POLÍTICAS Y LINEAMIENTOS DE SEGURIDAD INFORMÁTICA DE LA UNIVERSIDAD TECNOLÓGICA DE TABASCO

	Elaboró:	Revisó:	Autorizó:
Puesto	Director de Informática	Abogado General	Rector
Firma			
Nombre	Lic. Jorge Luis Hernández Vicencio	Lic. Carolina Belen Camargo Ruiz	Dr. Lenin Martínez Pérez

Este documento describe las políticas y normas de todos los sistemas de computación y comunicaciones usados por la Dirección General del Sistema Estatal de Informática

ÍNDICE

Este documento describe las políticas y normas de todos los sistemas de computación y comunicaciones usados por la Dirección General del Sistema Estatal de Informática

Este documento describe las políticas y normas de todos los sistemas de computación y comunicaciones usados por la Dirección General del Sistema Estatal de Informática

1. INTRODUCCIÓN

1.1. ALCANCE Y FUNCIÓN DEL MANUAL

Este documento cuenta con las políticas y lineamientos para su aplicación por todas las áreas de Tecnologías de la Información de la Universidad Tecnológica de Tabasco, incluyendo prestadores de servicios, los proveedores y todos los sistemas informáticos y de comunicaciones utilizados por los servidores públicos de esta Universidad.

Estos sistemas incluyen las redes de área local, las computadoras personales (PC) y demás sistemas administrativos, los centros de procesamiento locales de cómputo, de telecomunicaciones y de conmutación, los proveedores de servicios de Internet (ISP) y otros proveedores externos de servicios de información.

1.2. APLICACIÓN DE LOS ESTÁNDARES

El presente manual está basado en la norma Internacional ISO/IEC 27001:2005 que comprende el Sistema de Gestión de la Seguridad de la Información.

El término **"debe"** se utiliza claramente en todos los lineamientos para identificar los controles de seguridad informática requeridos en todas las áreas donde sean utilizadas las Tecnologías de Información y comunicaciones de voz IP o tradicional en sistemas híbridos.

En forma excepcional, la Dirección de Informática puede decidir no aplicar estos lineamientos en ciertas circunstancias, sin embargo, debe justificarse dicha excepción en función de una evaluación de los riesgos.

La Dirección de Informática es la responsable de mantener actualizadas las políticas y lineamientos, así como su publicación.

Todas las funciones directivas que responden por el uso de los equipos y de los sistemas de TI comparten esta responsabilidad por los recursos y operaciones bajo su control. En este documento, el término **"dirección"** corresponde a las unidades administrativas responsables de que se cumplan estas políticas y lineamientos.

1.3. REVISIÓN

Estas políticas y lineamientos serán revisados una vez cada seis meses o antes si existiera algún cambio de las responsabilidades de la seguridad de la información o significativo en los estándares internacionales, y si fuera necesario, se publicarán nuevamente.

2. POLÍTICA DE SEGURIDAD INFORMÁTICA

2.1. DEFINICIÓN TÉCNICA

La Seguridad Informática implica la protección de la información en términos de:

a) **Confidencialidad**: divulgar información sólo a las personas y los procesos autorizados;
b) **Integridad**: garantiza la exactitud e integridad de la información;
c) **Disponibilidad**: asegura el acceso y la utilización oportunos de la información y los sistemas de información como se requiera, y la protección de los equipos, software y demás activos de tecnología informática.

2.2. ALCANCE

Esta política se aplica a todos el personal administrativo, docente, alumno y proveedores, sistemas informáticos, software, documentación o información, equipos y demás recursos de Tecnologías de la Información.

2.3 INVENTARIO DE ACTIVOS

Se debe llevar un inventario centralizado y actualizado de los recursos de Tecnología de Información de la institución, así como contar con mecanismos de control según el tipo de información que contienen, procesan, transfieren, transportan o almacenan.

2.4 USO ACEPTABLE DE ACTIVOS

Todos los servidores públicos, contratistas y terceras partes son responsables de seguir las reglas existentes para el buen uso de la información y activos asociados con el procesamiento de dicha información.

Se debe contar con un procedimiento de restauración y resguardo de información para el uso aceptable de los activos de información.

2.5. CLASIFICACIÓN DE LA INFORMACIÓN.

Los activos informáticos deben estar clasificados con base al impacto que representan en la institución, y además en sus propiedades de seguridad como confidencialidad, disponibilidad e integridad.

Los dueños de los activos de información deben responsabilizarse de las necesidades de la institución para clasificar, valuar y compartir o restringir información, así como del impacto asociado a estas necesidades.

Para la incorporación de activos de información al inventario, se debe asignar una clasificación de seguridad y debe ser proporcionada por el dueño del activo.

2.6. ADMINISTRACIÓN DE RIESGOS

La Dirección de Informática debe generar una matriz de riesgos para sus activos de información.

El objetivo principal de la administración de riesgos es de disminuir el impacto de los eventos potenciales que pueden afectar el alcance de los objetivos de la Universidad materia de TIC.

Los controles de Seguridad Informática deben integrarse en una matriz donde se considere el costo de inversión, costo de operación y valor de la información a resguardar y demás activos en riesgo, considerando el riesgo por el daño que pudiera derivar de las violaciones potenciales de la seguridad.

2.7. RESPONSABILIDADES ADMINISTRATIVAS

La Dirección debe determinar las responsabilidades explícitas para implementar, operar y administrar los controles de Seguridad Informática.

2.8. DISCIPLINA INTERNA

Las políticas y lineamientos de Seguridad Informática deben cumplirse en todo momento. Cualquier incumplimiento será tratado de acuerdo con los procedimientos disciplinarios dispuestos por la Universidad.

2.9. CAPACITACIÓN DEL PERSONAL EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de Informática debe considerar en su plan de trabajo el proporcionar a los responsables de Tecnologías de la Información y Comunicaciones, programas de concientización, educación y capacitación adecuados en función de las necesidades, para que estos a su vez lo transmitan hacia los usuarios de los activos de información.

El personal debe recibir capacitación periódica (1 vez al año) que lo concientice sobre problemas de seguridad de la información.

Los usuarios deben recibir capacitación periódica (1 vez al año) que los concientice a una cultura de seguridad de la información.

Deben existir métodos que permitan afianzar la cultura de seguridad en el personal como:

1) Correos electrónicos.
2) Promover videos institucionales.
3) Promover pláticas de seguridad
4) Promover carteles o trípticos en materia de seguridad.

2.10. ESTÁNDARES TÉCNICOS Y ADMINISTRATIVOS

Los controles de seguridad informática deben cumplir con las normas de control básico y de los entornos específicos de la Dirección de informática. La Dirección podrá complementar estas políticas y lineamientos con normas del Gobierno del Estado de Tabasco adicionales.

2.11. IMPLEMENTACIÓN

A fin de implementar controles de seguridad informática que sean efectivos y eficaces, la política de la Dirección de Informática es:

a) Implementar un conjunto coherente y equilibrado de controles de prevención, detección y recuperación;
b) Implementar controles complementarios, y que se refuercen mutuamente, en todos los sistemas y actividades interrelacionadas. Debe evitarse el depender en un solo nivel de controles;
c) Automatizar los controles, cuando sea posible y se justifique el costo;
d) Simplificar los controles y reducir la variedad y complejidad de las herramientas de seguridad cuando sea posible y se justifique el costo.

3. RESPONSABILIDADES DEL ÁREA DE SOPORTE Y REDES EN EL ASPECTO DE SEGURIDAD INFORMÁTICA

3.1. PRINCIPIOS GENERALES

Todos los directivos y el personal tienen la responsabilidad de proteger la seguridad de los activos y de los recursos de TI bajo su control, de acuerdo con las instrucciones y la capacitación recibidas. Deben definirse responsabilidades expresas para la implementación, operación y administración de los controles de seguridad informática y deben discriminarse dichas responsabilidades de aquéllas que sean incompatibles cuando esto pudiera debilitar el nivel del control interno en forma inaceptable.

3.2. EXCEPCIONES

Si la Dirección no implementa ningún aspecto de estas normas debe:

a) Considerar e implementar controles compensatorios pertinentes;
b) Consultar al Departamento de soporte y redes a fin de identificar y de documentar claramente la aceptación de cualquier aumento consiguiente de los riesgos;
c) Informar la decisión tomada a Dirección de Informática.
d) Documentar y retener, para su inspección, suficiente información para justificar la decisión y medidas tomadas en vista de los riesgos propios, incluyendo las evaluaciones de riesgos documentadas.

3.3. RESPONSABILIDADES

a) Desarrollar, revisar y actualizar las políticas y normas.
b) Acordar las prioridades de seguridad informática de la Dirección de Informática;
c) Coordinar la implementación de las políticas y normas del Área de Seguridad
d) Informática de la Dirección de Informática;
e) Monitorear e informar sobre el trabajo de seguridad informática a la Dirección;
f) Dar asesoramiento sobre la seguridad física de todas las instalaciones de la Dirección de Informática;
g) Investigar los aspectos penales de las violaciones de la seguridad informática, cuando sea necesario.
h) Garantizar que la seguridad de todos los activos de TI esté debidamente protegida;
i) Garantizar que se le dé la prioridad correspondiente al trabajo de seguridad informática, de manera oportuna, en todos los proyectos de TI.

3.4. PERSONAL

Todos los servidores públicos son responsables de:

a) Cumplir con las instrucciones y los procedimientos de seguridad aprobados y aquellas responsabilidades de seguridad específicas documentadas en los objetivos personales y la descripción de tareas;

b) Mantener la confidencialidad de las contraseñas personales y evitar que terceros utilicen los derechos de acceso de los usuarios autorizados;
c) Proteger la seguridad de los equipos de cómputo, así como de la información bajo su control directo;
d) Informarle a la directiva inmediata o de seguridad cualquier sospecha de violaciones de la seguridad y de cualquier debilidad detectada en los controles de la misma, incluyendo sospechas de divulgación de contraseñas.

4. EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA.

4.1. PRINCIPIOS GENERALES

Los objetivos de la evaluación de riesgos son identificar y establecer las prioridades de los riesgos de Seguridad Informática desde la perspectiva del servicio al público, y planear las acciones necesarias para reducir dichos riesgos a un nivel que sea aceptable para la Dirección. Por lo tanto, debe llevarse a cabo una evaluación de riesgos cuando éstos no sean claros o acordados, a fin de aclarar los requisitos de control y las prioridades de administración de Seguridad Informática:

a) Daño potencial que pudiera surgir de una violación seria de la seguridad informática;
b) La probabilidad real de que ocurra dicha violación, teniendo en cuenta las amenazas imperantes y los controles complementarios individuales de los controles técnicos.

4.2. EVALUACIÓN DE LOS RIESGOS DE SEGURIDAD INFORMÁTICA

Se podrán aplicar las técnicas de gestión de riesgos a todos los sistemas informáticos o a los servicios o componentes individuales de los sistemas, cuando sea posible y conveniente.

El proceso de evaluación de riesgos debe considerar:

a) La importancia de la información, de los equipos, del software y de otros activos del sistema informático en cuestión;

b) Las actividades de la organización, los productos y servicios respaldados por los sistemas informáticos en cuestión;
c) El daño que pueda causarse como consecuencia de una violación seria de la seguridad de la información.
d) La probabilidad real de que ocurra dicha violación, teniendo en cuenta los controles existentes y las amenazas imperantes, el entorno en el que se utiliza o funciona el sistema, y la vida útil real de la información en cuestión;
e) Los controles adicionales requeridos para reducir los riesgos a un nivel aceptable;
f) Las acciones necesarias para implementar y aplicar los controles adicionales correspondientes. Si la Dirección considera que los riesgos identificados por esta evaluación son inaceptables, y estos no se pueden evitar ni reducir satisfactoriamente a través de métodos más efectivos, entonces se deben planificar e implementar mejoras en la seguridad informática.

4.3. REEVALUACIÓN

Deben analizarse los riesgos generales de seguridad informática anualmente a fin de tener en cuenta los requerimientos cambiantes, las amenazas y prioridades de la Dirección Informática. Deben registrarse las conclusiones de esta revisión y las mejoras efectuadas a los controles planificados, según sean necesarias y pertinentes.

5. SEGURIDAD DEL PERSONAL

5.1. PRINCIPIOS GENERALES

Los servidores públicos cumplen una función esencial al apoyar los controles efectivos de seguridad informática. La Dirección debe asegurarse de que los servidores públicos estén debidamente equipados y sean adecuadamente supervisados para contribuir a dicha función.

5.2. SELECCIÓN

A fin de reducir los riesgos potenciales debido a la existencia de servidores públicos de TI deshonestos, los procedimientos de selección de personal deben, en tanto sean adecuados para la función y para el candidato en cuestión y antes de que se realice alguna oferta de trabajo:

a) Recabar referencias;
b) Confirmar la veracidad del currículum vitae y de sus calificaciones;
c) Realizar verificaciones adicionales para puestos particularmente críticos.

5.3. DURANTE EL DESEMPEÑO DE SUS FUNCIONES

Durante el desempeño de sus funciones:

a) Los servidores deben estar familiarizados con los procedimientos de seguridad de la Dirección de Informática y estampar su firma de aceptación y entendimiento de los mismos;
b) Cuando corresponda, las descripciones de los puestos y los objetivos personales deben identificar las responsabilidades específicas de seguridad informática;
c) La Dirección no debe confiar excesivamente en las habilidades y los conocimientos de personas determinadas para la operación de controles importantes;
d) La administración debe documentar las autorizaciones de acceso de los servidores públicos a los sistemas. Las reglas de control de accesos basadas en las funciones facilitarán este proceso.
e) Cuando se transfiere a un empleado a otra área, el servidor público que realiza dicha transferencia deberá verificar que todos los derechos de acceso a los sistemas existentes, así como los demás controles de seguridad pertenecientes al empleado transferido, han sido cancelados. El área a la que se transfiere al empleado deberá implementar nuevos controles y la Dirección debe informar al área administrativa de seguridad informática que corresponda sobre cualquier transferencia de personal.

5.4. CONTRATOS DE SERVICIO

Debe exigírsele al personal contratado para suministrar bienes o prestar servicios de informática que cumplan con las normas y políticas de seguridad informática de la Dirección de Informática correspondientes.

5.5. HIGIENE Y SEGURIDAD

La Dirección debe tener en cuenta medidas de higiene y seguridad adecuadas para el personal en relación con los equipos de computación, así como también cumplir con la legislación respectiva.

5.6. MEDIDAS DISCIPLINARIAS Y SUSPENSIONES

Deben tenerse en cuenta los procedimientos disciplinarios de la Dirección cada vez que se omitan o utilicen incorrectamente los controles de seguridad informática, y la Dirección debe notificar a la Dirección de Administración y Finanzas o equivalente cualquier caso que ocurra. Si se aplican procedimientos disciplinarios contra un empleado, la Dirección debe considerar la suspensión de los derechos de acceso a los sistemas y las responsabilidades de seguridad respectivas hasta que el problema se haya resuelto satisfactoriamente.

5.7. TERMINACIÓN DE CONTRATO

Al momento de notificar la terminación del contrato de un empleado por cualquier motivo y en cualquier circunstancia, la Dirección de Administración y Finanzas debe considerar y cuando corresponda garantizar que:

a) Elimine los derechos de acceso a los sistemas, cuentas de correo electrónico, acceso a Internet, aplicativos y demás oportunidades en las que pueda existir un uso no autorizado de los sistemas de la Dirección de Informática.
b) Informar a la Dirección de Informática sobre cualquier terminación de contrato de personal;

c) Si representa un riesgo significativo para los sistemas de la Dirección de Informática, el empleado será llevado fuera de las instalaciones de la Dirección de Informática y se le denegará el acceso a las mismas en el futuro, además, que se recuperará e inhabilitará cualquier pase de acceso físico que le haya sido emitido;
d) Se deberán de remover los controles de acceso del empleado o terceros contratados como son:
   d.1) Accesos físicos a la institución
   d.2) Acceso a servicios de red
   d.3) Se recuperará y resguardará el software, los equipos, manuales y demás documentación de informática;
   d.4) Cuando se le permita al empleado continuar con sus funciones, se le seguirá vigilando para detectar cualquier actividad o comportamiento inusual. La Dirección debe considerar la necesidad de aumentar la supervisión de dicho empleado en estas circunstancias.

5.8 IDENTIFICACIÓN DE RIESGOS RELACIONADO CON TERCEROS

Se debe realizar un análisis de riesgos de seguridad entes de establecer una relación de negocios con alguna entidad externa.

Al ser detectado un incidente de seguridad por parte de terceros, se debe de notificar a la contraparte correspondiente de la Dirección

Los accesos de terceros a servicios de la Dirección de Informática (red, aplicaciones, equipos e información) deben estar autorizados por los responsables correspondientes.

6. SEGURIDAD FÍSICA

6.1. PRINCIPIOS GENERALES

Las instalaciones con fines específicos que alberguen equipos críticos requieren una mayor protección que la proporcionada a las oficinas comunes. Debe considerarse a todas las funciones de IT y al material relacionado como confidencial y protegerlos de manera acorde.

6.2. CONSTRUCCIÓN Y EMPLAZAMIENTO DE INSTALACIÓN DE TI

Las instalaciones de TI deben ser ubicadas y diseñadas de forma tal que se reduzcan los riesgos resultantes de desastres naturales, los inherentes a la zona circundante, y riesgos de otra naturaleza, y no deben llamar la atención innecesariamente sobre dicha finalidad.

Siempre debe solicitarse el consejo de los asesores en construcción, prevención de incendios y seguridad que correspondan, y cumplir con sus recomendaciones, incluyendo también los requerimientos legales y los códigos de prácticas correspondientes.

En la medida de lo posible, las instalaciones de TI deberán emplazarse y construirse a fin de reducir:

a) El acceso directo público o el acercamiento directo de vehículos;
b) El riesgo de inundaciones y otros peligros inherentes a la zona circundante y el medio ambiente;
c) La cantidad de vías de acceso a las instalaciones, contando con áreas de entrega, carga y depósito controladas por separado;
d) Los riesgos potenciales en el suministro de energía eléctrica, agua y de servicios de telecomunicaciones.

6.3. PROTECCIÓN CONTRA INCENDIO Y EXPLOSIÓN

Las medidas de prevención de incendios y explosiones deben incluir:

a) Las medidas de prevención de incendios en los planos de las instalaciones, tan pronto comience la construcción de las mismas;
b) La implementación de las recomendaciones correspondientes hechas por los fabricantes de los equipos;
c) Además de los dispositivos manuales esenciales, la instalación de sistemas automáticos de detección y extinción de incendios, los cuales deben ser supervisados las 24 horas del día siempre que sea posible;
d) El probar con regularidad los sistemas de advertencia de incendios de acuerdo con la recomendación técnica especializada. Debe hacerse un registro de dichas pruebas;
e) La capacitación adecuada en el uso de los equipos de extinción de incendios. Todo procedimiento relacionado debe ser documentado, evaluado, publicado y puesto en práctica;
f) La eliminación de material inflamable, por ejemplo, papeles y artículos de papelería de desecho, de los centros de cómputos o equipos de computación, o de otros lugares que representen un peligro potencial de incendio, a menos que se lo requiera para el trabajo programado.

6.4. PROTECCIÓN CONTRA DAÑOS PROVOCADOS POR EL AGUA

Para proteger los equipos contra el agua se debe utilizar sistemas de alarma, contar con techos y pisos impermeables y un sistema de drenaje adecuado.

6.5. CONTROL AMBIENTAL

La temperatura, la humedad y la ventilación dentro de las instalaciones que albergan equipos de computación y de comunicaciones y medios de almacenamiento de información debe cumplir con las normas técnicas estipuladas por los fabricantes de los equipos. Cuando sea necesario, debe vigilarse la calidad ambiental y tomar las medidas correctivas pertinentes.

6.6. SUMINISTROS DE ENERGÍA ELÉCTRICA

Los suministros de energía eléctrica deben cumplir con las normas técnicas estipuladas por los fabricantes de los equipos. Cuando sea necesario, debe vigilarse la calidad del suministro de energía eléctrica y tomar las medidas correctivas pertinentes.

Debe proporcionarse a los sistemas críticos una fuente alternativa de energía eléctrica adecuada, por ejemplo, generadores de reserva, y si fuera necesario, una fuente ininterrumpida de energía eléctrica (UPS). Deben probarse periódicamente las fuentes alternativas de energía eléctrica.

6.7. CONTROLES DE ACCESO FÍSICO

Debe protegerse la seguridad física de las instalaciones y del personal de TI mediante los siguientes controles:

a) Colocar los equipos de TI dentro de los perímetros de las áreas de seguridad mismas que deben ser vigiladas todo el tiempo y a las cuales solamente se le permitirá el acceso al personal autorizado. Registrar toda entrada y salida de las áreas de seguridad de informática. Los perímetros deben ser seguros hasta el grado que sea pertinente para los activos en riesgo, y deben seguir siendo protegidos y controlados cuando el área de seguridad esté desocupada;
b) Siempre que sea posible, se utilizará sistemas automatizados de control de acceso físico. Toda alternativa debe ser acordada, debiendo documentarse la decisión tomada;
c) Los controles de acceso deben garantizar que solamente el personal autorizado pueda acceder a las áreas de seguridad. Dicho acceso debe ocurrir solamente cuando exista la "necesidad de entrar".
d) Revisar las autorizaciones de acceso al menos cada seis meses, y revocarlas inmediatamente cuando ya no sean necesarias;
e) Los servidores públicos deben portar una identificación visible dentro de los perímetros de las áreas de seguridad;
f) Cuando corresponda, deben mantenerse en secreto los códigos de acceso de las cerraduras digitales, los cuales deben cambiarse periódicamente y cada vez que un miembro del personal ya no necesite tener acceso;

g) La Dirección debe considerar la utilización de alarmas que detecten el ingreso no autorizado de personas mediante coerción a las áreas de seguridad, y protejan al personal vulnerable.

6.8. VISITANTES

La definición de visitante incluye a todo empleado para el cual una oficina determinada no es su lugar habitual de trabajo. Los procedimientos aplicados para la recepción de todos los visitantes en las instalaciones u oficinas de TI deben:

a) Estar centralizados en una sola área controlada;
b) Siempre que sea posible, se debe recibirlos fuera del perímetro del área de seguridad.
c) Si esto no fuera posible, debe ubicarse la recepción de forma tal que se reciba a los visitantes antes de que éstos tengan acceso a las instalaciones de TI;
d) Confirmar y registrar efectivamente las identidades de los visitantes, las organizaciones a las que representen, y el objetivo de su visita antes de ser admitidos;
e) Registrar las fechas y horarios de entrada y salida;
f) Proporcionar a los visitantes gafetes distintivos, los cuales deberán portar durante su visita, y proporcionarles instrucciones básicas de seguridad y de prevención de incendios.
g) Garantizar que los visitantes estén bajo observación y sean supervisados durante su visita, en función de los riesgos;
h) Minimizar el acceso de los visitantes a las áreas de seguridad.

6.9. POLÍTICAS DE SEGURIDAD FÍSICA

Hacer del conocimiento de todo el personal de la Dirección de Informática las políticas de seguridad física, las cuales deben cumplirse por todo el personal de la Universidad.

Este documento está enfocado a todo el personal que labora en la Universidad y a externos que se encuentren en las instalaciones.

Incluye las políticas de seguridad física. Está dividido en las siguientes secciones:

- Sección A: Sobre las identificaciones de servidores públicos y visitas.
- Sección B: Sobre las visitas de externos
- Sección C: Sobre el resguardo de las zonas de trabajo.
- Sección D: Sobre los intentos de acceso no autorizado.
- Sección E: Sobre la salida de cómputo y comunicaciones.
- Sección F: Sanciones.

1. DEFINICIONES

Para facilitar la lectura y comprensión de este procedimiento, se consideran las siguientes definiciones:

a) Política: Decisión administrativa que determina la forma en la que serán interpretados los requerimientos de seguridad.
b) Política de Seguridad: Conjunto de reglas, leyes, criterios, y prácticas que regulan la forma de administrar, proteger y distribuir la información dentro y fuera de la organización.
c) Seguridad Física: Aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.

2. DESARROLLO

Sección A. Sobre las identificaciones de servidores públicos y visitas.

1) El área de Informática deberá entregar una tarjeta de control de acceso a cada servidor público la cual tiene como objetivo identificar al portador. Esta tarjeta debe ser usada en todo momento para acceder a las instalaciones de la Dirección de Informática

    a. Ver apartado Instrucciones para uso de credenciales.

2) Todos los servidores públicos deberán portar su credencial en un lugar visible y serán responsables de su tarjeta y del uso que se le dé. En caso de no contar con "porta- credencial" solicitarlo a la Dirección de Informática.

3) La credencial deberá mostrar la fotografía de la persona que la porta. No se permite pegar objetos en la tarjeta que no permitan ver la fotografía.
4) Si un usuario olvida su credencial en 3 ocasiones o más durante un mes será reportado a su jefe inmediato y en caso de reincidencia será sujeto de la sanción respectiva.
5) Si un usuario pierde su tarjeta deberá reportarla inmediatamente al área de la Informática.

Sección B. Sobre las visitas de externos.

1) Todas las visitas de externos deben ser escoltadas por las asistentes y/o por el servidor público que es visitado.
2) El visitante deberá registrarse en primera instancia en la recepción principal y esperar a que lo acompañe personal del área que visita. En caso de tratarse de una visita importante el servidor público podrá recibir al visitante desde la recepción.
3) Todos los asistentes deberán ser previamente notificadas a la visita de un externo y deberán registrar la ubicación, la persona que los acompañara y la hora de entrada y de salida del visitante.
4) El externo debe estar acompañado en todo momento por el servidor público a quien visitará desde que llega a las oficinas y hasta que concluya su visita, despidiéndolo en la recepción. Los externos no deberán quedarse sin escolta en ningún momento.
5) A ningún visitante se le permitirá acceder a ubicaciones restringidas o que no estén controladas. En caso de que un empleado sorprenda a un externo en esta situación deberá informar inmediatamente al área de la Dirección de Informática.

Sección C. Sobre el resguardo de las zonas de trabajo.

1) Todas las puertas de acceso a oficinas, sin excepción deben permanecer cerradas en todo momento.
2) En caso de una emergencia (terremoto, incendio, etc.) deben ser usadas las puertas de emergencia.
3) Las oficinas deben permanecer cerradas con llave cuando no se encuentren los directivos que las utilizan y nadie tendrá acceso a estas sin su consentimiento y la supervisión de su asistente.

4) No se permite mover equipos ni mobiliario de las salas de juntas y en caso de requerirlo debe notificarse previamente al responsable del área.
5) Se prohíbe hacer uso indebido de los recursos informáticos o de comunicaciones tales como equipo de cómputo, impresoras o teléfonos, Cualquier abuso será sancionado por la Dirección de Administración y Finanzas.
6) La persona que imparta un curso a externos será responsable de custodiar a los visitantes hasta que el curso haya concluido. El responsable no debe permitir que los visitantes accedan a áreas ajenas a las actividades del curso y debe cerrar todos los accesos cuando hayan finalizado las actividades.

Sección D. Sobre los intentos de acceso no autorizados.

1) Los servidores públicos no deben intentar ingresar a áreas restringidas en donde no tienen autorización. El empleado que sea sorprendido será sancionado.

   Las áreas restringidas son las siguientes:

Área	Acceso únicamente permitido
SITE de Informática	Personal operativo de la Dirección de Informática. Nota: Ningún externo o empleado que no sea personal operativo puede acceder al Site

2) Ningún usuario ni externo puede tener acceso al Site de Informática, edificio 1, vinculación, edificio 8, sin previa autorización del área responsable.

3) El término piggybacking se refiere a seguir a un usuario autorizado hasta un área restringida y acceder a la misma gracias a la autorización otorgada a dicho usuario. Al momento de que un servidor público ingresa por un control de acceso no debe permitir la entrada de otra persona sin autorización o de un compañero de trabajo sin tarjeta. Al empleado que se sorprenda permitiendo piggybacking será sancionado.

4) Las únicas personas que pueden permitir el acceso son las asistentes o el personal que reciba visitas -previa notificación- (Ver Sección B)

5) Las puertas de emergencia solo deben ser utilizadas como su nombre lo dice en caso de emergencia, cualquier abuso en su uso será sancionado.

Sección E. Sobre la salida de equipo de cómputo y comunicaciones.

2) Todo equipo de cómputo que sea propiedad del Universidad, podrá salir de las instalaciones únicamente con el formato de salida correspondiente y este deberá tener todas las firmas de autorización y visto bueno que se indican. Estos formatos deben solicitarlos a la Dirección de administrativa o de División el área de vigilancia deberá corroborar la salida.

Sección F. Sanciones

1) El incumplimiento de alguna de las políticas de seguridad física dará origen a una sanción emitida por la Dirección Administrativa.

6.10. VISITAS DE INGENIEROS Y PERSONAL DE SOPORTE TÉCNICO

Se requiere tomar medidas de prevención adicionales para los ingenieros y demás personal de soporte técnico de TI que visiten las instalaciones. Estas medidas se aplican a los visitantes que ingresan en las instalaciones de redes remotas, centros de cómputos descentralizados y sistemas de oficinas, además de los centros de datos. La Dirección debe considerar la necesidad de aplicar los siguientes controles:

a) Deben firmarse los acuerdos de confidencialidad pertinentes que cubran a los individuos y a las organizaciones que los emplean. El acceso de los ingenieros a la información confidencial debe ser el mínimo posible;
b) Los procedimientos aplicados al acceso de los ingenieros deben comprender también la notificación previa a la recepción sobre la visita de los mismos;
c) No se deberá habilitar permanentemente a los ingenieros y demás visitantes de soporte técnico para administrar los controles de seguridad informática de la Dirección de Informática, ya sean físicos o lógicos;
d) de ser necesario, deben hacerse copias de resguardo de la información antes que los ingenieros tengan acceso a los sistemas o los equipos;
e) al finalizar el trabajo de ingeniería, deben realizarse las verificaciones correspondientes, cuando sean necesarias, para confirmar que:
    i. se haya finalizado con éxito el trabajo autorizado;

ii. no siga existiendo ninguna información o software remanente que no sea de la Dirección de Informática;
iii. no haya habido ningún acceso no autorizado a los sistemas;
iv. la información y el software de la Dirección de Informática permanecen en su mismo estado, o que se los restableció a su estado original anterior al trabajo efectuado;
v. las computadoras personales no tienen virus;
vi. todas las contraseñas de acceso a los sistemas de ingeniería han sido modificadas e inhabilitadas;

f) no deben sacarse de la Dirección de Informática los medios magnéticos que contengan información confidencial, a menos que:
   i. se imposibilite su lectura primero, o
   ii. se los proporcione bajo un acuerdo de confidencialidad por escrito a un representante autorizado de una organización de servicios aprobada para ese fin.

6.11. EQUIPOS

Debe protegerse la seguridad de los equipos mediante las siguientes medidas generales:

a) deben guardarse los equipos bajo llave y asegurarlos cuando sean dejados sin supervisión. Cuando sea posible y adecuado para el riesgo, deben adaptárseles dispositivos contra manipulación indebida para minimizar la posibilidad de que el equipo sea removido o manipulado, que se instalen equipos en el área;
b) los equipos de seguridad, tales como los equipos de cifrado de datos, deben ser instalados siempre en gabinetes de seguridad;
c) se debe ubicar los equipos de manera que se reduzca el acceso innecesario del personal a las áreas de seguridad;
d) no deben ubicarse los monitores ni las impresoras cerca de las ventanas, ni colocarlos de forma tal que puedan ser fácilmente observados;
e) debe prohibirse el comer, beber y fumar, así como el uso de teléfonos móviles/celulares en los centros de cómputo;
f) los procedimientos deben garantizar que el mantenimiento de los equipos se lleve a cabo de acuerdo con las recomendaciones de los fabricantes;

g) no puede conectarse equipo alguno a los sistemas o redes de la red universitaria sin aprobación previa y, cuando se considere apropiado, bajo la supervisión de un empleado.

6.12. CABLES

Siempre que sea posible:

a) las líneas eléctricas y de telecomunicaciones deben ingresar en las instalaciones de forma subterránea, con instalaciones alternativas disponibles desde otra fuente y a través de una ruta de ingreso independiente;
b) los cables deben ser enrutados e instalados de manera que se evite cualquier interferencia o daños accidentales o deliberados;
c) los cables instalados en locales compartidos no deben estar al alcance de los otros locatarios.

6.13. MEDIOS DE ALMACENAMIENTO DE DATOS Y SOFTWARE

Deben protegerse los medios magnéticos mediante controles de seguridad física adecuados que incluyan el almacenamiento de la información o el software importante en gabinetes o cajas fuertes a prueba de fuego. Las instalaciones destinadas al almacenamiento de la información ubicadas en otros lugares deberán recibir el mismo nivel de protección física que aquéllas ubicadas dentro de las instalaciones de la Dirección de Informática.

6.14. ESCRITORIO DESPEJADO Y ENTORNO DE TRABAJO

Deben adoptarse las siguientes medidas a fin de proteger la seguridad de las áreas generales de oficinas:

a) cuando ya no se esté utilizando un equipo, por ejemplo, los sistemas de las oficinas, debe cerrarse la sesión y protegerlo para que no sea usado sin autorización;

b) al final de cada jornada deben apagarse todos los equipos portátiles, por ejemplo, las laptops, o bien restringir el acceso al software de los mismos. Para minimizar el riesgo de robo y la pérdida potencial de información personal o delicada, deben guardarse bajo llave y en un lugar seguro todos los equipos portátiles durante la noche.
c) deben guardarse en un lugar seguro las llaves de los escritorios, gabinetes, cajas fuertes y otras instalaciones de almacenamiento similares, y proceder de igual manera con los registros de las combinaciones de las cerraduras digitales y cualquier otra información delicada similar. Además, deben implementarse los procedimientos establecidos para la manipulación y el almacenamiento seguro de las llaves;
d) Fuera del horario de trabajo y cuando no se los utilice, deben guardarse en cajones o gabinetes con llave los documentos, papeles, disquetes, equipos de cómputo portátiles, teléfonos móviles y otros artículos similares;
e) los pisos deben mantenerse libres de cajas, paquetes, equipos excedentes, etc. para reducir los riesgos para el personal durante una evacuación de emergencia y en otras situaciones, por ejemplo, durante la búsqueda de paquetes sospechosos;
f) no debe colocarse la correspondencia confidencial en bandejas de salida después de la última recolección del día. No debe dejarse sin supervisión ninguna información confidencial en máquinas de fax o impresoras que no cuenten con dispositivos de seguridad.

6.15. ELIMINACIÓN DE DESECHOS Y OTROS MATERIALES

El material de desecho y los equipos excedentes de informática deben ser eliminados en forma segura. En particular:

a) la papelería membretada de la Dirección de Informática y los papeles que contengan información sobre la compañía (incluyendo el papel para listados) no deben ser reciclados como hojas de borrador fuera de las instalaciones;
b) debe borrarse toda información y software que permanezca aún en los equipos y dispositivos de almacenamiento de información, incluyendo las PC, los disquetes, CD- ROM y cintas magnéticas, antes que la Dirección de Informática los deseche, incluyendo, si se le considera esencial, la destrucción física de las unidades de almacenamiento de datos. Los CD que contengan información y software deben ser destruidos;

c) deben quitárseles todos los logotipos y marcas registradas de la Dirección de Informática a los equipos y las unidades de almacenamiento de datos antes de desecharlos;
d) los contratos celebrados para la eliminación del material confidencial deben poner como requisito la utilización de métodos seguros.

6.16. POLÍTICA PARA EL USO DE CONTRASEÑAS

Se debe proporcionar el correcto diseño y uso de nombres de usuario y contraseñas dentro del SITE de Informática, así como establecer un estándar para la creación de contraseñas fuertes o robustas, su resguardo y la frecuencia de cambio.

Esta política incluye a todo el personal de la Dirección de Informática que utilicé o sea responsable de una cuenta interna con acceso a herramientas o información confidencial, así como para consolas de operación y servidores dentro del SITE de Informática.

6.16.1 GUÍAS GENERALES

Las contraseñas NO deben tener las siguientes características:

a) Tener menos de 8 caracteres
b) Ser palabras de diccionarios comunes
c) Ser palabras comunes como:
   i. Nombre de familiares, mascotas, amigos, compañeros, etc.
   ii. Nombre de marcas, compañías, hardware, software.
   iii. Cumpleaños, y otra información personal como dirección o teléfono.
   iv. Cualquiera de las anteriores escribiéndolos al revés.
   v. Cualquiera de las anteriores seguida de un numero como secreto.

Las contraseñas robustas deberán seguir las siguientes características:

a) Tener caracteres en mayúsculas y minúsculas
b) Tener números y caracteres especiales .0-9, ¡@#$^&()+|~-=\´{}[]:";´<>?,./)
c) Utilizar al menos 8 caracteres alfanuméricos

d) NO utilizar información personal, nombre de familiares, etc.
e) NO utilizar el usuario como contraseña.
f) Las contraseñas NO deberán ser almacenadas en medios electrónicos.
g) Las contraseñas deben ser creadas de tal manera que se puedan recordar utilizando algún tipo de algoritmo relacionado.

6.16.2 RESGUARDO DE CONTRASEÑAS

No se deben compartir las contraseñas con ninguna persona, incluyendo asistentes o secretarias, todas las contraseñas deben ser tratadas como sensibles y confidenciales. Recomendaciones de resguardo:

a) Nunca revelar la contraseña a través de una conversación telefónica.
b) Nunca revelar una contraseña a través de un correo electrónico. Nunca hablar de una contraseña en frente de otras personas
c) Nunca revelar la contraseña a compañeros de trabajo en vacaciones, cada quien debe tener su cuenta propia.

6.16.3 BLOQUEOS POR EXCESO DE INTENTOS FALLIDOS

En donde la tecnología lo permita, se deberá implementar un control que límite a 8 intentos de acceso fallidos, después de los cuales se procederá a bloquear la cuenta en cualquiera de las dos formas siguientes:

a) Por espacio de una hora con opción a restablecerla mediante la solicitud expresa al administrador, si la tecnología lo permite.
b) De manera indefinida hasta que si el titular de la cuenta de acceso solicite el restablecimiento mediante el procedimiento autorizado.

6.16.4 ROTACIÓN PROGRAMADA DE CONTRASEÑAS

En donde la tecnología lo permita, se deberán establecer controles que automáticamente requieran al usuario el cambio de la contraseña cada tres meses bajo los siguientes parámetros:

a) La contraseña nueva no puede ser igual a la inmediata anterior ni a la segunda inmediata anterior.
b) La contraseña nueva debe cumplir la política de construcción aplicable.

Si por limitante tecnológica no es posible establecer un control automático, el cambio de la contraseña cada tres meses se hará por procedimiento estándar de operación.

TRANSITORIOS

PRIMERO. Las situaciones no previstas en los presentes políticas y lineamientos serán presentadas ante la Dirección de Informática.

SEGUNDO. Los presentes lineamientos entrarán en vigor al día siguiente de su aprobación.

TERCERO. Una vez que entren en vigor los presentes lineamientos difúndase en el Sistema Automatizado Integral de Información de las Universidades Tecnológicas.

Las presentes políticas y lineamientos fueron aprobados por el Rector de la Universidad Tecnológica de Tabasco, a los veintisiete días del mes de agosto del año dos mil veintiuno.