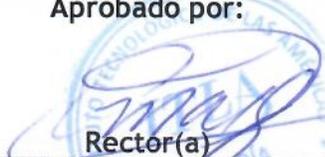




INSTITUTO TECNOLÓGICO DE LAS AMÉRICAS
Departamento de Tecnología de la Información
y
Comunicaciones

Manual de Políticas de Seguridad de la Información

Código documental: MC-TI-01	Versión: 1	Fecha de actualización (dd-mm-aa): 01-nov-2021	Tipo de proceso: Procesos de Soporte o Apoyo
Preparado por:  Director(a) de TIC's	Revisado por:  Encargado(a) de Calidad en la Gestión	Aprobado por:  Rector(a)	



Manual de Políticas de Seguridad de la Información

ITLA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

INFORMACION GENERAL SOBRE EL MANUAL

Contenido

HISTORIA	5
FILOSOFIA INSTITUCIONAL	5
MISION:.....	5
VISION:	5
VALORES INSTITUCIONALES:.....	5
INTRODUCCIÓN.....	6
OBJETIVOS	6
ALCANCE	6
RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL	8
CAPÍTULO I. POLÍTICAS GENERALES PARA USUARIOS DE LOS ACTIVOS DE INFORMACIÓN:.....	9
1.1. POLÍTICA DE RESPONSABILIDAD DE LOS EMPLEADOS RESPECTO AL CONTROL DE ACCESO A LOS SISTEMAS.....	9
1.2. POLÍTICA DE ACCESO REMOTO A LA RED.....	10
1.3. POLÍTICA DE CONFIDENCIALIDAD EN EL ÁREA DE TRABAJO.....	11
1.4. POLÍTICA DE RETIRO DE LOS EQUIPOS FUERA DE LAS INSTALACIONES DE LA EMPRESA.	12
1.5. POLÍTICA DE USO DEL CORREO ELECTRÓNICO Y LOS RECURSOS INFORMÁTICOS.	13
1.6. POLITICA DE USO ADECUADO DEL INTERNET.	15
1.7. POLITICA DE ENVÍO DE INFORMACIÓN A TERCEROS.	16
1.8. POLÍTICAS DE DETECCIÓN Y RESPUESTA A INCIDENTES:	18
1.8.1. POLÍTICA DE REPORTE DE BRECHAS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN.	18
1.8.2. POLÍTICA DE RESPALDO DE DATOS EN ESTACIONES DE TRABAJO CLASIFICADAS COMO CRÍTICAS (INCLUYENDO EQUIPOS PORTÁTILES).	20
1.8.3. POLÍTICA DE ACCESO DE TERCEROS A INFORMACIÓN CONFIDENCIAL.	21
CAPÍTULO II. POLÍTICAS PARA EL PERSONAL GERENCIAL Y/O SUPERVISOR:	22
2.1. POLÍTICA DE MANTENIMIENTO DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN DE CLIENTES.	22

2.2. POLÍTICA DE DISTRIBUCIÓN Y DIVULGACIÓN DE INFORMACIÓN.	24
2.3. POLÍTICA PARA LA CONTRATACIÓN DE PERSONAL FIJO O TEMPORAL.	25
2.4. POLÍTICA PARA LA CONTRATACIÓN DE PROVEEDORES EXTERNOS.	26
2.5. POLÍTICA PARA EL USO DE ACUERDOS DE CONFIDENCIALIDAD (PERSONAL Y TERCEROS).	27
2.6. POLÍTICA PARA LA SEGURIDAD DE LA GESTIÓN DE PROYECTOS.	29
2.7. POLÍTICA DE DISTRIBUCIÓN DE PROGRAMAS DE INDUCCIÓN AL PERSONAL.	30
CAPÍTULO III. POLÍTICAS PARA EL PERSONAL TÉCNICO:	31
3.1. POLÍTICA PARA LA INSTALACIÓN DE NUEVOS EQUIPOS DE CÓMPUTO.	31
3.2. POLÍTICA PARA LA ADMINISTRACIÓN DEL CONTROL DE ACCESO.	32
3.3. POLÍTICA PARA EL CONTROL DE ACCESO AL SOFTWARE DE SISTEMAS OPERATIVOS.	33
3.4. POLÍTICA DE CREACIÓN DE ACCESOS PARA EL USO DE INTERNET.	34
3.6. POLÍTICA DE REVISIÓN DE REGISTROS DE AUDITORIA (LOGS).....	35
3.7. POLÍTICAS RELACIONADAS AL MANTENIMIENTO DE HARDWARE Y SOFTWARE:	37
3.7.1. POLÍTICA PARA LA APLICACIÓN DE ACTUALIZACIONES AL SOFTWARE.	37
3.7.2. POLÍTICA PARA LA INSTALACIÓN DE HERRAMIENTAS DE OFIMÁTICA.	38
3.7.3. POLÍTICA PARA LA IMPLEMENTACIÓN DE ANTIVIRUS CORPORATIVO.	39
3.8. POLÍTICAS DE DETECCIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:	40
3.8.1. POLÍTICA DE INVESTIGACIÓN DE LA CAUSA Y EL IMPACTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	40
3.8.2. POLÍTICA DE DEFENSA CONTRA ATAQUES INTERNOS O EXTERNOS.....	41
3.8.3. POLÍTICA PARA ASEGURAR LA INTEGRIDAD EN LAS INVESTIGACIONES SOBRE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	43
3.9. POLÍTICAS DE RECUPERACIÓN Y RESTAURACIÓN DE OPERACIONES Y FUNCIONES CRÍTICAS:	44
3.9.1. POLÍTICA PARA LA RECUPERACIÓN DE SISTEMAS EN CASO DE FALLAS.....	44
3.9.2. POLÍTICA PARA EL ALMACENAMIENTO DE LA INFORMACIÓN DE RESPALDO	46
3.9.3. POLÍTICA PARA ESTABLECER UN PLAN DE SEGURIDAD DE LA INFORMACIÓN Y LOS ACTIVOS TECNOLÓGICOS PARA LA RECUPERACIÓN Y CONTINUIDAD DE LA OPERACION EN CASO DE DESASTRES.	48
3.10. POLÍTICAS DE AUDITORIA Y MONITOREO DE LA SEGURIDAD.....	50
3.10.1 POLÍTICA DE AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN Y ANÁLISIS DE VULNERABILIDAD Y RIESGO.	50

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.10.2. POLÍTICA DE MONITOREO DE SEGURIDAD DE LA INFORMACIÓN.....	52
3.10.3. POLÍTICA DE MONITOREO DE LA PLATAFORMA TECNOLÓGICA (DISPOSITIVOS DE RED, SERVIDORES, BASES DE DATOS Y DISPOSITIVOS DE SEGURIDAD).....	53
3.11. POLÍTICAS PARA EL CONTROL DE ACCESO A INFORMACIÓN Y SISTEMAS:.....	54
3.11.1. POLÍTICA PARA LA ADMINISTRACIÓN DEL ACCESO A USUARIOS.....	54
4.0 POLÍTICA DE USO ACEPTABLE DE LOS RECURSOS DE INFORMACIÓN.....	55
5.0 NORMAS APLICABLES AL USO DE COMPUTADORAS O ESTACIONES DE TRABAJO.....	56
6.0 NORMAS GENERALES APLICABLES AL USO DE LOS SISTEMAS DE INFORMACIÓN.....	56
7.0 NORMAS APLICABLES AL USO DE INTERNET.....	57
8.0 NORMAS APLICABLES AL USO DEL CORREO ELECTRÓNICO.....	57
9.0 DIVULGACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.....	58
10.0 INFORME DE INCUMPLIMIENTOS O INFRACCIONES.....	59
GLOSARIO.....	59

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

HISTORIA

El Instituto Tecnológico de Las Américas (ITLA) es una institución técnica de estudios superiores, fundada en el año 2000 por el Estado dominicano mediante decreto no. 1296-00, de fecha 15 de diciembre del 2000, modificado por el Decreto Núm. 240-08 de fecha 14 de junio del 2008. Única especializada en educación tecnológica en la República Dominicana.

Comprometidos con la calidad ITLA obtuvo en julio de 2006 la certificación ISO 9001:2000, para así satisfacer las necesidades y expectativas de sus usuarios a través de la mejora continua de los procesos educativos y soluciones de alta tecnología.

FILOSOFIA INSTITUCIONAL

MISSION:

Formar profesionales en alta tecnología promoviendo la educación especializada, sustentada en la innovación y el emprendimiento, contribuyendo al desarrollo de los sectores productivos de la nación.

VISION:

Ser referente de educación especializada en alta tecnología con egresados destacados emprendedores en innovación, soluciones tecnológicas efectivas y altos estándares de calidad a nivel nacional e internacional.

VALORES INSTITUCIONALES:

- Ética
- Responsabilidad
- Transparencia
- Integridad
- Compromiso
- Lealtad
- Honestidad

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

INTRODUCCIÓN

El presente documento constituye el Manual de Políticas de Seguridad de la Información para el Instituto Tecnológico de las Américas (ITLA), el cual fue visto, analizado y aceptado en su contenido por el Consejo Académico y todos los miembros de la organización.

OBJETIVOS

El Manual de Políticas de Seguridad de la Información del Instituto Tecnológico de las Américas (ITLA) tiene por finalidad dar a conocer los lineamientos de seguridad para el resguardo de los activos de información y de la infraestructura tecnológica que soporta las operaciones de (ITLA), a fin de aplicar y dar cumplimiento a las normas y leyes estipuladas que rigen la materia, emplear las mejores prácticas y los marcos referenciales como fundamento para la Gestión de la Seguridad de la Información de la empresa.

ALCANCE

Este manual debe emplearse para servir de dirección en la protección de los activos de información de la empresa. Las políticas aquí enmarcadas, deben ser cumplidas por todos los empleados y terceros relacionados que acceden a la información del Instituto Tecnológico de las Américas (ITLA).

Este manual está basado en las **NORMAS ISO** vigentes al 2018 en el Instituto Nacional de Normalización (INN), para Ciberseguridad. En especial enfoque con la **NCh-ISO27002:2013**, de igual forma se extiende los conceptos a las siguientes normas:

- **NCh-ISO27000:2014:** Sistemas de gestión de seguridad de la información - Visión general y vocabulario.
- **NCh-ISO27001:2013:** Sistemas de gestión de la seguridad de la información - Requisitos.
- **NCh-ISO27002:2013:** Código de prácticas para los controles de seguridad de la información.
- **NCh-ISO27003:2014:** Guía de implementación del sistema de gestión de seguridad de la información.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- **NCh-ISO27005:2014:** Gestión del riesgo de seguridad de la información.
- **NCh-ISO27013:2013:** Orientación sobre la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.
- **NCh-ISO27014:2015:** Gobernanza de seguridad de la información.
- **NCh-ISO27018:2015:** Código de práctica para la protección de la información personal de identificación (PII) en nubes públicas que desempeñen el rol de procesadores de PII.
- **NCh-ISO27031:2015:** Directrices para la preparación de las tecnologías de la informática y comunicaciones para la continuidad del negocio.
- **NCh-ISO27032:2015:** Directrices para la ciber protección.
- **NCh-ISO27036/1:2015:** Seguridad de la información en las relaciones con los proveedores
Parte 1: Visión general y conceptos.
- **NCh-ISO27036/2:2015:** Seguridad de la información para las relaciones con proveedores - Parte 2: Requisitos.
- **NCh-ISO27036/3:2015:** Seguridad de la información para las relaciones con proveedores - Parte 3: Directrices para la seguridad en la cadena de suministro de las tecnologías de la información y la comunicación.
- **NCh-ISO27040:2015:** Seguridad de almacenamiento.
- **NCh-ISO27003:2014:** Guía de implementación del sistema de gestión de seguridad de la información.
- **NCh-ISO27005:2014:** Gestión del riesgo de seguridad de la información.
- **NCh-ISO27031:2015:** Directrices para la preparación de las tecnologías de la informática y comunicaciones para la continuidad del negocio.
- **NCh-ISO27037:2015:** Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

RESPONSABILIDAD Y CUMPLIMIENTO DEL MANUAL

La Alta Gerencia del Instituto Tecnológico de las Américas (ITLA) es responsable de apoyar el proceso de implementación de las Políticas de Seguridad de la Información y asignar los recursos necesarios para su cumplimiento.

La Gerencia de Seguridad de la Información es responsable del apoyo ante todas las Gerencias del Instituto Tecnológico de las Américas (ITLA) durante el proceso de revisión y asesoría de cualquier actividad o asunto relacionado a la Seguridad de la Información.

La Gerencia de Seguridad de la Información es responsable de supervisar la implementación de las Políticas de Seguridad de la Información, velar porque el personal a su cargo les dé cumplimiento y apoyar a la Gerencia de Tecnología cuando se requiera.

La Gerencia de Seguridad de la Información es responsable de verificar periódicamente el cumplimiento de las Políticas de Seguridad de la Información.

La Gerencia de Tecnología es responsable de la implementación y administración de los controles técnicos aplicables a las Políticas de Seguridad de la Información.

Es responsabilidad de los supervisores de las distintas unidades administrativas, dar a conocer el contenido del presente manual entre los empleados bajo su supervisión, así como exigirles su firma en señal de haberse efectuado la lectura y entendimiento correspondiente.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

CAPÍTULO I. POLÍTICAS GENERALES PARA USUARIOS DE LOS ACTIVOS DE INFORMACIÓN:

1.1. POLÍTICA DE RESPONSABILIDAD DE LOS EMPLEADOS RESPECTO AL CONTROL DE ACCESO A LOS SISTEMAS.

Declaración de la Política:

Todo empleado al que se le otorgue un código de usuario (o login), con su respectiva contraseña, o cualquier otra forma de acceso autorizado, es responsable de su uso y protección, estos son únicos e intransferibles.

Objetivo:

Establecer la responsabilidad de los empleados del Instituto Tecnológico de las Américas (ITLA). respecto al uso y protección de los códigos de usuarios/contraseñas y otros modos de autenticación asignadas para acceder a los sistemas y aplicaciones de la Empresa.

Criterios para la implementación de la política:

- Concientizar la no divulgación de las credenciales de conexión a los diferentes sistemas de la Empresa por parte de los empleados del Instituto Tecnológico de las Américas (ITLA).
- Sólo está permitido el uso de ID´s genéricos cuando existen otros controles establecidos (por ejemplo, usuarios de conexión a sistemas, usuarios de mayor privilegio, entre otros).

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todo el personal del Instituto Tecnológico de las Américas (ITLA), que haga uso de sistemas de información y equipos que requieran contraseñas y otros modos de autenticación para su acceso.

Responsabilidades:

- Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA). deben asegurar que el personal bajo su cargo conozca y le dé cumplimiento a esta política.
- Todos los empleados del Instituto Tecnológico de las Américas (ITLA) deben dar cumplimiento a esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.2. POLÍTICA DE ACCESO REMOTO A LA RED.

Declaración de la Política:

El acceso remoto a la red y a los recursos de la empresa será permitido sólo cuando los usuarios autorizados son autenticados, la información viaje encriptada a través de la red y los privilegios sobre la misma sean restringidos.

Objetivo:

Proporcionar medios de acceso seguros desde y hacia fuentes externas acordes con el valor de la información que estará expuesta a través de la red. Utilizando medios seguros, tales como la Red Privada Virtual o Virtual Private Network, el cual proporciona el acceso a través de las redes públicas.

Criterios para la implementación de la política:

- Asegurar el acceso a la red interna del Instituto Tecnológico de las Américas (ITLA) al personal autorizado y autenticado por los mecanismos de control.
- Asegurar la confidencialidad de los datos e información transmitidos entre los usuarios remotos y la red interna a través de técnicas de cifrado.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a los usuarios que reciben autorización para tener acceso remoto a la red del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), deben asegurar que el personal bajo su cargo, que reciba autorización de acceso remoto a la red de la empresa, conozca y le dé cumplimiento a esta política.
- Todo usuario que tenga asignado un equipo de computación tiene responsabilidad directa en el cumplimiento de las políticas de seguridad.
- Es Responsabilidad de la Gerencia de Tecnología de la Información proporcionar canales de comunicación seguros.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.3. POLÍTICA DE CONFIDENCIALIDAD EN EL ÁREA DE TRABAJO.

Declaración de la Política:

Toda la información y los activos necesarios para el procesamiento de los datos del Instituto Tecnológico de las Américas (ITLA) deben pertenecer a un área dentro de la empresa y se debe garantizar la confidencialidad de los mismos por parte de los integrantes de cada Gerencia.

Objetivo:

Establecer el derecho a cada Gerencia del Instituto Tecnológico de las Américas (ITLA) gestionar la información y los accesos a la misma por parte del resto de las áreas de la empresa y terceros.

Criterios para la implementación de la política:

- Los empleados deben cumplir los criterios de confidencialidad de la empresa.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los empleados del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- La Gerencia de Tecnología de la Información debe implementar los medios idóneos para el cumplimiento de esta Política.
- Todos los empleados del Instituto Tecnológico de las Américas (ITLA) deben dar cumplimiento a esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.4. POLÍTICA DE RETIRO DE LOS EQUIPOS FUERA DE LAS INSTALACIONES DE LA EMPRESA.

Declaración de la Política:

Sólo el personal debidamente autorizado puede retirar equipos pertenecientes a (ITLA) fuera de las instalaciones. Esta persona en todo momento es el responsable por la seguridad del mismo y de la información que contenga, por lo que se deben tomar medidas de protección ante el acceso no autorizado a las unidades de almacenamiento de cada equipo que se disponga retirar de la Empresa.

Objetivo:

Constatar que al momento de retirar un equipo de la empresa se haya obtenido la autorización necesaria, además de validar que el mismo no almacene información confidencial.

Criterios para la implementación de la política:

- Tener un inventario de control con los equipos que están fuera de las instalaciones de la Empresa.
- Revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.
- Proteger la información contenida en las unidades de almacenamiento que se dispongan a retirar de las instalaciones de la Empresa.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los empleados y, en particular, al personal Gerencial y/o Supervisor del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores, son responsables de ejecutar esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.5. POLÍTICA DE USO DEL CORREO ELECTRÓNICO Y LOS RECURSOS INFORMÁTICOS.

Declaración de la Política:

El correo electrónico y los recursos informáticos deben ser utilizados solo para los propósitos de la empresa y deben tomarse las previsiones de seguridad requeridas para la protección de la información de la empresa.

Objetivo:

Establecer normas en el uso del correo electrónico y los recursos informáticos, asegurando la confidencialidad e integridad del contenido del correo y en los dispositivos de almacenamiento de los recursos informáticos, evitando el mal uso del mismo y de los recursos tecnológicos en la red interna.

Criterios para la implementación de la política:

- Definir los requisitos para la revisión periódica de los controles de acceso.
- Indicar los requisitos para la autorización formal de las solicitudes de acceso.
- Señalar los perfiles de acceso de usuario normales para los roles de trabajo regulares en la organización.
- Controlar el envío de correos electrónicos tanto en la red interna de la empresa como por líneas públicas inseguras que puede comprometer la confidencialidad y la integridad de la información transmitida.
- El envío de copias de archivos a los colegas en la red interna, crea duplicados innecesarios y también compromete la integridad del documento y/o archivo original.
- La recepción, la falta de detección, y la introducción de virus, no sólo puede dañar los sistemas y datos propios, sino que también pueden distribuirse a través de la red de la empresa, originando impactos mayores.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los empleados del Instituto Tecnológico de las Américas (ITLA), que hacen uso del correo electrónico y recursos informáticos de la empresa.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Responsabilidades:

- Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), son responsables de que el personal bajo su cargo conozca sobre esta política y le dé cumplimiento.
- Todos los empleados del Instituto Tecnológico de las Américas (ITLA) deben dar cumplimiento a esta política.
- La Gerencia del Tecnología de la Información debe ofrecer las herramientas necesarias para el uso del correo electrónico y los recursos informáticos de forma segura.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.6. POLITICA DE USO ADECUADO DEL INTERNET.

Declaración de la Política:

El uso del Internet debe ser sólo para los propósitos relacionados a la empresa y deben tomarse las previsiones de seguridad requeridas para la protección de la información de la Empresa. Cualquier uso no directamente relacionado con procesos internos, debe ser aprobado por el Gerente del área solicitante y supervisado por la Gerencia encargada de la supervisión de seguridad.

Objetivo:

Asegurar que el uso de Internet sea para fines relacionados con la empresa, para mitigar el riesgo al descargar archivos e información de la red, así como garantizar la optimización el uso del ancho de banda para las operaciones internas de la empresa.

Criterios para la implementación de la política:

- La conexión a tiempo completo al Internet ofrece la oportunidad incomparable para la infiltración oportunista y malévolos de los piratas informáticos quienes pueden ver la ubicación física y lógica en la red y sondear los puntos de vulnerabilidad.
- La identificación de toda la información relacionada a las aplicaciones del negocio y los riesgos de la información que está expuesta.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todo el personal del Instituto Tecnológico de las Américas (ITLA), que hace uso de Internet, los cuales deben seguir las políticas de la Empresa para el buen uso del Internet.

Responsabilidades:

- Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), deben asegurar que el personal bajo su cargo conozca y dé cumplimiento a esta política.
- Todo usuario que tenga asignado un equipo de computación tiene responsabilidad directa en el cumplimiento de las políticas de seguridad.
- La Gerencia de Tecnología de la Información debe brindar herramientas para la protección y acceso a Internet.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.7. POLITICA DE ENVÍO DE INFORMACIÓN A TERCEROS.

Declaración de la Política:

Antes de enviar la información confidencial a terceros, debe verificarse que el receptor previsto esté autorizado a recibir tal información y exista el compromiso de protegerla conforme a su confidencialidad.

Objetivo:

Garantizar la integridad y confidencialidad de la información a ser enviada a un tercero externo a la empresa.

Criterios para la implementación de la política

- Los terceros que reciben la información pueden no tratarla de manera confidencial, dando por resultado que esta sea accedida por personas no autorizadas.
- Señalar las responsabilidades del empleado, contratista, y cualquier otro usuario de no comprometer la organización, por ejemplo, a través de la difamación, hostigamiento, imitación envío de cadenas de correos, compra no autorizada.
- Definir la utilización de técnicas de criptografía, por ejemplo, para proteger la confidencialidad, la integridad y autenticidad de la información.
- Definir los controles y restricciones asociadas con el envío de recursos de comunicación, por ejemplo, para no divulgar información sensible y evitar que sean oídos o interceptados al hacer una llamada telefónica por: personas en su vecindad inmediata al utilizar teléfonos móviles y la intervención de la línea telefónica, y otras formas de escuchar a escondidas a través del acceso físico al auricular del teléfono o la línea telefónica, o utilizando receptores de la exploración, y/o personas al extremo del receptor.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y en general a todos los empleados del Instituto Tecnológico de las Américas (ITLA), y en especial a todos los Gerentes, Coordinadores y/o Supervisores que tienen bajo su responsabilidad la manipulación de activos de información críticos para la empresa.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Responsabilidades:

- Aquellos que tienen bajo su responsabilidad la manipulación de activos de información críticos para la empresa, son también responsables de asegurar su manipulación bajo esquemas seguros.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.8. POLÍTICAS DE DETECCIÓN Y RESPUESTA A INCIDENTES:

1.8.1. POLÍTICA DE REPORTE DE BRECHAS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN.

Declaración de la Política:

La identificación de cualquier brecha o debilidad de la seguridad de la información se debe reportar inmediatamente a la Gerencia encargada de tecnología y a la Gerencia de Seguridad de la Información a través de los canales y procesos definidos por la empresa con el objeto de proceder con la identificación de cualquier daño causado, efectuar cualquier restauración o reparación requerida además de facilitar la recopilación de cualquier evidencia asociada.

Objetivo:

Identificar cualquier brecha de seguridad de la información que resulte o no de incidentes de seguridad cuyo último efecto es el daño o pérdida de datos de un sistema. El reporte oportuno de vulnerabilidades es vital para tomar las acciones correctivas necesarias de acuerdo al caso.

Criterios para la implementación de la política:

- Cuando no existen procedimientos para reportar debilidades en la seguridad de la información, hay la posibilidad de que personal inexperto pueda intentar corregir una debilidad de la seguridad en programas de aplicación o sistemas operativos, lo cual podría interrumpir la continuidad de procesos críticos del negocio.
- El atraso en darle inicio a las investigaciones pertinentes que debe llevar a cabo la Gerencia encargada de la supervisión de seguridad puede incrementar las pérdidas potenciales asociadas al incidente detectada.
- Si el personal no está consciente de la importancia de reportar brechas potenciales de seguridad de la información, los incidentes podrían permanecer sin investigación por un período inaceptable.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los empleados y terceros del Instituto Tecnológico de las Américas (ITLA), quienes son corresponsables de velar por la seguridad de los activos de información de la Empresa.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Responsabilidades:

- Todo usuario que tenga asignado un equipo de computación tiene responsabilidad directa en el cumplimiento de las políticas de seguridad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.8.2. POLÍTICA DE RESPALDO DE DATOS EN ESTACIONES DE TRABAJO CLASIFICADAS COMO CRÍTICAS (INCLUYENDO EQUIPOS PORTÁTILES).

Declaración de la Política:

La información y datos almacenados en las estaciones de trabajo críticas de la empresa se deben respaldar periódicamente.

Objetivo:

Establecer la práctica de respaldar la información almacenada en estaciones de trabajo para evitar pérdidas que conlleven al retraso y/o paralización de las operaciones de la Empresa.

Criterios para la implementación de la política:

- Los datos contentivos en las estaciones de trabajo se pueden alterar o perder, debido a fallas internas de hardware o software; tales datos pueden ser de valor significativo y su pérdida puede generar costos importantes en la Empresa.
- Asignar a las copias de seguridad una protección física adecuada y ambiental coherente con los estándares aplicados en el sitio principal.
- Probar las copias de seguridad regularmente para mantener la continua confiabilidad de las mismas y su correcto funcionamiento.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y todos los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), responsables de la generación y/o modificación de información confidencial de la Empresa.

Responsabilidades:

- Todo personal de la Empresa que tenga asignado un computador portátil es responsable de tomar las consideraciones necesarias para evitar la pérdida de información.
- La Gerencia de Tecnología de la Información debe implementar los medios idóneos para el cumplimiento de esta Política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

1.8.3. POLÍTICA DE ACCESO DE TERCEROS A INFORMACIÓN CONFIDENCIAL.

Declaración de la Política:

El acceso de terceros a la información confidencial se permite sólo a personas con la debida autorización y justificación del requerimiento, se debe tener control y registro sobre la información accedida.

Objetivo:

Evitar y detectar el acceso no autorizado a los activos de información de la empresa por parte de personas ajenas a la misma.

Criterios para la implementación de la política:

- Definir los requisitos para la revisión periódica de los controles de acceso.
- Señalar los requisitos para la autorización formal de las solicitudes de acceso.
- Eliminar o bloquear inmediatamente los derechos de acceso a los usuarios que hayan cambiado de rol o trabajo o dejado la organización.
- Verificar periódicamente para eliminar o bloquear los identificadores (ID) y cuentas de usuario redundantes.
- Resguardar documentos clasificados como confidenciales en zonas no accesibles por terceros a la empresa.
- Incluir en los documentos con clasificación crítica de seguridad cláusulas de confidencialidad y no divulgación, tanto en pie de páginas, firmas de correo, entro otros.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todo el personal del Instituto Tecnológico de las Américas (ITLA), el cual debe seguir los procedimientos de almacenamiento y manipulación de los activos de información de acuerdo a su clasificación.

Responsabilidades:

- Todos los Gerentes, Coordinadores y/o Supervisores deben asegurar que el personal bajo su cargo conozca y le dé cumplimiento a esta política.
- La Gerencia de Tecnología de la Información debe brindar las herramientas para brindar los accesos y el correspondiente monitoreo de ellos.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

CAPÍTULO II. POLÍTICAS PARA EL PERSONAL GERENCIAL Y/O SUPERVISOR:

2.1. POLÍTICA DE MANTENIMIENTO DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN DE CLIENTES.

Declaración de la Política:

La información referente a los clientes y de terceros de la empresa es confidencial, se debe proteger y salvaguardar del acceso y divulgación no autorizado.

Objetivo:

Mantener la información de los clientes como confidencial es un requisito legal y esencial para la credibilidad de la empresa.

Criterios para la implementación de la política:

- La confidencialidad de la información de los clientes puede comprometerse si se divulga a terceros no autorizados.
- La confidencialidad de la información puede ser comprometida si accede a las peticiones de personas no autorizadas.
- Asegurar la confidencialidad de la información confidencial a través de la implementación de técnicas criptográficas.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y en general a todos los empleados del Instituto Tecnológico de las Américas (ITLA), y a los Gerentes, Coordinadores y/o Supervisores que tienen bajo su responsabilidad la manipulación de activos críticos de información.

Responsabilidades:

- Todos los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), son responsables de darle cumplimiento a esta política. Aquellos que tienen bajo su responsabilidad la manipulación de activos de información muy críticas para la Empresa, son también responsables de asegurar su manipulación bajo esquemas más seguros.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- La Gerencia de Tecnología de la Información es responsable de proveer herramientas especializadas para cifrar la información considerada y clasificada como crítica o confidencial.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

2.2. POLÍTICA DE DISTRIBUCIÓN Y DIVULGACIÓN DE INFORMACIÓN.

Declaración de la Política:

Los Gerentes, Coordinadores y/o Supervisores deben asegurarse que todos los empleados estén completamente enterados de sus deberes y responsabilidades referentes a compartir o distribuir información (pública y/o confidencial) dentro o fuera de la empresa.

Objetivo:

Garantizar la distribución y divulgación de información de la Empresa con previa autorización del propietario, de manera interna o externa, a fin de prevenir los riesgos asociados.

Criterios para la implementación de la política:

- La liberación de cierta información, aun cuando sea de forma inadvertida a terceros fuera de la Empresa, puede contravenir regulaciones legales que pueden conducir al procesamiento legal y otras penalidades.
- El receptor de la información o los sistemas del receptor, podría comprometer la confidencialidad de documentos sensibles, convirtiéndose en una potencial amenaza a la seguridad.
- Desarrollar e implementar una política organizacional para la protección de datos y privacidad.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los empleados del Instituto Tecnológico de las Américas (ITLA), y en particular, a los Gerentes, Coordinadores y Supervisores.

Responsabilidades:

- Los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), deben conocer sobre esta política y darle cumplimiento.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

2.3. POLÍTICA PARA LA CONTRATACIÓN DE PERSONAL FIJO O TEMPORAL.

Declaración de la Política:

Se deben realizar las respectivas revisiones de los antecedentes de cualquier persona que opte a un cargo, tenga relación comercial o de contratación con el Instituto Tecnológico de Las Américas (ITLA).

Objetivo:

Seleccionar adecuadamente el personal fijo o contratado dentro de la organización en base a la responsabilidad del cargo al cual optará el aspirante.

Criterios para la implementación de la política:

- Comprobar los aspectos relacionados con su perfil y resumen curricular.
- Revisar la procedencia, formación, referencias personales, entre otros.
- Evaluar el perfil del personal a ser seleccionado por cargo y responsabilidad asociada al mismo.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los Gerentes del Instituto Tecnológico de las Américas (ITLA) quienes tienen bajo su responsabilidad la contratación de nuevos empleados y/o contratistas.

Responsabilidades:

- La Gerencia encargada de los asuntos administrativos es responsable de realizar las respectivas revisiones de los antecedentes de los postulados a los diferentes cargos dentro de la organización en conjunto con el apoyo de las Gerencias encargadas de Tecnología de la Información y supervisión de la seguridad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

2.4. POLÍTICA PARA LA CONTRATACIÓN DE PROVEEDORES EXTERNOS.

Declaración de la Política:

Todos los proveedores externos, contratados para dar servicios a (ITLA), deben comprometerse a cumplir con las políticas de Seguridad de Información. Este compromiso se establecerá en el contrato respectivo o en constancia separada.

Objetivo:

Dar a conocer las Políticas de Seguridad de la Información relacionadas a los contratistas y/o terceros, a fin de garantizar el cumplimiento de las mismas.

Criterios para la implementación de la política:

- Cuando no existe mención sobre la Seguridad de la Información en el contrato con terceros, y se determina un evento de seguridad una vez concluida la contratación, puede dificultarse la determinación de responsabilidades sobre estos eventos.
- Cuando no se hace referencia sobre las políticas de Seguridad de Información de ISC S.A en el contrato con proveedores externos, los activos de información pueden estar en riesgo debido a que su propio entendimiento sobre las políticas seguramente difiere de los del Instituto Tecnológico de las Américas (ITLA).

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a cualquier empleado y, en particular, al personal supervisor del (ITLA) que requiera contratar servicios de terceros.

Responsabilidades:

- Todos y cada uno de los empleados y supervisores del Instituto Tecnológico de las Américas (ITLA), que deban contratar a terceros, son responsables de ejecutar esta política.
- Todos los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), son responsables de que el personal bajo su cargo conozca y de cumplimiento sobre esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

2.5. POLÍTICA PARA EL USO DE ACUERDOS DE CONFIDENCIALIDAD (PERSONAL Y TERCEROS).

Declaración de la Política:

Al momento de la contratación entre (ITLA) y un empleado (fijo y temporal) o empresa de servicios, deben firmarse los respectivos acuerdos de confidencialidad y no divulgación de la información que se maneje entre ambas partes.

Objetivo:

Emplear los acuerdos de confidencialidad como mecanismos legales para los casos que se divulgue sin autorización información confidencial.

Criterios para la implementación de la política:

- De no firmarse un acuerdo de confidencialidad, los secretos del Negocio y Financieros de la empresa podrían ser divulgados a personas externas.
- En caso de no incluir las cláusulas de confidencialidad en los contratos con terceros, estos tendrán acceso a los sistemas de información y proyectos de la Empresa, siendo posible que la información sensible sea divulgada a terceros o usada para transacciones ilícitas, incluso a través de conversaciones informales.
- Cuando un empleado renuncia o se le pide su retiro de la empresa y no ha firmado la Declaración de Confidencialidad, la Empresa podría quedar expuesta a la fuga de información confidencial posterior al egreso del empleado.
- Establecer los términos para devolver o destruir información al cese del acuerdo; y las acciones esperadas a ser tomadas en caso de violación de este acuerdo.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los Gerentes del Instituto Tecnológico de las Américas (ITLA) quienes tienen bajo su responsabilidad la contratación de nuevos empleados y/o contratistas.

Responsabilidades:

- La Gerencia encargada de los asuntos administrativos es responsable por mantener actualizado el documento Declaración de Confidencialidad y hacerlo firmar al momento del ingreso del empleado (fijo y contratado).

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- La Gerencia encargada de la supervisión de seguridad es responsable de proveer las actualizaciones de las cláusulas de confidencialidad y especificaciones de seguridad del Documento de Contratación.
- La Gerencia encargada los asuntos administrativos es responsable de hacer firmar los contratos con terceros y velar que las cláusulas de confidencialidad y especificaciones de seguridad estén incluidas y actualizadas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

2.6. POLÍTICA PARA LA SEGURIDAD DE LA GESTIÓN DE PROYECTOS.

Declaración de la Política:

La Gerencia encargada de la gestión de proyectos dentro del Instituto Tecnológico de las Américas (ITLA) debe garantizar en conjunto con las Gerencias que se encargan de Tecnología de la Información y la supervisión de seguridad la revisión de los aspectos de Seguridad de la Información de cualquier proyecto a ser ejecutado o implementado por la empresa.

Objetivo:

Garantizar la ejecución de proyectos bajo los estándares de seguridad de la información y así resguardar la confidencialidad, integridad y disponibilidad de la información relacionada con el producto final a la culminación del proyecto.

Criterios para la implementación de la política:

- En caso que la Gerencia encargada de la gestión de los proyectos no muestre interés sobre la aplicación de las políticas de Seguridad de la Información, se pondrían en riesgo los activos de información en la empresa y sus clientes.
- Aprobar metodologías y procesos para la seguridad de la información, por ejemplo, evaluación de riesgos, clasificación de la información.
- Incorporar durante las fases de análisis, desarrollo, pruebas e implementación de los proyectos las evaluaciones de riesgo y seguridad de la información.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a la Alta Gerencia del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- La Gerencia encargada de la gestión de proyectos del Instituto Tecnológico de las Américas (ITLA) es responsable por tomar en consideración los aspectos de seguridad de la información ante cada proyecto a ser implementado o considerado por la organización.
- Las Gerencias encargadas de Tecnología de la Información y Seguridad de la Información son responsables por brindar el apoyo necesario durante las fases de gestión de proyectos.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

2.7. POLÍTICA DE DISTRIBUCIÓN DE PROGRAMAS DE INDUCCIÓN AL PERSONAL.

Declaración de la Política:

El personal del Instituto Tecnológico de las Américas (ITLA) (fijo y temporal) debe recibir información y herramientas que les permitan mejorar su conocimiento y entendimiento respecto a la Seguridad de la Información, así como a las posibles vulnerabilidades, medidas de resguardo y prevención contempladas por la empresa.

Objetivo:

Capacitar y desarrollar el nivel de conciencia del personal de la empresa sobre los riesgos de seguridad de la información de forma tal que las acciones preventivas sean parte de las actividades laborales regulares.

Criterios para la implementación de la política:

- La información confidencial puede ser ilegalmente adquirida, dañada o modificada debido a desconocimiento en materia de Seguridad de la Información.
- La información confidencial puede ser comprometida por el personal si asume sus responsabilidades sin haber recibido entrenamiento específico sobre Seguridad de la Información.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- La Gerencia de Tecnología de la Información y la Gerencia de Seguridad de la Información son responsables de establecer los requerimientos y planificar las actividades correspondientes.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

CAPÍTULO III. POLÍTICAS PARA EL PERSONAL TÉCNICO:

3.1. POLÍTICA PARA LA INSTALACIÓN DE NUEVOS EQUIPOS DE CÓMPUTO.

Declaración de la Política:

La instalación de todo nuevo equipo de cómputo debe ser planeada formalmente y notificada a todas las partes interesadas previa instalación para su incorporación o actualización en el ciclo de gestión de los activos.

Objetivo:

Planificar la instalación de nuevos equipos de cómputo regido por un procedimiento que garantice el cumplimiento de las mejores prácticas y las políticas descritas en este documento, de tal forma que se puedan evitar interrupciones innecesarias y brechas de seguridad.

Criterios para la implementación de la política:

- Identificar todos los activos y documentar la importancia de estos activos.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y al personal técnico del Instituto Tecnológico de las Américas (ITLA), responsable de llevar a cabo la instalación de nuevos equipos de cómputo, sistemas y nuevos componentes.

Responsabilidades:

- Todos los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas (ITLA), son responsables de que el personal bajo su cargo conozca sobre esta política y le den cumplimiento.
- La Gerencia de Tecnología de la Información debe ser la responsable de instalar y coordinar los controles de cambio necesarios para la instalación de cualquier nuevo equipo de cómputo.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.2. POLÍTICA PARA LA ADMINISTRACIÓN DEL CONTROL DE ACCESO.

Declaración de la Política:

El código de usuario (o login), o cualquier otro medio de acceso, así como la selección de contraseñas y otros modos de autenticación, su uso y administración como mecanismo prioritario para el control de acceso a sistemas, debe adherirse a las mejores prácticas.

Objetivo:

Establecer un estándar de creación y uso de códigos de usuario y claves robustas, protección de las mismas y su frecuencia de cambio, en los sistemas informáticos que son accedidos por la combinación de la identificación del usuario y su contraseña y otros modos de autenticación, siendo la correcta administración de las credenciales de acceso un área clave en la seguridad de la información.

Criterios para la implementación de la política:

- La contraseña y otros modos de autenticación y la clave de acceso del usuario está directamente relacionada con el perfil y su nivel de admisión en los sistemas.
- Aplicar la separación de roles de control de acceso.
- Cuando se requiere autenticación y verificación de identidad sólidas, se debieran utilizar métodos de autenticación alternativos para las claves secretas, como los medios criptográficos, tarjetas inteligentes, dispositivos o medios biométricos.
- Requerimientos para la autorización formal de las solicitudes de acceso.
- Requerimientos para la revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y al personal técnico del Instituto Tecnológico de las Américas (ITLA), encargado de administrar los accesos de los sistemas, aplicaciones, carpetas compartidas, entre otros.

Responsabilidades:

- La Gerencia de Tecnología de la Información de información es la responsable de su implementación.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.3. POLÍTICA PARA EL CONTROL DE ACCESO AL SOFTWARE DE SISTEMAS OPERATIVOS.

Declaración de la Política:

El acceso a configuración de sistemas operativos y otras utilidades debe ser restringido a personas autorizadas que realicen funciones de administración o gestión de los sistemas operativos.

Objetivo:

Controlar las operaciones de los equipos de cómputo; preinstalados donde se encuentran los comandos y las utilidades que mantienen el ambiente de operación del mismo. Todos los sistemas tanto en los equipos de cómputo como de los servidores, deben reforzarse para eliminar todas las herramientas y utilidades innecesarias antes de entregarse a los usuarios.

Criterios para la implementación de la política:

- Autenticar los usuarios autorizados, de acuerdo con una política definida de control de acceso.
- Registrar los intentos de autenticación exitosos y fallidos al sistema.
- Registrar la utilización de los privilegios especiales del sistema.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y al personal técnico del Instituto Tecnológico de las Américas (ITLA), encargado de administrar los Sistemas Operativos de los servidores y estaciones de trabajo.

Responsabilidades:

- La Gerencia de Tecnología de la Información debe asegurar que el personal responsable de administrar los sistemas operativos conozca y le dé cumplimiento a esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.4. POLÍTICA DE CREACIÓN DE ACCESOS PARA EL USO DE INTERNET.

Declaración de la Política:

El personal responsable de la definición de accesos a Internet debe asegurarse que la red del Instituto Tecnológico de las Américas ITLA esté protegida tanto de intrusiones externas, como del acceso inapropiado a Internet por parte de los usuarios de la empresa, utilizando las herramientas de restricción de acceso debidamente configuradas.

Objetivo:

Controlar el acceso y uso del Internet utilizando los dispositivos de protección de periferia requeridos y mitigando los riesgos que se presentan al descargar archivos e información del Internet con código malicioso, así como garantizar el uso óptimo del ancho de banda de la empresa.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a la Gerencia encargada de la administración de los Sistemas, quien provee los accesos a Internet a los usuarios de la red interna.

Responsabilidades:

- Las Gerencias del Instituto Tecnológico de las Américas ITLA son responsable de la definición de los perfiles de acceso a Internet del personal bajo su supervisión y la administración de los accesos a Internet será responsabilidad de la Gerencia encargada de la administración de los Sistemas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.6. POLÍTICA DE REVISIÓN DE REGISTROS DE AUDITORIA (LOGS).

Declaración de la Política:

Los registros deben ser revisados regularmente por el personal entrenado y las discrepancias deben ser informadas a la Dirección General y a la Gerencia encargada de la supervisión de la seguridad.

Objetivo:

Almacenar los archivos de control de auditoría generados por los sistemas, los cuales contienen todos los detalles de los cambios y actualizaciones realizados a los registros y al ambiente de producción por si se requiere una revisión posterior.

Criterios para la implementación de la política:

Producir registros de auditoría que incluyan, cuando sea pertinente:

- La identificación de los usuarios.
- Las fechas, tiempos y los detalles de los eventos claves, por ejemplo, la entrada y salida del sistema.
- La identidad o localización del terminal, si es posible.
- Los registros de los intentos de acceso exitosos y rechazados al sistema.
- Los registros de los intentos de acceso exitosos y rechazados a los datos y de otros recursos.
- Los cambios a la configuración del sistema.
- La utilización de privilegios.
- La utilización aplicaciones y utilidades del sistema.
- El acceso a los archivos y su clase de acceso.
- La activación y desactivación del sistema de protección, tales como, los sistemas contra virus y los sistemas de detección de intrusos.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a la Gerencia encargada de la administración de los sistemas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Responsabilidades:

- La Gerencia encargada de la administración de los Sistemas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.7. POLÍTICAS RELACIONADAS AL MANTENIMIENTO DE HARDWARE Y SOFTWARE:

3.7.1. POLÍTICA PARA LA APLICACIÓN DE ACTUALIZACIONES AL SOFTWARE.

Declaración de la Política:

Las actualizaciones para resolver errores en el software deben ser aplicados regularmente a menos que se demuestre que el mismo no se requiere, o se justifique su no implementación.

Objetivo:

Instalar las actualizaciones de software para la corrección de errores (bugs) reportados por los proveedores de software o usuarios. Las actualizaciones de software deben proceder de fuentes seguras y deben ser probados previo su implementación.

Criterios para la implementación de la política:

- Tomar inmediatamente la acción adecuada ante una vulnerabilidad que requiera atención técnica de inmediato.
- Mantener un registro de auditoría para todos los procesos evaluados.
- Realizar seguimientos regularmente y evaluarse al proceso de gestión de vulnerabilidades técnicas para asegurar su eficacia y eficiencia.

Alcance:

Esta política va dirigida a las Gerencias encargadas de la Seguridad de la Información y la administración de los sistemas.

Responsabilidades:

- Gerencia de Tecnología de la Información del Instituto Tecnológico de las Américas (ITLA).

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.7.2. POLÍTICA PARA LA INSTALACIÓN DE HERRAMIENTAS DE OFIMÁTICA.

Declaración de la Política:

Las estaciones de trabajo del Instituto Tecnológico de las Américas (ITLA) solo deben contar con las herramientas de oficina estándar y aplicaciones requeridas por el usuario, sobre la base de sus roles y funciones.

Objetivo:

Evitar que en las estaciones de trabajo se instalen aplicaciones no requeridas para el desempeño de las labores de los empleados. Los usuarios solo deben contar con las herramientas de ofimáticas definidas.

Criterios para la implementación de la política:

- Contar con número limitado de herramientas minimiza los riesgos de exposición a vulnerabilidades no detectadas por los fabricantes.
- Notificar a las Gerencias encargadas de Tecnología de la Información y Seguridad de la Información la necesidad de instalar una nueva herramienta de trabajo para su correspondiente evaluación, prueba y posterior implementación en producción.
- Mantener actualizado el inventario de herramientas necesarias para mantener la operativa del Instituto Tecnológico de las Américas (ITLA).
- Desarrollar e implementar las directrices para la utilización de dispositivos móviles, especialmente para la utilización fuera de los predios de la empresa.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los empleados del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- Los Gerentes, Coordinadores y/o Supervisores del Instituto Tecnológico de las Américas ITLA, deben asegurar que los empleados que le reportan conozcan sobre esta política y den cumplimiento.
- La Gerencia de Tecnología de la Información debe brindar las herramientas necesarias para dar cumplimiento a esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.7.3. POLÍTICA PARA LA IMPLEMENTACIÓN DE ANTIVIRUS CORPORATIVO.

Declaración de la Política:

Se requiere la implantación de Antivirus y otros recursos de control, que provean protección a todos los servidores y estaciones de trabajo de la red del Instituto Tecnológico de las Américas (ITLA).

Objetivo:

Contar con los mecanismos de prevención, detección y eliminación de virus informáticos en todos los equipos que conforman la Red interna.

Algunos temas de seguridad de la información que deben considerarse al implantar la política son:

- Realizar revisiones regulares del contenido del software y datos de los sistemas que sustentan procesos críticos del negocio; la presencia de cualquier archivo no aprobado o modificaciones no autorizadas debe ser investigada formalmente.
- Ejecutar el código malicioso en un ambiente aislado lógicamente.
- Bloquear cualquier uso de código malicioso.
- Bloquear la recepción de código malicioso.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y al personal de la Gerencia de Tecnología de la Información de la empresa.

Responsabilidades:

- La Gerencia de Tecnología de la Información debe instalar el antivirus de la empresa en todas las estaciones de trabajo, equipos portátiles y servidores.
- La Gerencia de Seguridad de la Información es la encargada de realizar la selección de la herramienta que mejor se adapte a las necesidades de la empresa.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.8. POLÍTICAS DE DETECCIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:

3.8.1. POLÍTICA DE INVESTIGACIÓN DE LA CAUSA Y EL IMPACTO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Declaración de la Política:

Los incidentes de seguridad de la información deben ser investigados de forma apropiada por el personal convenientemente entrenado y calificado para ello.

Objetivo:

Investigar los incidentes de seguridad de la información para la identificación de su causa y la valoración de su impacto en los sistemas e información del Instituto Tecnológico de las Américas (ITLA).

Alcance:

Esta política va dirigida a las Gerencias encargadas de la Seguridad de la Información y Tecnología de la Información quienes tienen bajo su responsabilidad llevar a cabo la investigación de los incidentes y vulnerabilidades de seguridad de la información y su impacto asociado.

Responsabilidades:

- Las Gerencias encargadas de la seguridad y Tecnología de la Información bajo la supervisión de la Dirección General.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.8.2. POLÍTICA DE DEFENSA CONTRA ATAQUES INTERNOS O EXTERNOS.

Declaración de la Política:

Es prioridad reducir al mínimo las posibilidades de ataques informáticos, contra los sistemas e información de la empresa, a través de una combinación de sistemas de protección perimetral, control de acceso y procedimientos robustos de seguridad. Para reducir la incidencia y posibilidad de ataques internos o externos los estándares de control de acceso y de clasificación de los datos deben ser revisados periódicamente y su mantenimiento debe ser constante.

Objetivo:

Identificar ataques contra sistemas y/o aplicaciones de la empresa para implementar los procedimientos apropiados con el fin de reducir el impacto o eliminar el riesgo, elaborando posteriormente un control de daños para ajustar los procedimientos y prevenir su ocurrencia futura.

Criterios para la implementación de la política:

- Señalar los perfiles de acceso de usuario normales para los roles de trabajo comunes en la organización.
- Colocar la separación de roles de control de acceso, por ejemplo, solicitud de acceso, autorización de acceso, administración de acceso.
- La identificación de toda la información relacionada a las aplicaciones del negocio y los riesgos de la información que está expuesta.
- Monitorear los cambios a la configuración del sistema.
- Revisar las direcciones y protocolos de red.
- Revisar las alarmas activadas por el sistema de control de acceso.
- Verificar la activación y desactivación del sistema de protección, tales como, los sistemas contra virus y los sistemas de detección de intrusos.

Alcance:

Esta política va dirigida a las Gerencias encargadas de Tecnología de la Información y supervisión de la Seguridad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Responsabilidades:

- La Gerencia de Tecnología de la Información del Instituto Tecnológico de las Américas (ITLA) es responsable de dar cumplimiento a esta política bajo el apoyo de la Gerencia encargada de la supervisión de la seguridad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.8.3. POLÍTICA PARA ASEGURAR LA INTEGRIDAD EN LAS INVESTIGACIONES SOBRE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

Declaración de la Política:

El uso de los sistemas de información debe monitorearse regularmente y todos los acontecimientos inesperados deben ser registrados y analizados. Tales sistemas deben también ser periódicamente auditados y los resultados del análisis de los eventos detectados e históricos deben ser combinados para consolidar la integridad de cualquier investigación subsiguiente.

Objetivo:

Monitorear y auditar regularmente los sistemas de información para garantizar la integridad y confiabilidad de las investigaciones relacionadas con incidentes de seguridad.

Criterios para la implementación de la política:

- Es importante que las investigaciones sobre supuestos incidentes de seguridad de la información estén registradas formalmente. Esto asegura que la investigación sobre el incidente se pueda revisar posteriormente.
- Implantar las responsabilidades y los procedimientos para manipular eficazmente los eventos y debilidades de la seguridad de la información.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a la Gerencia encargada de la administración de los Sistemas.

Responsabilidades:

- La Gerencia de Tecnología de la Información del Instituto Tecnológico de las Américas (ITLA) es responsable de dar cumplimiento a esta política bajo el apoyo de la Gerencia encargada de la supervisión de la seguridad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.9. POLÍTICAS DE RECUPERACIÓN Y RESTAURACIÓN DE OPERACIONES Y FUNCIONES CRÍTICAS:

3.9.1. POLÍTICA PARA LA RECUPERACIÓN DE SISTEMAS EN CASO DE FALLAS.

Declaración de la Política:

Se deben tomar las medidas necesarias para proteger la integridad de la infraestructura tecnológica, contando con los procedimientos adecuados de respaldo, continuidad y recuperación de operaciones, que puedan ponerse en ejecución cuando se requiera.

Objetivo:

Establecer procedimientos de respaldo y recuperación para que, en caso de fallas en la operación regular, se cuenten con los mecanismos para restablecer los servicios.

Criterios para la implementación de la política:

- La indisponibilidad de los sistemas e información que sufra una interrupción, en el proceso normal de operación puede afectar la continuidad del negocio y generar cuantiosas pérdidas a la empresa.
- La corrupción y pérdida de información confidencial puede afectar las operaciones y atrasar procesos críticos del negocio.
- La información requerida al localizarse y restaurarse podría estar corrupta.
- La información se puede perder o sobrescribir por la restauración incorrecta de los medios de respaldo.

Alcance:

Esta política va dirigida a las Gerencias encargadas de Tecnología de la Información y Seguridad de la Información y a todos los empleados del Instituto Tecnológico de las Américas (ITLA), y en particular, a los Gerentes, Coordinadores y/o Supervisores.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Responsabilidades:

- La Gerencia de Tecnología de la Información es responsable de prestar el servicio de respaldo y recuperación necesario para mantener la continuidad de las operaciones, así como el restablecimiento de las operaciones en caso de fallas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.9.2. POLÍTICA PARA EL ALMACENAMIENTO DE LA INFORMACIÓN DE RESPALDO

Declaración de la Política:

Los medios y lugar de almacenamiento usados para archivar la información respaldada deben ser apropiados al valor de la misma y al tiempo de duración prevista para estos. El almacenamiento de archivos electrónicos debe reflejar las necesidades de la empresa y cualquier requisito legal o regulatorio aplicable.

Objetivo:

Garantizar la disponibilidad de la información respaldada, para que la misma pueda ser restaurada cuando se requiera.

Criterios para la implementación de la política:

- El almacenamiento de los respaldos en sitios no adecuados o bien resguardados puede dificultar la recuperación en caso de pérdida de la información y poner en peligro la continuidad operativa.
- La debilidad en la duración de los medios usados para el almacenamiento de los archivos, puede dar lugar a fallas en la recuperación de los datos requeridos.
- Almacenar las copias de seguridad en una ubicación alejada, a una distancia suficiente como para evitar daños provenientes de un desastre en el local principal
- Asignar a la información de copias de seguridad un nivel adecuado de protección física y ambiental coherente con los estándares aplicados en el sitio principal.
- En situaciones donde la confidencialidad es importante, proteger las copias de seguridad por medio de encriptación.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a la Gerencia de Tecnología de la Información responsable de llevar a cabo los respaldos de la información de la Empresa y de asegurar su recuperación en caso de requerirse.

Responsabilidades:

- La Gerencia de Tecnología de la Información es responsable de brindar resguardo seguro de los respaldos y ofrecer medios de almacenamiento óptimos.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- La Gerencia de Seguridad de la Información es responsable de asegurar que se lleve a cabo el respaldo de la información confidencial de la empresa y que sea posible su recuperación en caso de requerirse.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.9.3. POLÍTICA PARA ESTABLECER UN PLAN DE SEGURIDAD DE LA INFORMACIÓN Y LOS ACTIVOS TECNOLÓGICOS PARA LA RECUPERACIÓN Y CONTINUIDAD DE LA OPERACION EN CASO DE DESASTRES.

Declaración de la Política:

El ITLA debe disponer de un plan de seguridad de la información y activos tecnológicos que permita la recuperación de éstos y la continuidad de las operaciones tecnológicas, cubriendo las actividades críticas y esenciales que dependan de la infraestructura de tecnologías de información. Dicho plan debe incluir los requerimientos resultantes de un análisis de vulnerabilidad, riesgo e impacto a la organización.

Objetivo:

Contar con un Plan de Seguridad de la Información y Activos Tecnológicos que garantice la continuidad de los servicios críticos, una vez que ocurran eventos inesperados que interrumpen los procesos de la institución.

Criterios para la implementación de la política:

- Cuando no existe un compromiso de la Directiva, o la Alta Gerencia de la institución, para el desarrollo del plan de seguridad y recuperación en caso de desastres, podría dificultarse el desarrollo e implementación del mismo.
- Las fallas al estimar el impacto de incidentes de seguridad, a corto y mediano plazo, pueden resultar en un nivel inapropiado de respuesta para la definición de un buen Plan de seguridad y recuperación en caso de desastres.
- Cuando no se reproducen condiciones reales durante las pruebas del plan de recuperación, el valor de tales pruebas es limitado.
- Comprender los riesgos que enfrenta la organización en términos de probabilidad e impacto en el tiempo, incluyendo la identificación y priorización de los procesos críticos de la organización.
- Identificar todos los activos involucrados en procesos críticos de la operación.
- Comprender el impacto que probablemente tienen en la institución las interrupciones causadas por incidentes relacionados a la seguridad de la información (es importante que las soluciones manejen las incidencias que causen impactos menores, así como los incidentes graves que puedan amenazar la viabilidad de la organización), y establecer los objetivos de la institución para los recursos de procesamiento de la información.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- Considerar la adquisición de los seguros adecuados que formarán parte del proceso de continuidad de la operación global, así como una parte de la gestión de riesgo operacional.
- Identificar y considerar la implementación de los controles preventivos y de mitigación adicionales.
- Identificar los recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos de seguridad de la información identificados.
- Asegurar la protección de los recursos de procesamiento de la información y la propiedad de la organización.
- Asegurar que las informaciones, bases de datos, respaldos, sistemas y equipos, puedan ser restablecidas con eficacia en caso de que ocurra cualquier eventualidad.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todos los responsables de activos de información del Instituto Tecnológico de las Américas (ITLA).

Responsabilidades:

- La Gerencia de Seguridad de la Información es responsable de elaborar y actualizar el Plan de Seguridad de la Información y Activos Tecnológicos para la correcta recuperación en caso de desastres y poder dar continuidad al negocio.
- Las Gerencias encargadas de la Seguridad de la Información y Tecnología de la Información deben llevar a cabo todas las acciones requeridas para ejecutar las pruebas del plan de continuidad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.10. POLÍTICAS DE AUDITORIA Y MONITOREO DE LA SEGURIDAD

3.10.1 POLÍTICA DE AUDITORIAS DE SEGURIDAD DE LA INFORMACIÓN Y ANÁLISIS DE VULNERABILIDAD Y RIESGO.

Declaración de la Política:

Siempre que se requiera la Gerencia encargada de la supervisión de seguridad tendrá acceso a los sistemas y archivos con el objeto de llevar a cabo auditorias de seguridad de la información. Periódicamente se llevarán a cabo auditorias, Análisis de Vulnerabilidad y Riesgo, a fin de detectar posibles nuevas vulnerabilidades y validar el cumplimiento y efectividad de las Políticas de Seguridad de la Información.

Objetivo:

Realizar análisis de riesgo y auditorias periódicas con el objeto de constatar el cumplimiento de las políticas de seguridad de la información para detectar posibles brechas de seguridad las cuales requieran acciones correctivas y monitorear las actividades de usuarios o sistemas cuando se considere necesario.

Criterios para la implementación de la política:

- Para que la definición de políticas de seguridad en una Empresa cumpla su objetivo, se requiere su revisión y reforzamiento continuo.
- Las auditorias deben realizarse con el objeto de:
 - Asegurar la integridad, confidencialidad y disponibilidad de la información y recursos de la empresa.
 - Investigar posibles incidentes de seguridad.
 - Asegurar el cumplimiento de las políticas de seguridad en la empresa.
 - Monitorear actividades de usuarios y/o sistemas cuando se requiera.
- La seguridad es dinámica, ya que cada día se detectan nuevas vulnerabilidades y aparecen nuevas técnicas de intrusión.
- Implantar las responsabilidades y los procedimientos para manipular eficazmente los eventos y debilidades de la seguridad de la información.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

Alcance:

Esta política va dirigida a las Gerencias encargadas de Tecnología de la Información y supervisión de la seguridad, así como a la Dirección General.

Responsabilidades:

- La Gerencia de Seguridad de la Información es el responsable de mantener actualizada la política y dar cumplimiento a la misma.
- La Dirección General debe proveer los recursos y el apoyo necesario para la ejecución de auditoria, análisis de vulnerabilidad y riesgo cuando se requiera.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.10.2. POLÍTICA DE MONITOREO DE SEGURIDAD DE LA INFORMACIÓN.

Declaración de la Política:

El comportamiento de la infraestructura tecnológica de la empresa y la ocurrencia de incidencias de seguridad deben ser monitoreados e investigados por el personal capacitado y calificado para ello.

Objetivo:

Realizar el monitoreo continuo en tiempo real, del comportamiento de la seguridad Empresa.

Criterios para la implementación de la política:

- La definición de políticas de seguridad e incorporación de tecnologías, permiten la administración proactiva de la seguridad.
- El análisis de eventos una vez ocurrido el daño, no es suficiente, se requiere su monitoreo en tiempo real para la detección y respuesta oportuna.
- Implantar las responsabilidades y los procedimientos para manipular eficazmente los eventos y debilidades de la seguridad de la información.

Alcance:

Esta política va dirigida al personal de las Gerencias encargadas de Tecnología de la Información y supervisión de la Seguridad.

Responsabilidades:

- La Gerencia de Tecnología de la Información debe proveer los recursos y el apoyo necesario para el cumplimiento de esta política.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.10.3. POLÍTICA DE MONITOREO DE LA PLATAFORMA TECNOLÓGICA (DISPOSITIVOS DE RED, SERVIDORES, BASES DE DATOS Y DISPOSITIVOS DE SEGURIDAD).

Declaración de la Política:

Todo elemento de hardware o software, que se incorpore a la plataforma tecnológica de la empresa, debe integrarse a la plataforma de monitoreo que administra la Gerencia de Tecnología de la Información y deben tener activas sus trazas de auditoría, a fin de monitorear su comportamiento y detectar cualquier evento de seguridad.

Objetivo:

Efectuar el monitoreo continuo de los dispositivos de red, servidores, bases de datos, servicios y componentes de seguridad de la empresa, con el propósito de conocer su estado y responder oportunamente ante la ocurrencia de eventos, evitando daños o pérdida de la operatividad de los procesos críticos de la empresa.

Algunos temas de seguridad de la información que deben considerarse al implantar la política:

- El análisis de eventos una vez ocurrido el daño no es suficiente. Se requiere su monitoreo en tiempo real para la detección y respuesta oportuna.
- Implementar la acción adecuada ante un incidente de seguridad de información.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y al personal de la Gerencia encargada de la administración de los Sistemas.

Responsabilidades:

- La Gerencia de Tecnología de la Información debe realizar el monitoreo operativo continuo de los dispositivos de la red.
- La Gerencia de Tecnología de la Información debe realizar el monitoreo continuo de los eventos de seguridad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

3.11. POLÍTICAS PARA EL CONTROL DE ACCESO A INFORMACIÓN Y SISTEMAS:

3.11.1. POLÍTICA PARA LA ADMINISTRACIÓN DEL ACCESO A USUARIOS.

Declaración de la Política:

El acceso a todos los equipos y sistemas operacionales incluyendo los derechos de acceso o privilegios, debe ser otorgado, cumpliendo con los privilegios de acceso para dicho rol durante el proceso de definición de perfiles.

Objetivo:

Administrar adecuadamente el acceso de los usuarios a los equipos y sistemas de información, que permitan establecer controles que identifiquen posibles brechas y vulnerabilidades de seguridad de la información en los estándares de control de acceso previamente definidos.

Criterios para la implementación de la política:

- La carencia de un procedimiento para la administración del control de acceso puede dar lugar al acceso no autorizado a los sistemas de información, de tal modo que se comprometa la confidencialidad y potencialmente la integridad de los datos.
- La asignación de privilegios inadecuados al personal inexperto puede dar lugar a problemas y a errores accidentales.
- Todo acceso a los sistemas de información, debe ser registrado en los archivos de control de auditoría.
- Los perfiles deben ser bien definidos por parte de los dueños de la información a ser accesible a través de cualquier equipo o sistema.

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y al personal técnico del Instituto Tecnológico de las Américas (ITLA), responsable de definir y administrar los niveles de acceso a los sistemas.

Responsabilidades:

- La Gerencia de Tecnología de la Información es responsable por otorgar los accesos a los usuarios basando en su rol y funciones dentro del Instituto Tecnológico de las Américas (ITLA).

ANEXO

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

4.0 POLÍTICA DE USO ACEPTABLE DE LOS RECURSOS DE INFORMACIÓN

Objetivo:

Esta política tiene el objetivo de fijar las normas fundamentales que deben regir los controles básicos a ser establecidos por la empresa de manera que se garantice el uso adecuado de los recursos relativos a los sistemas de información. La Empresa elaborará instructivos conforme al contenido de la presente política y velar por el cumplimiento de las mismas por parte de todo usuario de los sistemas de información, incluyendo empleados, contratistas y otros autorizados a tal uso.

Alcance:

Esta política define y detalla el uso aceptable de la información que se maneja a través de los sistemas de información y las herramientas de Internet y Correo Electrónico del Instituto Tecnológico de las Américas (ITLA), para así proteger al usuario y a la empresa de situaciones que pongan en peligro los sistemas y la información que contienen, agilizando los procesos operacionales de los distintos entes internos de la empresa, aumentar la eficiencia y efectividad en la prestación de los servicios.

Propiedad de los Recursos:

ITLA define en su Política de Uso que todo el recurso tecnológico es de su propiedad y será tratado como activo, s i e n d o por lo tanto sujeto de administración y control. En cuanto a los datos e información, los considera activos estratégicos. Como tales, deberán ser usados en función del trabajo. ITLA es el máximo responsable para la gobernabilidad de estos recursos, asimismo es la responsable de su coordinación y control. Como responsable técnico en la administración y distribución del servicio, se define a la Gerencia encargada de la administración de los Sistemas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

5.0 NORMAS APLICABLES AL USO DE COMPUTADORAS O ESTACIONES DE TRABAJO.

- Los equipos de cómputo, impresoras, y otros equipos electrónicos, son propiedad del Instituto Tecnológico de las Américas (ITLA).
- El uso del equipo de cómputo será destinado únicamente para apoyar las funciones propias del Instituto Tecnológico de las Américas (ITLA).
- El equipo de cómputo debe estar conectado a un regulador de voltaje o sistema de energía ininterrumpida.
- Todo disco flexible o unidad de almacenamiento portátil, deberá ser protegido y verificado para asegurar que no esté infectado con algún virus informático.
- El cambio de equipo de cómputo de una unidad administrativa a otra, debe ser notificado, con oportunidad, a la Gerencia encargada de la administración de los Sistemas, indicando con precisión marca, modelo, números de inventario y serie, enviando copia a la Gerencia encargada de los asuntos administrativos. El reemplazo de algún equipo de cómputo debe ser evaluado por la Gerencia encargada de la supervisión de la Seguridad.

6.0 NORMAS GENERALES APLICABLES AL USO DE LOS SISTEMAS DE INFORMACIÓN.

- Los sistemas de información del Instituto Tecnológico de las Américas (ITLA), incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad de la empresa, y sólo pueden utilizarse para fines estrictamente autorizados.
- Es responsabilidad de la empresa tomar las medidas necesarias para salvaguardar la confidencialidad de los datos personales de los empleados o de los ciudadanos contenidos en sus sistemas de información, conforme a las normas aplicables.
- Los programas y recursos utilizados en los sistemas de información de la empresa deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas sólo podrán ser instalados por personal autorizado a tales efectos. Además, no podrán instalarse programas sin la previa autorización de la Gerencia encargada de la supervisión de la seguridad, aunque sean programas libres de costos.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización o ser utilizados para fines ajenos a las funciones o poderes de la empresa.

7.0 NORMAS APLICABLES AL USO DE INTERNET.

- Los sistemas de comunicación y acceso a Internet son propiedad del Instituto Tecnológico de las Américas (ITLA) y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la empresa y nunca con fines no autorizados o para actividades personales.
- Las operaciones realizadas a través de Internet pueden generar responsabilidad por parte de las áreas del Instituto Tecnológico de las Américas (ITLA), por lo que los usuarios que tengan acceso a Internet no deberán emplearlas para información personal o uso de los accesos realizados a través de Internet. ITLA monitoreará y auditará los accesos realizados por los usuarios a través de su sistema de información, el acceso a Internet y el contenido de lo accedido para preservar la integridad de sus recursos.

8.0 NORMAS APLICABLES AL USO DEL CORREO ELECTRÓNICO.

- El sistema de correo electrónico es propiedad del Instituto Tecnológico de las Américas (ITLA) y es parte íntegra de sus sistemas de información, por lo que el mismo se reserva el derecho absoluto de intervenir, auditar e investigar para constatar el uso adecuado del mismo.
- Las operaciones realizadas por medio del correo electrónico pueden generar responsabilidad por parte del Instituto Tecnológico de las Américas (ITLA), por lo que los usuarios de las cuentas de correo electrónico no tienen expectativa de privacidad alguna con relación a la información contenida en dichas cuentas. Las cuentas están sujetas a auditorías y revisiones sin previo aviso por el personal autorizado.
- El correo electrónico podrá utilizarse únicamente para propósitos autorizados relativos a las funciones de trabajo. Se prohíbe el uso del mismo para otros asuntos o actividades personales en menoscabo de la imagen de la empresa o sus empleados.
- La empresa establecerá las normas mediante las cuales se asignan las cuentas de correo electrónico, incluyendo las medidas de seguridad aplicables, como son los códigos de acceso y las contraseñas y otros modos de autenticación, los controles de acceso a servidores, los

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

sistemas para auditar el uso del sistema, la integridad y seguridad de los datos y las comunicaciones enviadas.

- Durante horas laborables, los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de empresa, a menos que estén autorizados a tal uso.
- Con el propósito de mantener y hacer buen uso de nuestros recursos, los empleados deben revisar sus mensajes y documentos, y eliminar los que no sean necesarios.
- Los mensajes enviados deberán utilizar un lenguaje cordial, manteniendo la ética.
- Todo correo debe incluir la firma del remitente, en el cual se incluye: nombres y apellidos, cargo que desempeña en la empresa, dirección de correo electrónico, números contactos, dirección de oficina y dirección de sitio Web de la empresa.
- Se encuentra prohibido los mensajes que contengan comunicaciones con la intención de ofender o difamar, así como comentarios, caricaturas, chistes de carácter sexual o discriminatorio que puedan ser considerados como hostigamiento o falta de respeto hacia otras personas. También se consideran violaciones a esta política los mensajes tipos cadenas, pornografía, chistes, ventas personales, y de índole político o religioso.

9.0 DIVULGACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Cualquier actualización, modificación o cambio en las Políticas de Seguridad de la Información deben ser comunicadas a todo el personal del Instituto Tecnológico de las Américas (ITLA) a través de la Gerencia encargada de la supervisión de la seguridad.

CUMPLIMIENTO DE LA POLÍTICA

El incumplimiento de las políticas relacionadas a los sistemas de información podría conllevar sanciones. Las normas aquí establecidas deben interpretarse como complementarias a las Políticas de Seguridad de la Información. ITLA se reserva la facultad de comenzar los procesos administrativos, civiles o penales pertinentes a los actos cometidos, aunque los mismos no estén expresamente prohibidos en este documento, si dichos actos, directa o indirectamente, ponen en riesgo la seguridad, integridad y confiabilidad de la información, el equipo y los sistemas de información de la empresa. Tanto estas normas como las que sean aplicables, serán revisadas y actualizadas periódicamente, por lo que es responsabilidad de las áreas estar al tanto de las mismas y los usuarios el contenido de las mismas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

10.0 INFORME DE INCUMPLIMIENTOS O INFRACCIONES

Cualquier empleado o contratista que tome conocimiento de hechos o circunstancias que de acuerdo a un criterio razonable constituyan una violación o incumplimiento de las políticas, procedimientos o estándares establecidos, deberá informarlo inmediatamente al responsable de la Política. La Empresa investigará toda violación que sea denunciada/informada con los procedimientos de investigación establecidos, y basándose en los resultados de dicha investigación, tomará las medidas necesarias para subsanarlas o las acciones que considere apropiadas. Se mantendrá la confidencialidad de la investigación dentro del marco jurídico.

GLOSARIO

- **Acceso Lógico:** es un mecanismo que, a través de un elemento identificador y autenticador de usuarios, como, por ejemplo: nombre de usuario y contraseña, se provee la entrada a redes de computadoras, sistemas e información en una organización.
- **Acceso Remoto:** es una solución que permite que usuarios distantes tengan acceso a plataformas y servicios de una red organizacional.
- **Activo:** recurso del sistema de información o relacionado con éste, necesario para que la empresa funcione correctamente y alcance los objetivos propuestos por su dirección.
- **Activo de Información:** es una pieza definible de información, bien sean textos, documentos, archivos e información almacenados en archivos compartidos, bases de datos, programas, sistemas de aplicaciones, servicios y equipos utilizados para crear, acceder, almacenar y transmitir esta información, que independientemente del medio que lo pueda contener (por ejemplo, papel, disquete, CD-ROM y cinta magnética), es reconocida como valiosa para la organización.
- **Administración Basada en Roles:** es un sistema para controlar cuáles usuarios tienen acceso a recursos basados en el rol del usuario. Los derechos de acceso se agrupan por nombres de roles, y el acceso a los recursos se restringe a los usuarios que han sido autorizados para asumir el rol asociado. A cada usuario se le asigna uno o más roles.
- **Amenaza:** evento que puede desencadenar un incidente en la empresa, produciendo daños o pérdidas materiales o inmateriales en sus activos.
- **Autenticación:** la validación de autenticidad de muchos documentos legales, financieros y de otros tipos se determina por la presencia o ausencia de una firma manuscrita autorizada o

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

de una firma digital. La firma digital permite que una de las partes pueda enviar un mensaje firmado a la otra parte, con las propiedades de autenticación (íntegro, auténtico y no repudio).

- **Autorización:** es el proceso de aceptar o denegar el acceso de un usuario a los recursos de la red una vez que el usuario ha sido autenticado con éxito. La cantidad de datos y servicios a los que el usuario podrá acceder dependen del nivel de autorización que tenga establecido.
- **Brecha de Seguridad (sinónimo agujero de seguridad):** como su nombre lo indica, una brecha es una apertura que puede permitir el acceso de terceros no autorizados.
- **Certificación:** el proceso a través del cual una entidad de confianza confirma la autenticidad de la identidad de un usuario.
- **Certificación Electrónica:** es el proceso a través del cual una entidad de confianza confirma la autenticidad de la identidad de un usuario utilizando un medio electrónico o digital. La Autoridad de Certificación (Certification Authority-CA) es una entidad de confianza, reconocida y aceptada por todos, muy difícil de suplantar.
- **Certificado Electrónico:** es el mensaje de datos proporcionado por un proveedor de servicio de certificación que le atribuye certeza y validez a la firma electrónica.
- **Confidencialidad:** se refiere a garantizar que la información esté accesible sólo a personas autorizadas a tener acceso según sus roles, responsabilidades y funciones asociadas la Organización.
- **Correo Electrónico:** es un servicio automatizado cuya funcionalidad es similar a la del correo regular, pero utilizando los equipos de computación y una aplicación que permiten enviar mensajes o paquetes a otro usuario o grupo de personas a una dirección específica a través de la red interna de una Organización o Internet.
- **Contraseña:** en algunas aplicaciones aparece denominada como password proveniente del idioma inglés, es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto y es intransferible.
- **Control:** práctica, procedimiento o mecanismo que reduce el nivel de riesgo en plataformas, sistemas o aplicaciones.
- **Control de Acceso:** mecanismo que en función de la identificación ya autenticada que permite acceder a datos o recursos.
- **Control de Cambios:** es un proceso que se lleva a cabo cuando se desea realizar algún cambio en el ambiente operacional de la Organización, estos cambios pueden ser: actualizar una aplicación, incorporar dispositivos, cambian una versión de Sistema Operativo, entre otros. El Control de cambios persigue asegurar la integridad de las operaciones y prevenir cualquier alteración que pueda afectar la continuidad de las operaciones.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- **Cortafuegos:** (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.
- **Criptografía:** es la ciencia de mantener la información segura a través de mecanismos de escritura oculta, la criptografía es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.
- **Dueño de Información/activo/sistema:** es la unidad o persona responsable por dicho recurso, quien tiene la responsabilidad de definir quienes tienen acceso al mismo y con qué niveles de privilegios (lectura, escritura, modificación, impresión).
- **Evento/Incidente de Seguridad:** cualquier hecho o evento que podría afectar a las operaciones de la Empresa o poner en riesgo a los empleados, recursos tecnológicos o prestigio de la misma.
- **Firma Electrónica:** es una técnica que se basa en la criptografía de clave pública para asegurar que un mensaje no sea manipulado.
- **Firma Digital:** es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel.
- **Identificación:** este tipo de servicio corresponde a la determinación de la identidad real del usuario que opera el sistema; es decir, se intenta definir si realmente la persona es quien dice ser. Existen diversas tecnologías para reforzar los esquemas de identificación.
- **Identificación Basada en Tokens:** identificación de usuario utilizado para proteger la información o la identidad. A diferencia de las soluciones de seguridad basadas en software, este tipo de identificación como las tarjetas inteligentes se consideran como un token tipo hardware.
- **Smart Card:** son tarjetas que contienen la información del usuario y generalmente su contraseña; el riesgo de utilizar este tipo de sistemas es el robo de la tarjeta, lo que permitiría una fácil suplantación del usuario.
- **Impacto:** consecuencia sobre un activo de la materialización de una amenaza.
- **Incidente:** es cualquier evento que represente un riesgo para la continuidad de las operaciones o que pueda alterar la confidencialidad, integridad o disponibilidad de la información utilizada para la realización de las actividades de una Organización.
- **Integridad:** consiste en mantener la información sin alteraciones o modificaciones no autorizadas.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- **Internet:** Término utilizado para hacer referencia a la red de mayores dimensiones del mundo, conectando miles de redes en todo el mundo. El Internet surgió del ARPANET.
- **Norma:** es un documento técnico que contiene una especificación que debe ser cumplida.
- **Norma ISO:** son estándares publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que sirven de referencia como mejores prácticas recomendadas para diversas áreas.
- **Procedimiento:** es el modo de ejecutar determinadas acciones, con una serie de pasos claramente definidos, que permiten realizar una actividad determinada.
- **Procedimientos de Respuesta a Incidentes:** es el proceso de responder ante un evento de seguridad que atente contra la continuidad de las operaciones de la organización, contar con procedimientos documentados y alineados a los requerimientos de la empresa, ayudará a minimizar la pérdida de recursos tales como datos, tecnología, activos de capital, ingresos, clientes, accionistas, entre otros.
- **Propiedad Intelectual:** supone el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano.
- **Respaldo de Información:** consiste en realizar una copia de la información que se encuentra en el ambiente operativo de una Organización, la misma sirve de resguardo en caso de daño o alteración de la versión original que se encuentra en uso.
- **Restauración:** es el proceso de devolver un sistema o información a su estado original antes de sufrir algún daño o alteración.
- **Riesgo:** es la probabilidad de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas a un activo de información, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene de acuerdo a la criticidad del activo y su probabilidad de ocurrencia.
- **Servidor:** es una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de un ordenador y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.
- **Sistema Críticos:** se considera un sistema como crítico cuando su caída o interrupción afecta la continuidad de las operaciones de una organización.
- **Sistemas de Detección/Prevención de Intrusos (IDS/IPS):** una vez que el firewall permite la entrada de tráfico a la red puede ser que éste sea regular o malicioso; más aún, puede ser

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

que en el tráfico interno de la red circule código malicioso. Este tipo de tráfico debe ser analizado con sistemas especiales como los sistemas de detección de Intrusos (IDS), el cual permite, sobre la base de reglas predefinidas, detectar y notificar el flujo de dicho código para poder tomar acción en cuanto esto suceda.

Adicionalmente, en muchas ocasiones, el atacante enmascara el ataque en tráfico permitido por el firewall con el objetivo de explotar las vulnerabilidades de los diferentes sistemas dentro de una red y utilizarlas como caminos para realizar los ataques por lo que se requiere de un IDS para detectarlo.

Un IDS se encuentra en constante actividad revisando todo el tráfico que fluye por la red corporativa, así como el que sale o llega de Internet a fin de alertar sobre la existencia de paquetes que pudieran comprometer las operaciones de la empresa o inclusive llegar a bloquear transacciones maliciosas.

- **Sistemas de Gestión de Actualizaciones:** permiten a los administradores de las Tecnologías de Información implantar las últimas actualizaciones de software (aplicaciones y sistemas operativos) de forma automática y centralizada a los equipos de una red.

Con el objeto de corregir vulnerabilidades detectadas por los escáneres de vulnerabilidad o reportadas por los fabricantes.

Se debe incluir la obligatoriedad de pruebas preliminares en sistemas operativos a fin de garantizar que la corrección no cause nuevas vulnerabilidades en los mismos.

- **Sistema de Información:** es un conjunto organizado de elementos que están diseñados para procesar datos y proporcionar información que apoyen la toma de decisiones.

- **Sistema Operativo:** son aplicaciones o Software diseñado para controlar el hardware de un sistema específico de procesamiento de datos con el objetivo de que los usuarios y los programas de aplicación puedan usar con facilidad dicho hardware.

- **Software:** son aplicaciones que permiten la operación de los equipos de cómputo o hardware, igualmente, permiten realizar procesos de negocio de forma automatizada.

- **Recursos Tecnológicos:** es cualquier elemento que conforme la red interna: estaciones de trabajo, servidores, cables, dispositivos, periféricos, elementos de seguridad, componentes de la red, entre otros.

- **Trazas de Auditoria:** se refiere al registro que se genera cuando cualquier usuario realiza una actividad en una aplicación cliente-servidor, estación de trabajo, sistema informático, servidor y cualquier recurso tecnológico.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: MC-TI-01
		VERSIÓN: 1

- **VPN (Virtual Private Network):** es la interconexión de un conjunto de computadores haciendo uso de una infraestructura pública (regularmente Internet), normalmente compartida, para simular una infraestructura dedicada o privada.
- **Vulnerabilidad:** es una debilidad de seguridad o brecha de seguridad, que indica que un activo de información es susceptible daños a través de ataques intencionales o fortuitos.