IT4+, versión 02	2016	IT4+® es el modelo de gestión sobre el que se construyó la Estrategia TI para Colombia, el cual es un modelo resultado de la experiencia, de las mejores prácticas y lecciones aprendidas durante la implementación de la estrategia de gestión TIC en los últimos 12 años en las entidades del Estado colombiano. IT4+® es un modelo integral que está alineado con la estrategia empresarial u organizacional y permite desarrollar una gestión de TI que genere valor estratégico para la organización y sus clientes. Está conformado por los siguientes componentes: Estrategia de TI, Gobierno de TI, Análisis de información, Sistemas de Información, Gestión de servicios tecnológicos, Apropiación y uso.
Decreto 1078	2015	Por el cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el cual incluye el Decreto 2573 de 2014, el cual establece los lineamientos generales de la Estrategia de Gobierno en Línea.
Ley 1712	2014	Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.
Decreto 2573	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Directiva Presidencial 004	2012	Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública.
CONPES 3650	2010	Lineamientos sobre la Importancia de la Estrategia de Gobierno en Línea.
CONPES 3670	2010	Lineamientos de política para la continuidad de los Programas de Acceso y Servicio Universal a las Tecnologías de la Información y Comunicación.
Ley 1341	2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Decreto 1151	2008	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
ISO/IEC 27005	2008	Gestión de Riesgos en Seguridad de la Información.
Ley 527	1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

POLÍTICAS DE SEGURIDAD DIGITAL

El Tecnológico de Antioquia, Institución Universitaria, consiente de la importancia de preservar la seguridad de sus activos de tecnología y de información, define las Políticas de Seguridad Digital, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de TIC, buscando preservar la confidencialidad, integridad y disponibilidad de la información.

POLÍTICA DE LA ORGANIZACIÓN

La Política Establece un marco de referencia para iniciar, conocer e implementar la seguridad digital al interior del Tecnológico de Antioquia, Institución Universitaria, por medio de la definición de roles y responsabilidades de los miembros de la Comunidad Educativa (Empleados, docentes, contratistas, estudiantes) y proveedores, la separación de deberes, el contacto con las autoridades y la incorporación de la seguridad digital en todos los procesos Institucionales.

Alcance

- A. La Política es de aplicación obligatoria para toda Comunidad Educativa, cualquiera sea su calidad jurídica, el área a la cual pertenezca, el lugar (local o remoto) donde realice las actividades inherentes al cargo y cualquiera sea el nivel de las tareas que desempeñe, incluyendo a visitantes y proveedores.
- B. Definir y dar a conocer las Políticas de Seguridad Digital - "Seguridad y Privacidad de la Información" a todos los miembros de la Comunidad Educativa, visitantes y proveedores que tengan acceso a activos de información y de tecnología.
- C. Toda la Comunidad Educativa y proveedores, debe preservar la confidencialidad de la información y la no divulgación, que por razones de su cargo o responsabilidades designadas estén bajo su custodia, así mismo conocer y aceptar el tratamiento de datos personales conforme a las políticas institucionales y la ley.
- D. Toda la información que genere, procese, almacene, transfiera o transmita el Tecnológico de Antioquia, Institución Universitaria en medios físicos o digitales, en sus activos de información y de tecnología, es de su propiedad y solo puede ser utilizada para el cumplimiento de las funciones institucionales.
- E. Todos los miembros de la Comunidad Educativa, visitantes y proveedores que tengan acceso a "activos de información" son responsables de su uso y protección mientras estén en su custodia ya sea física o electrónica, de tal forma que se evite su modificación, pérdida y divulgación no autorizada, acorde a su valor, confidencialidad e importancia.
- F. El Comité de Informática Institucional será el responsable de garantizar que todos los proyectos de TIC que sean llevados a esa instancia cumplan con las Políticas de Seguridad Digital "Seguridad y Privacidad de la Información" y se incluyan los controles y análisis de riesgos inherentes a cada proyecto. Además de revisar y gestionar de ser necesario los Incidentes de Seguridad que se presentes en los sistemas de información, Servicios tecnológicos y en la infraestructura tecnológica de la Institución.

POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

La Política asegura que los miembros de la Comunidad Educativa conozcan, comprendan y tomen conciencia sobre las responsabilidades que tienen con la seguridad y privacidad de la información y cumplan con los lineamientos establecidos por la Institución, además

de asegurar que son idóneos en los roles asignados y que se protegen los intereses del Tecnológico de Antioquia, Institución Universitaria, como parte del proceso de vinculación, ejecución, cambio o terminación de ésta.

Alcance

- A. La Política aplica para toda la Comunidad Educativa, visitantes y proveedores y es de estricto cumplimiento.
- B. A toda la Comunidad Educativa se le debe dar a conocer las Políticas de Seguridad Digital y a los proveedores cuando por su relación con la Institución tengan acceso a cualquiera de los activos de información y/o de tecnología.
- C. Contar con un procedimiento de entrega de puesto de trabajo que incluya el control de activos de información y de tecnología a cargo de los miembros de la Comunidad Educativa y permita verificar su cumplimiento y entrega de inventario, al igual que garantizar el retiro de credenciales de acceso a los activos de información y de tecnología Institucionales.
- D. Todos los empleados y contratistas con asignación de equipos de cómputo al momento de dejar definitivamente el puesto de trabajo (cambio de funciones o retiro) deben dejar toda la información institucional en los equipos y no borrarla.
- E. Todos los miembros de la Comunidad Educativa y cuando sea pertinente los visitantes y/o proveedores, deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización para el desempeño de su labor.

POLÍTICA DE CONTINUIDAD

La Política de Continuidad está diseñada como instrumento para prevenir y/o reaccionar adecuadamente ante incidentes que pongan en riesgo el desarrollo de las actividades propias de su misión, permitiendo responder de manera eficiente ante una eventualidad, restablecer en el menor tiempo posible la prestación de sus servicios y mitigar el impacto. La Política debe ser revisada y actualizada por cada vigencia y debe tener en cuenta la incorporación de nuevos activos críticos de información y tecnología que la institución adquiera o desarrolle.

Alcance

- A. La Política aplica para todos los activos críticos de información y de tecnología que posee la Institución y es de estricto cumplimiento.
- B. La Coordinación TIC debe identificar para cada vigencia los activos críticos de información y tecnología.
- C. La Coordinación TIC debe contar con un Plan de tratamiento de Riesgos y Seguridad de la Información que permita identificar y tratar riesgos que afecten la continuidad de las operaciones, los cuales deben ser actualizados para cada vigencia.
- D. Todos los miembros de la Comunidad Educativa son responsables de informar a los líderes de procesos o a la Coordinación TIC de cualquier incidente que afecte la continuidad de procesos debido a fallas en los recursos tecnológicos, sistemas de información o cualquier servicio de tecnología.
- E. La Coordinación TIC debe mantener, promover y formular soluciones que permitan apoyar la continuidad de las operaciones tecnológicas de la Institución.



- F. La Coordinación TIC debe incluir en todos los contratos de tecnología, que involucren activos críticos de información y de tecnología, las condiciones que garanticen el servicio, incluyendo los tiempos máximos de recuperación y ventanas de mantenimiento, así mismo definir y exigir sistemas redundantes, donde aplique.
- G. La Coordinación TIC debe informar oportunamente a la Comunidad Educativa de cualquier ventana de mantenimiento programada o de cualquier falla en los activos críticos de información o de tecnología.
- H. La Coordinación TIC es responsable de diseñar y utilizar un formato para reportar incidencias de seguridad que afecten la continuidad de las operaciones de tecnología en la Institución.

POLÍTICA DE USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS

La Política da lineamientos del buen uso a los recursos Tecnológicos: correo electrónico, internet, redes sociales, activos de información y de tecnología, uso de software y acceso WIFI que provee el Tecnológico de Antioquia, Institución Universitaria a toda la Comunidad Educativa, invitados y proveedores en las sedes de la Institución.

Alcance

- A. Aplica para toda la Comunidad Educativa, invitados y proveedores que tienen acceso a los recursos: Servicios de correo electrónico, internet, redes sociales, activos de información y de tecnología, uso de software y WIFI.
- B. Se debe hacer seguimiento y adaptación del uso de los recursos tecnológicos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido de los sistemas.
- C. Todos los miembros de la Comunidad Educativa son responsables de la correcta utilización de los recursos, respetando las Políticas de Seguridad Digital, incluyendo la responsabilidad sobre contenidos en comunicaciones enviadas a través de mensajería y/o correo electrónico.
- D. Los mensajes que son dirigidos a toda la organización solo podrán ser enviados por las personas autorizadas para realizar envíos masivos.
- E. La Institución contará con un sistema de protección perimetral, que proteja la navegación y los mensajes de correo electrónico entrantes y salientes, contra malware, spam y otros medios de ataque a los activos de información y de tecnología.
- F. Todos los miembros de la Comunidad Educativa son responsables de utilizar solo herramientas proporcionadas por la Institución para el desarrollo de actividades donde se requiera apoyo de TI, como Microsoft 365 (Teams, Forms, Outlook, Onedrive, etc.). Queda prohibido el uso de herramientas TI que no sean autorizadas por la Coordinación TIC.
- G. Para garantizar la trazabilidad de la información institucional se deben utilizar cuentas genéricas para todos los procesos administrativos.
- H. Toda cuenta de correo electrónico que no se esté utilizando y no tenga un responsable activo debe ser deshabilitada.

- I. Los envíos masivos internos deben realizarse a través de listas de distribución institucionales o con copia oculta para evitar compartir la información de las cuentas destino.
- J. Los líderes de procesos o áreas serán los responsables de la asignación, modificación o bloqueo de cuentas genéricas institucionales de su dependencia, a través de los medios de gestión y control que la institución defina.
- K. Se prohíbe utilizar el servicio de internet, mensajería instantánea y correo electrónico para ver, compartir o distribuir temas relacionados con pornografía, delincuencia, armas, discriminación y cualquier tema que atente contra la dignidad humana.
- L. Utilizar siempre un lenguaje apropiado en sus comunicaciones atendiendo principios éticos de la comunicación electrónica de datos.
- M. Es responsabilidad de toda la Comunidad Educativa revisar y leer los correos institucionales, clasificarlos, priorizarlos y almacenarlos de acuerdo al proceso o actividad en las que participa y depurar para evitar que se llene el buzón.
- N. Está prohibida la suplantación, el enmascaramiento o la firma de otro usuario en el uso de cualquier recurso de información.
- O. Está prohibida la replicación de mensajes que son exclusivos para una persona en particular.
- P. Está prohibido enviar correo tipo SPAM, es decir "correo basura" o no deseado relacionado con falsos virus. con publicidad de empresas, cadenas de mensaje, pornografía y bromas.
- Q. Está prohibido utilizar el servicio de correo electrónico o mensajerías instantánea para realizar acoso, calumnias, burlas, sátiras, epígrafes, sarcasmos, ultrajes, amenazas con intención de intimidar, insultar o cualquier otra forma de actividad hostil para deshonorar a una persona o entidad.
- R. Está prohibido obtener copias intencionales de archivos, códigos o contraseñas o información ajena.
- S. Todos los responsables de cuentas de correo electrónico son responsables de su buen manejo, que incluye garantizar ambientes de uso adecuados. No usarlo para navegar en páginas no seguras, café internet o cualquier ambiente que no garantice seguridad para tus datos.
- T. En caso de detectar vulneración en su cuenta, generación de SPAM o cualquier uso indebido no autorizado por el propietario de la cuenta de correo electrónico, se debe proceder al cambio de contraseña por parte del usuario titular de la cuenta. En caso de que el sistema de correo Institucional detecte la vulneración, se procede a bloquear y/o resetear la contraseña para garantizar la seguridad de la información.
- U. Está prohibido usar la cuenta de correo electrónico para uso diferente al Institucional o usar la cuenta de otro usuario o entregar a un tercero la contraseña propia.
- V. Todas las cuentas de correo electrónico deben ser creadas en un único sistema definido por la institución que permita centralizar su gestión, cambio de contraseña y garantizar uniformidad y control. Queda prohibido crear cuentas en sitios diferentes al definido por la institución.

- W. La Coordinación TIC debe garantizar que la totalidad de las cuentas electrónicas tengan acceso a un sistema central donde el usuario pueda cambiar o recuperar la contraseña de sus cuentas de correo electrónico. No se pueden crear cuentas o permitir su uso si no cuentan con esta funcionalidad (cambio de contraseña por parte del usuario).

POLÍTICA DE GESTIÓN DE ACTIVOS DE TECNOLOGÍA Y DE INFORMACIÓN

La Política define las responsabilidades en el uso adecuado y protección tanto de sus activos de tecnología como de información, teniendo en cuenta su identificación y clasificación, lo que permite recibir un nivel apropiado de protección, de acuerdo con su importancia, y se efectúe un manejo adecuado para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de la información almacenada en ellos.

Alcance

- A. Aplica para toda la Comunidad Educativa, invitados y proveedores que tienen acceso a los activos de tecnología y/o información, los cuales deben ser utilizados para el desarrollo de las actividades propias de su cargo o rol dentro de la Institución, nunca para su beneficio personal o en detrimento de los objetivos institucionales.
- B. El Tecnológico de Antioquia, Institución Universitaria debe contar con un sistema de inventario de sus activos de tecnología, que permita la asignación o movimiento de inventario entre miembros de la Comunidad Educativa, garantizando la gestión y control de esos activos.
- C. Todos los activos de tecnología de la institución deben tener un ID (placa) para su fácil identificación y control.
- D. Todos los activos de tecnología deben estar inventariados y asignados a un funcionario de la institución.
- E. Los miembros de la Comunidad Educativa que tienen a cargo "activos de información" son responsables de su uso y protección mientras estén en su custodia ya sea física o electrónica.
- F. La Coordinación TIC es responsable de Administrar y custodiar los activos de tecnología y de información alojados en el Centro de Datos, así mismo de dar los lineamientos para la administración y gestión de todos los activos de información y tecnología que utiliza el Tecnológico de Antioquia, Institución Universitaria.
- G. Solo la Coordinación TIC, a través de su área de soporte, será la única autorizada para realizar movimientos de activos de tecnología.
- H. Es responsabilidad de todos los miembros de la Comunidad Educativa que tengan activos de tecnología a su cargo entregarlos en buen estado, cuando se presente retiro de la entidad, cambio de funciones o culminación del contrato según sea el caso.
- I. El sistema de inventario Institucional debe garantizar una información veraz y actualizada.

POLÍTICA DE CONTROL DE ACCESO

La Política define las directrices generales y de seguridad, lo mismo que la asignación de roles y perfiles para un acceso controlado tanto a los activos de información como de tecnología del Tecnológico de Antioquia, Institución Universitaria.



Alcance

- A. Aplica para toda la Comunidad Educativa, invitados y proveedores que tienen acceso a los activos de tecnología y/o información y carnet institucional.
- B. La Coordinación TIC es la encargada de suministrar a toda la Comunidad Educativa, invitados y proveedores las credenciales de acceso a los "activos de tecnología" que por su rol o función requieren de acceso, además de establecer que estas credenciales son de uso personal e intransferible.
- C. Cualquier acceso remoto solo se puede hacer a través de VPNs institucionales, autorizadas previamente por la Coordinación TIC.
- D. Todos los activos críticos de información institucionales deben tener ingreso controlado a través de credenciales y perfiles que restrinjan su manejo dentro del mismo sistema de información.
- E. Los líderes técnicos son los responsables de asignar los perfiles en cada sistema de información de acuerdo a los requerimientos del líder del área encargada del proceso respaldado por el sistema de información.
- F. La Coordinación TIC es la responsable de implementar los protocolos de seguridad en la infraestructura de red local, que permitan acceder a los recursos de manera segura.
- G. No está permitida la conexión a la red local (LAN) de equipos que no sean de propiedad del Tecnológico de Antioquia, Institución Universitaria. En caso de ser necesario, solo la Coordinación TIC estará facultada para realizar el proceso de verificación y autorización de conexión de manera temporal.
- H. Toda la Comunidad Educativa, proveedores y visitantes pueden acceder al servicio WIFI y son responsables de cumplir las Políticas de Seguridad Digital.

POLÍTICA DE SEGURIDAD PARA LA GESTIÓN DE CONTRASEÑAS

Define lineamientos con respecto al uso adecuado de contraseñas, sus características y manejo seguro, orientado a preservar la seguridad de los activos de información y de tecnología institucionales.

Alcance

- A. Aplica para toda la Comunidad Educativa, invitados y proveedores que tienen a su cargo credenciales para acceso a los activos de información y de tecnología de la institución.
- B. Las credenciales asignadas a cada miembro de la Comunidad Educativa son personales e intransferibles, al igual que el carnet institucional que se le asigne para el ingreso a las instalaciones del Tecnológico de Antioquia, Institución Universitaria. El mal uso que se dé a estas, es de exclusiva responsabilidad del usuario titular de las credenciales o carnet.
- C. Todos los sistemas de información críticos deben solicitar las credenciales de acceso (usuario y contraseña) para permitir el ingreso.
- D. Todos los activos de información al igual que los de tecnología que requieran ingreso de credenciales deben permitir el cambio de contraseña por parte del usuario.

- E. Toda la Comunidad Educativa con acceso a activos de información y de tecnología Institucionales es responsable de asegurar la privacidad de las contraseñas asignadas.
- F. Todos los miembros de la comunidad Educativa que utilicen activos de tecnología y/o información son responsables de bloquear el equipo en el momento en que se retiren a una zona donde pierda visibilidad y control de este.
- G. Toda contraseña segura debe cumplir con las siguientes características:
- 1) La longitud de la contraseña debe estar entre 8 y 12 caracteres.
 - 2) Las aplicaciones en las cuales la tecnología utilizada no contemple una longitud mínima de ocho caracteres, la longitud mínima deberá ser la máxima contemplado por el sistema.
 - 3) La contraseña como mínimo debe estar compuesta por una combinación de letras Mayúsculas, minúsculas y caracteres numéricos.
 - 4) No se deben utilizar palabras contenidas en el nombre de la cuenta o del titular de la cuenta.
 - 5) Se debe evitar utilizar secuencias básicas de teclado (por ejemplo: "qwerty", "asdf" o las típicas en numeración: "1234" ó "98765")
 - 6) No repetir los mismos caracteres en la misma contraseña. (ej.: "111222").
 - 7) No enviar nunca la contraseña por correo electrónico o en un mensaje de texto. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
 - 8) No deben usarse palabras o nombres comunes que aparezcan en los diccionarios.
 - 9) No debe haber una relación obvia con el usuario, sus familiares, nombre de la entidad, abreviaciones relacionadas a la entidad, ciudad, país, año, fecha de nacimiento, el grupo de trabajo u otras asociaciones parecidas, ya que pueden ser identificadas de manera fácil a través de un ataque de ingeniería social.
 - 10) Si hay indicios para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
 - 11) No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que sea posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores, esto se debe gestionar desde el sistema que asigne las credenciales.
 - 12) Cada sistema debe establecer los mecanismos para que la contraseña asignada al usuario le sea transmitida de la manera más confidencial posible.
 - 13) No se debe escribir la contraseña en papeles y dejarla en sitios donde pueda ser encontrada por terceros.
 - 14) No se debe almacenar la contraseña en la computadora en texto plano. Algunos cuadros de diálogo o ventanas emergentes de los navegadores presentan una opción para guardar o recordar la contraseña; no debe seleccionarse esa opción.
 - 15) Las aplicaciones deben almacenar las contraseñas en forma cifrada.
 - 16) Las contraseñas predefinidas que traen los equipos y aplicaciones, deben cambiarse inmediatamente al ponerse en operación.
 - 17) Cuando el titular de la cuenta se retira o cambia de función, las credenciales deben ser actualizadas con la nueva información de responsable y obligar el cambio de contraseña o en su defecto desactivar la cuenta.

POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Los lineamientos establecidos buscan minimizar los riesgos de daños e interferencias a los activos de información y de tecnología del Tecnológico de Antioquia, Institución Universitaria, evitando accesos físicos, tanto internos como externos no autorizados.

Alcance

- A. Aplica para toda la Comunidad Educativa, invitados y proveedores que tienen acceso a las instalaciones del Tecnológico de Antioquia, Institución Universitaria.
- B. El acceso al Centro de Datos de la Institución está a cargo de la Coordinación TIC, la cual es la responsable de enrolar, asignar tarjetas de acceso y dar los permisos de acceso según el caso, con el fin de garantizar la seguridad de los activos de información y de tecnología alojados en éste.
- C. La Dirección Administrativa y Financiera, a través del profesional de Servicios Generales en conjunto con la Coordinación TIC, son los responsables establecer los mecanismos de custodia de las imágenes y videos, así como los tiempos de retención de dicha información del sistema de CCTV.
- D. Se debe realizar control de ingreso y retiro de las instalaciones del Tecnológico de Antioquia, Institución Universitaria de activos de tecnología y realizar registro de cada movimiento de acuerdo a las directrices y formatos entregados por el profesional de Compras y Almacén adscrito a la Dirección Administrativa y Financiera.
- E. Los puntos de acceso a la institución y las zonas comunes deben ser controladas y monitoreadas mediante CCTV.
- F. El ingreso y salida de todos los miembros de la comunidad Educativa, visitantes y proveedores, deben cumplir con los controles implementados y registrados de ser necesario.

POLÍTICA DE SEGURIDAD DE LAS OPERACIONES Y COMUNICACIONES

La Política establece lineamientos para fortalecer la protección de los activos de información y de tecnología y el uso correcto de software legal, derechos de autor y respaldo de la información.

Alcance

- A. Esta política aplica para todos los activos de información y de tecnología, utilizados en el Tecnológico de Antioquia, Institución Universitaria.
- B. La Coordinación TIC debe controlar que no se instale software sin licencia o sin la debida autorización institucional.
- C. No se deben compartir carpetas, discos duros a través de la red con todos los usuarios. Se debe restringir el acceso solo a los interesados.
- D. Todos los miembros de la Comunidad Educativa son responsables de utilizar software legal y utilizar solo "activos de información" autorizados por el Tecnológico de Antioquia, Institución Universitaria.
- E. Toda la Comunidad Educativa, invitados y proveedores que tenga acceso a los recursos de tecnología y/o de información y que manipule información Institucional local, tiene la responsabilidad de realizar copias de seguridad de forma periódica, utilizando medios Institucionales como OneDrive o discos externos. La periodicidad será definida por el usuario dependiendo de la cantidad de cambios que realice sobre ella.

- F. Todo sistema de información deberá tener copias de seguridad diarias y almacenar las 3 últimas mensuales, Garantizando seguridad y recuperación ante desastres.
- G. Se debe realizar periódicamente, el mantenimiento preventivo y correctivo de los equipos alojados en el Centro de Datos: servidores, aire acondicionado, sistema de control de incendios, sistema de alimentación ininterrumpida –UPS, etc.
- H. La Coordinación TIC debe administrar el Centro de Datos, licenciamiento de software y provisión de la infraestructura tecnológica alojada en el Centro de Datos para el adecuado funcionamiento de los servicios de información.
- I. La Coordinación TIC debe disponer en todo momento para el Centro de Datos de un sistema de control de acceso, sistema de control de temperatura y humedad, un sistema de detección y extinción de incendios y un sistema de alimentación eléctrica adicional como UPS y planta de energía.
- J. La Coordinación TIC establece mecanismos para monitorear, diagnosticar y resolver problemas de disponibilidad y rendimiento de la infraestructura tecnológica.
- K. La Coordinación TIC es la encargada de administrar la infraestructura de red y proporcionar la configuración necesaria para el cumplimiento de las funciones y/ actividades de cada área.
- L. La Coordinación TIC contará con mecanismos de seguridad para la protección ante amenazas y permita controlar el tráfico de entrada y de salida de la red LAN-WAN, lo mismo que utilizar segmentación que mejore la seguridad, control del tráfico y optimización del rendimiento de red.
- M. Se dispondrá de herramientas de seguridad antimalware y antispam debidamente licenciadas, que minimizan el riesgo de contagio de software malicioso.
- N. Todos los equipos de cómputo deben tener un Sistema antimalware instalado y licenciado. En caso de sospecha de infección de algún equipo de cómputo, el usuario debe informar a la Coordinación TIC, de acuerdo al procedimiento establecido.
- O. Todos los puntos de acceso (puntos de red) a la red LAN que no estén siendo utilizados deben ser bloqueados, así mismo está prohibido el uso de cualquier equipo de red que no sea institucional o autorizado por la Coordinación TIC.
- P. Al finalizar la vida útil o determinar que ya no son necesarios para las labores institucionales, los medios de almacenamiento de equipos de cómputo, medios de almacenamiento extraíbles, discos externos u otros medios que puedan contener información institucional, deben ser sometidos a borrado que impida su recuperación de información. En caso de imposibilidad tecnológica de aplicar un borrado, los medios deben ser sometidos a destrucción siguiendo los lineamientos sobre manejo de residuos electrónicos institucionales.

POLÍTICAS DE SEGURIDAD PARA LA RELACIÓN CON LOS PROVEEDORES DE SERVICIOS TECNOLÓGICOS

Se establecen lineamientos para el manejo de la relación con proveedores que administren información o servicios tecnológicos institucionales que aseguren la portabilidad de datos, confidencialidad y no revelación, ventanas de mantenimiento, manejo de incidentes y cualquier otro acuerdo contemplado para garantizar la confidencialidad, integridad y disponibilidad de la información y la seguridad de los servicios adquiridos.

Alcance

- A. Esta Política aplica para todos los procesos, sistemas de información y servicios contratados con proveedores externos de tecnología.
- B. Supresión, devolución o destrucción de datos al final del contrato o a petición del Tecnológico de Antioquia, Institución Universitaria ("Portabilidad de datos"); Después de la terminación de los Servicios, el proveedor dispondrá en el menor tiempo posible los Datos del Tecnológico de Antioquia existentes en el Entorno de producción, disponibles para la exportación vía archivos planos y entregará una copia en el formato de la Base de datos utilizada en producción. Después de la devolución de la totalidad de los datos, el proveedor eliminará de forma inmediata o de otro modo, inhabilitará todos los accesos y las copias de los Datos del Entorno de Producción y cualquier otro entorno perteneciente al Tecnológico de Antioquia.
- C. Confidencialidad de datos y no revelación: el proveedor deberá mantener la confidencialidad sobre toda la información del Tecnológico de Antioquia, Institución Universitaria, que pueda conocer durante el desarrollo del contrato y no utilizará la información para la presentación de su producto en otras organizaciones. La propiedad, titularidad y reserva de los datos e información almacenada en los repositorios de datos que sean generados y/o utilizados por el proveedor para el cumplimiento de las funciones contractuales pactadas, pertenecen de forma exclusiva al Tecnológico de Antioquia, Institución Universitaria. El proveedor se compromete a respetarla, reservarla, no copiarla y a guardar absoluta reserva sobre toda la información que conozca por su actividad, que le sea dada a conocer por el Tecnológico de Antioquia, Institución Universitaria con ocasión del desarrollo del objeto del contrato. El proveedor se obliga a devolver de inmediato al Tecnológico de Antioquia, Institución Universitaria, toda la información facilitada para la prestación del servicio, en la medida en que ya no resulte necesaria en la ejecución del mismo; absteniéndose de mantener copia parcial o total de la información y documentos obtenidos o generados con ocasión de la relación contractual al vencimiento del plazo.
- D. Requerimientos de autoridad: Salvo que la ley lo requiera de otro modo, el proveedor notificará en el menor tiempo posible al Tecnológico de Antioquia sobre cualquier orden judicial, administrativa o arbitral de un organismo competente que reciba y que se refiera a los Datos que el Tecnológico de Antioquia haya almacenado. El proveedor proporcionará al Tecnológico de Antioquia información que este en su poder para que este pueda responder a los requerimientos de manera oportuna.
- E. Propiedad Intelectual: El Tecnológico de Antioquia, Institución Universitaria conserva todos los derechos de propiedad intelectual sobre los Datos que se almacenan o procesan en los sistemas de información.
- F. Contenido y Protección: el proveedor de servicios en la nube o en lugares externos a la institución, deberá adoptar controles y prácticas de seguridad para los servicios, diseñados para proteger la integridad, confidencialidad y disponibilidad de su contenido, incluyendo Integridad de los datos, Control de acceso, bloqueo y detección de Ransomware, antimalware, copias de seguridad y recuperación ante desastres. Sin embargo, El Tecnológico de Antioquia es responsable de la seguridad de los dispositivos utilizados por la Institución para el acceso al servicio, y evitar posibles vulnerabilidades, tales como virus y software malicioso (malware), troyanos (Trojan horses), gusanos (worms) u otras rutinas de programación presentes en las estaciones de trabajo antes de operar la información almacenada; al igual que el uso indebido que se dé a la misma.

- G. Ventanas de mantenimiento o indisponibilidad del servicio: El proveedor debe Planear e informar con antelación (Mínimo 48 horas antes) cualquier cambio, ventana de mantenimiento, actualización o mejora en la infraestructura, software o cualquier componente del servicio y este debe ser concertado y aprobado por la Coordinación TIC del Tecnológico de Antioquia, Institución Universitaria antes de ser ejecutado.
- H. Control de Acceso: La Coordinación TIC deberá documentar y definir controles, perfiles y roles a los proveedores que requieran tener acceso a la información por medio de la infraestructura tecnológica de la institución. Así mismo todo nuevo desarrollo debe permitir el control de acceso a los sistemas de información a través del Directorio Activo Institucional (LDAP).
- I. Comunicaciones: La Coordinación TIC debe establecer comunicación con los proveedores exclusivamente por los canales institucionales dispuesto para dicha actividad y velar que las condiciones de comunicaciones sean seguras y por medios autorizados en el marco del respeto.
- J. Manejo de incidentes: Analizar en conjunto con los proveedores incidentes siempre y cuando sean de un grado que afecten ambas partes con el fin de establecer las posibles causas de este incidente, para posteriormente identificar el impacto y ejecutar las acciones pertinentes para remediar o contener el incidente.
- K. Niveles de Servicio y Operación: Todos los contratos de tecnología que requieran establecer niveles de servicio y/o, como sistemas de información o de servicio, deben incluir explícitamente los niveles de servicio y de operación en los contratos.
- L. La Coordinación TIC debe verificar periódicamente el cumplimiento efectivo de los acuerdos de niveles de servicios establecidos con los proveedores.

POLÍTICA DE SEGURIDAD PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La Política establece lineamientos sobre la adquisición, desarrollo y mantenimiento de sistemas de información y establece la seguridad como parte integral de los sistemas de información durante todo el ciclo de vida.

Alcance

- A. Esta Política aplica para toda adquisición, desarrollo y mantenimiento de sistemas de información que el Tecnológico de Antioquia, Institución Universitaria requiera para su operación.
- B. La Coordinación TIC acompañada de los líderes funcionales de los sistemas de información son responsables de dar cumplimiento a los estándares de seguridad establecidos en las Políticas de Seguridad Digital.
- C. La Coordinación TIC establece los lineamientos de seguridad de la infraestructura tecnológica, que garantice el cumplimiento de los controles y la salvaguarda de la información de manera segura.
- D. La Coordinación TIC, acompañada de la "Unidad de Virtualidad y Desarrollo" adoptarán el enfoque de seguridad en los procesos de desarrollo de tecnología que se adelantan, sobre todo en las infraestructuras críticas.
- E. Todos los sistemas de información, aplicaciones y portales del Tecnológico de Antioquia, Institución Universitaria, adquiridos o desarrollados no deben permitir la

modificación de parámetros a nivel de sistema operativo y software. Así mismo, se debe garantizar que no se visualicen en pantalla ni se almacene en base de datos las contraseñas con cadenas de conexión e información en texto plano.

- F. Los sistemas de información, aplicaciones y portales del Tecnológico de Antioquia, Institución Universitaria deben garantizar que la información establecida como reservada, cuente con mecanismos seguridad necesarios que eviten su alteración o borrado por personal no autorizado.
- G. Todos Los desarrollos Internos y Externos deben acogerse a las Políticas de Seguridad Digital de la Institución, incluyendo el cumplimiento de Derechos de autor y software legal.
- H. La Unidad de Virtualidad y Desarrollo de la Institución debe definir todos los requerimientos técnicos y funcionales para nuevos desarrollos, incluyendo pruebas, documentación, soporte y garantía del producto final.
- I. La Unidad de Virtualidad y Desarrollo debe acompañar las pruebas funcionales para el recibo a satisfacción para paso a producción. El recibo a satisfacción debe quedar documentado.
- J. La Coordinación TIC con apoyo de la Unidad de Virtualidad y Desarrollo es la encargada de aprobar las migraciones a producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.
- K. Se deben Realizar pruebas para asegurar que se cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, documentado las pruebas realizadas y aprobando los pasos a producción.
- L. Definir el servicio y los acuerdos de niveles de servicio para la atención de incidencias y peticiones a nivel funcional.
- M. Todo portal o micro sitio debe estar incorporado a la página principal Institucional (www.tdea.edu.co). No se admiten portales o micro sitios independientes o sueltos del Portal principal.

POLÍTICA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Política establece los lineamientos que se deben adoptar en el tratamiento de incidentes de seguridad que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información y/o de tecnología y los responsables del reporte y tratamiento.

Alcance

- A. Esta Política aplica y es de estricto cumplimiento para todos los miembros de la Comunidad Educativa y proveedores, son responsables de informar a través del servicio de "Mesa de Servicio", cualquier incidente de seguridad que se pueda presentar, tales como: uso indebido, alteración, divulgación no autorizada, acceso indebido a activos de información y de tecnología, entre otros.
- B. Promover entre la Comunidad Educativa la importancia de reportar los incidentes de seguridad, los procedimientos y medios para realizarlo.
- C. La Coordinación TIC evaluará como incidentes de seguridad de la información, eventos asociados a: incumplimiento de las Políticas de Seguridad Digital - "Seguridad y Privacidad de la Información" y los que correspondan a delitos

informáticos calificados como tales por la normatividad vigente y los eventos que materialicen riesgos de seguridad digital.

- D. La Coordinación TIC es la encargada de realizar la trazabilidad de los incidentes detectados o reportados, establecer posibles causas, implementar medidas correctivas y proponer planes de mejora.
- E. La Coordinación TIC realizará seguimiento de cumplimiento de Políticas a través de indicadores que anualmente se deben revisar para su actualización de acuerdo a las necesidades de seguridad Digital.
- F. La Coordinación TIC debe socializar y utilizar el formato definido para informes de incidentes y tratamiento de riesgos TIC.