e.s.e | UNIVERSITARIA DEL ATLÁNTICO

DIRECCIÓN TICS

POLÍTICA

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Guía para los funcionarios y contratistas de la E.S.E.

Introducción

Objetivo:

- Introducir el tema y hacer entender la relevancia de la política de seguridad de la información.
- Capacitar a los funcionarios y contratistas para proteger los datos y cumplir con las normativas legales.

Importancia:

- **Protección de datos sensibles:** En la E.S.E., se maneja información altamente confidencial, como historias clínicas, datos financieros, y personales de pacientes y empleados.
- **Cumplimiento legal:** La Ley 1581 de 2012 y las resoluciones correspondientes obligan a las entidades públicas a cumplir estrictos lineamientos sobre protección de datos.

ADELANTOS

RESOLUCIÓN N° 0312 DEL 31 DE JULIO DEL 2023

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

RESOLUCIÓN N°0113 MARZO 4/2024

COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAMPAÑAS SOCIALIZACIÓN

CORREOS MASIVOS

Fundamentos Legales

LEY 1581 DE 2012:

Regula la protección de datos personales en Colombia.
Todos los funcionarios y contratistas deben conocer esta ley para garantizar que el manejo de la información se realice con respeto a la privacidad de los titulares de los datos.
Define los principios de tratamiento, como la legalidad, seguridad, acceso, y circulación restringida.

RESOLUCIÓN 500 DE 2021:

Dicta medidas de seguridad de la información específicas para entidades del Estado, obligando a las E.S.E.s a implementar políticas claras de seguridad.

RESOLUCIÓN 1519 DE 2020:

Establece pautas para la accesibilidad y transparencia en los sitios web, incluyendo cómo garantizar que la información personal sea segura en el entorno digital.

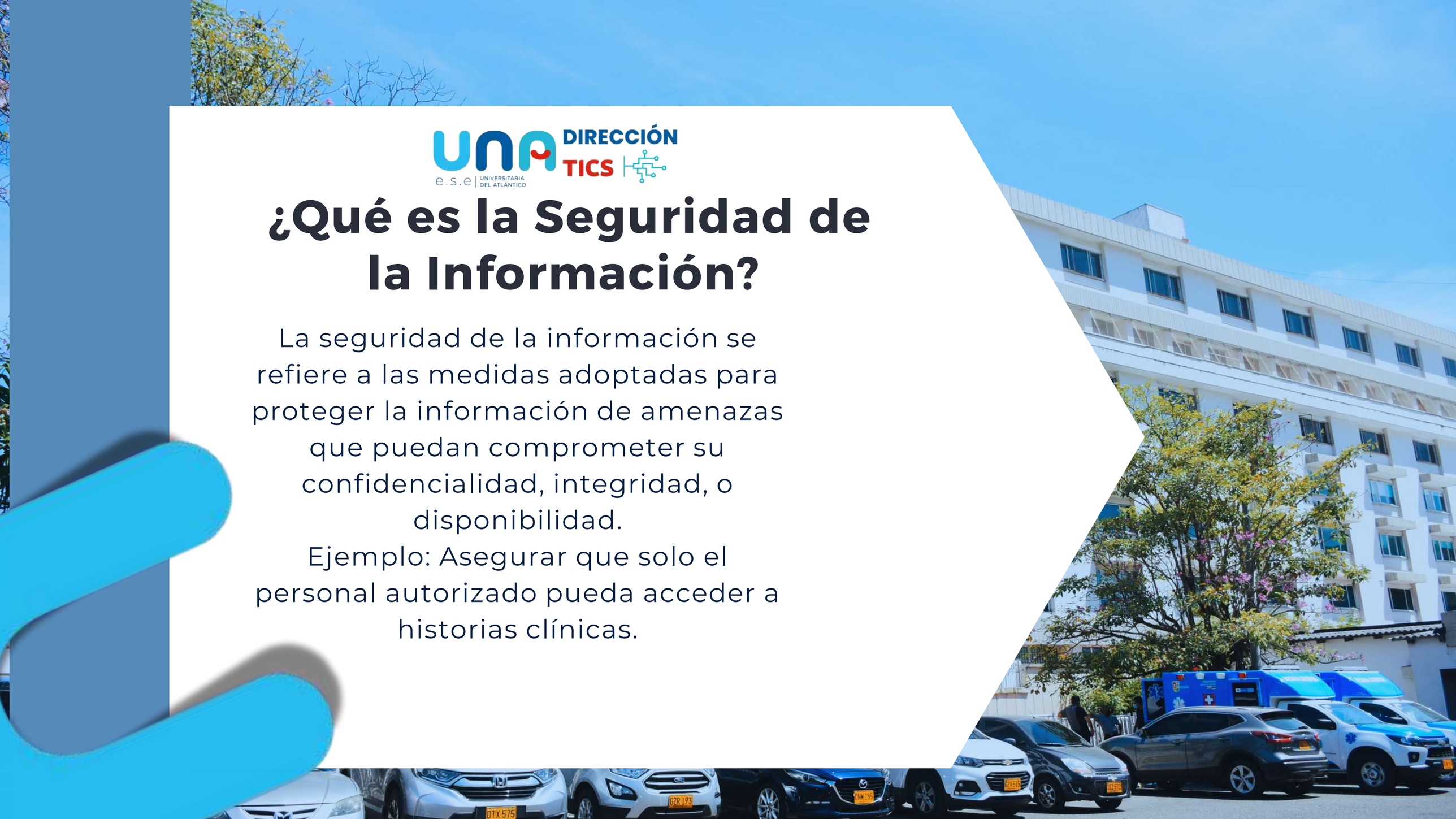
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO DIRECCIÓN TICS

¿Qué es la Seguridad de la Información?

La seguridad de la información se refiere a las medidas adoptadas para proteger la información de amenazas que puedan comprometer su confidencialidad, integridad, o disponibilidad.

Ejemplo: Asegurar que solo el personal autorizado pueda acceder a historias clínicas.



Datos importantes

01

SEGURIDAD

Se refiere a la protección de la información contra riesgos como accesos no autorizados, robos, daños o manipulaciones maliciosas. La seguridad se enfoca en la prevención de amenazas externas e internas que puedan comprometer la confidencialidad, disponibilidad e integridad de la información.

02

PRIVACIDAD

La privacidad se refiere al control que tiene un individuo sobre su información personal. Consiste en la capacidad de decidir quién puede acceder, utilizar y compartir su información y en qué circunstancias. Proteger la privacidad implica asegurar que los datos personales sean recopilados, almacenados y utilizados de manera legal y ética.

03

INTEGRIDAD

La integridad de la información se refiere a garantizar que los datos no han sido alterados de forma no autorizada o accidental. Asegura que la información es precisa, consistente y fiable, sin haber sido modificada de forma indebida. Mantener la integridad es fundamental para asegurar que la información sea creíble y útil.

Vulnerabilidad:

Una vulnerabilidad es una debilidad o fallo en un sistema, proceso o procedimiento que podría ser explotado por una amenaza para causar daño o pérdida de información. Las vulnerabilidades pueden surgir debido a errores humanos, fallas en la seguridad de un sistema o falta de actualizaciones en software, entre otros factores.

Amenaza

Una amenaza es cualquier circunstancia, evento o acción malintencionada que puede afectar la integridad, confidencialidad o disponibilidad de la información. Las amenazas pueden incluir virus informáticos, hackeos, robo de dispositivos, desastres naturales, entre otros eventos que representan un riesgo para la seguridad de la información.

Riesgo

El riesgo se refiere a la probabilidad de que una amenaza explote una vulnerabilidad y cause un daño a la información o al sistema. Es la combinación de la probabilidad de ocurrencia de un evento dañino y el impacto que dicho evento tendría en la organización. Identificar, evaluar y gestionar los riesgos es fundamental para proteger la información de forma efectiva.

Control:

Los controles son medidas o acciones implementadas para prevenir, mitigar o reducir los riesgos asociados con las amenazas y vulnerabilidades. Los controles pueden ser técnicos (como firewalls, cifrado de datos), administrativos (políticas, procedimientos) o físicos (cámaras de seguridad, controles de acceso). Estos controles ayudan a proteger la información y a garantizar la seguridad de los activos de una organización.

Amenazas comunes:

01 Ciberataques: Hackers pueden robar datos sensibles o interrumpir los sistemas.

02 Pérdida de datos: Falta de copias de seguridad o desastres físicos pueden provocar pérdidas irreversibles de datos.

03 Accesos no autorizados: Funcionarios no autorizados pueden visualizar, alterar o eliminar información confidencial.

UNA e.s.e | UNIVERSITARIA DEL ATLÁNTICO DIRECCIÓN TICS

IMPACTO DE UN INCIDENTE:

Consecuencias legales: Multas o sanciones impuestas por violar leyes de protección de datos.

Económicas: Gastos asociados con recuperación de datos o multas.

Reputacionales: Pérdida de confianza pública y daño a la imagen institucional.

OBJETIVOS

de la Política de Seguridad y Privacidad

PROTECCIÓN DE LA INFORMACIÓN CONFIDENCIAL:

Proteger los datos de pacientes y del personal.

CUMPLIMIENTO DE NORMAS LEGALES:

Asegurar que la E.S.E. cumple con todas las normativas aplicables (Ley 1581, Resolución 500).

ASEGURAR LA DISPONIBILIDAD Y LA INTEGRIDAD DE LOS SISTEMAS Y DATOS:

Mantener los sistemas operando de manera segura y asegurarse de que la información no sea alterada sin autorización.

Evitar accesos no autorizados:

Implementar controles de acceso fuertes para proteger la información de miradas no deseadas.

ROLES Y RESPONSABILIDADES

GERENTE Y DIRECTORES

Aseguran que se implementen las medidas de seguridad y establecen directrices claras.
Ejemplo: El director TIC es responsable de garantizar que las infraestructuras tecnológicas estén seguras.

COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

Supervisan y coordinan la implementación de la política de seguridad.
Deben realizar auditorías y hacer cumplir las normativas.

FUNCIONARIOS Y CONTRATISTAS

Deben cumplir con las políticas y procedimientos establecidos, y proteger la información que manejan en sus tareas diarias

Procedimientos Clave

Clasificación de la información:

Identificar qué datos son sensibles y clasificarlos (p. ej., público, restringido, confidencial).
Ejemplo: Historias clínicas son información confidencial.

Gestión de accesos y contraseñas:

Uso de contraseñas robustas y cambios periódicos, junto con el control de accesos.

Respaldo (Backups) de información crítica:

Hacer copias de seguridad regularmente para evitar la pérdida de datos importantes.

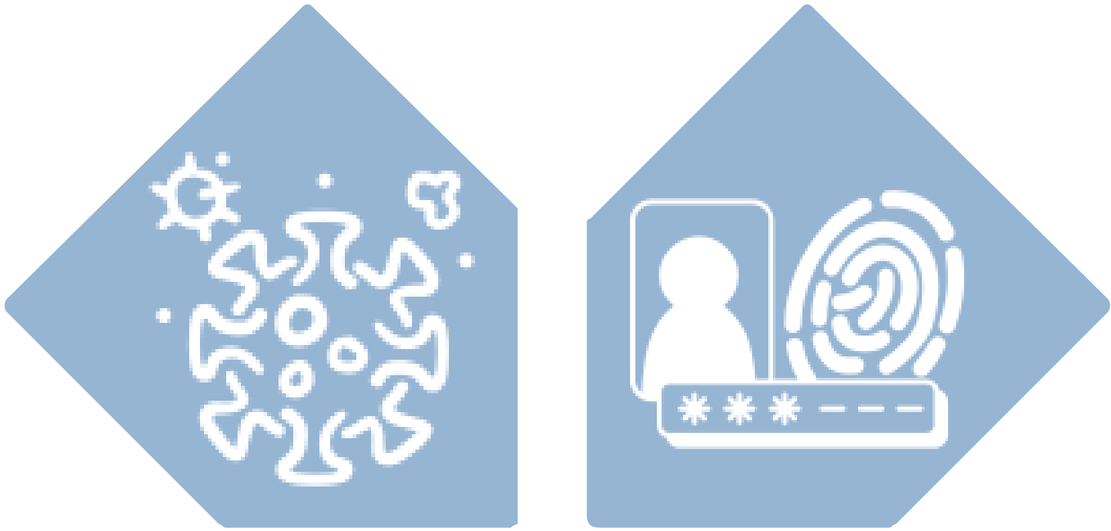
Manejo seguro de dispositivos:

Controlar el uso de dispositivos USB o laptops personales.
Ejemplo: Prohibir el uso de dispositivos no autorizados para transferir datos institucionales.

Uso adecuado del correo electrónico y redes sociales

Implementar políticas que restrinjan el envío de información confidencial a través de plataformas no seguras.
Ejemplo: Prohibir enviar información de pacientes por correos personales.

Medidas Técnicas y Administrativas



01

ANTIVIRUS Y FIREWALL:

Mantener sistemas de protección actualizados para prevenir intrusiones y virus.

02

AUTENTICACIÓN DE MÚLTIPLES FACTORES (MFA):

Exigir doble verificación en accesos sensibles para evitar accesos no autorizados.

03

CIFRADO DE DATOS SENSIBLES:

Asegurar que la información confidencial, como historias clínicas, esté cifrada tanto en almacenamiento como en tránsito.

04

CAPACITACIÓN PERIÓDICA AL PERSONAL:

Organizar capacitaciones continuas para actualizar a los funcionarios sobre nuevas amenazas y mejores prácticas.

Participación de los Funcionarios y contratistas

Qué hacer en caso de detectar una amenaza:

Reportar de inmediato a la Dirección TIC

Buenas prácticas en el manejo de la información:

No dejar datos confidenciales desprotegidos, usar solo dispositivos seguros.

Obligación de reportar incidentes:

Todo funcionario y contratista es responsable de reportar cualquier posible incidente de seguridad.

Conclusiones

Compromiso de toda la E.S.E.:

La seguridad de la información es responsabilidad de todos los funcionarios y contratistas.

La política de seguridad es evolutiva:

Debe ajustarse continuamente para enfrentar nuevas amenazas.

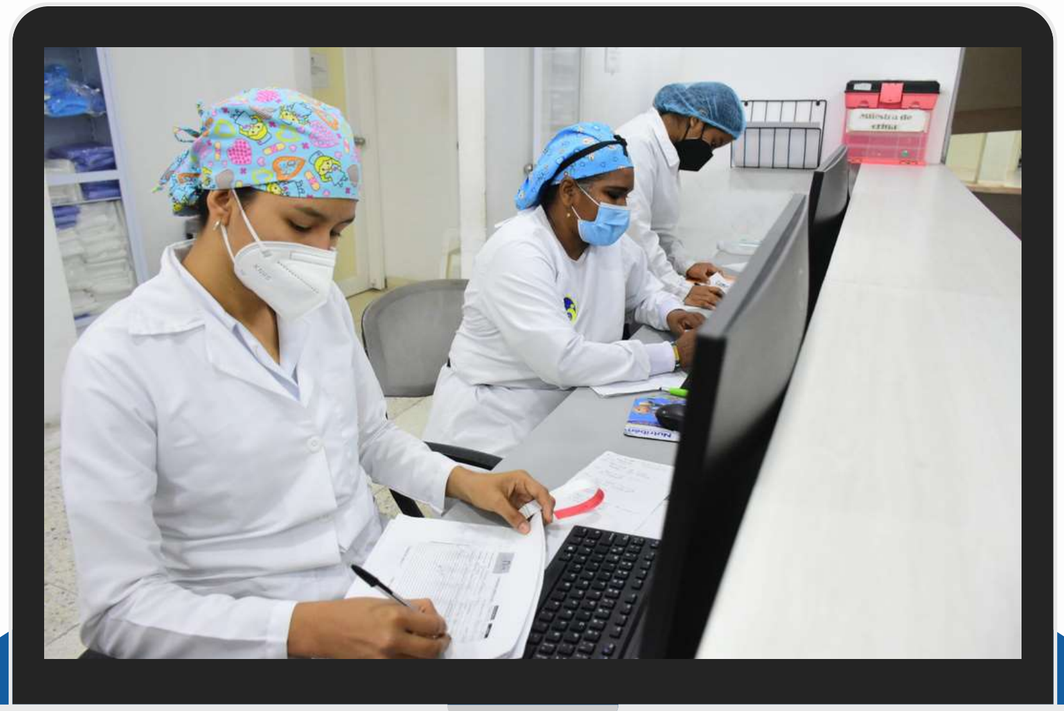
La prevención es la mejor defensa:

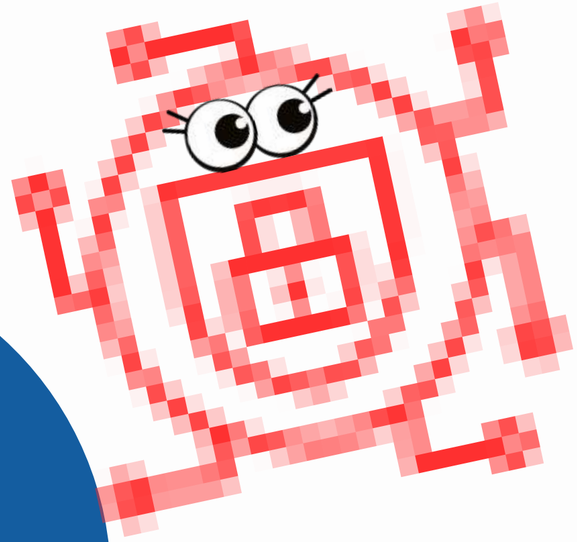
Con buenas prácticas se pueden evitar muchos incidentes antes de que ocurran


GRACIAS
A TODOS
POR SU ATENCIÓN

UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

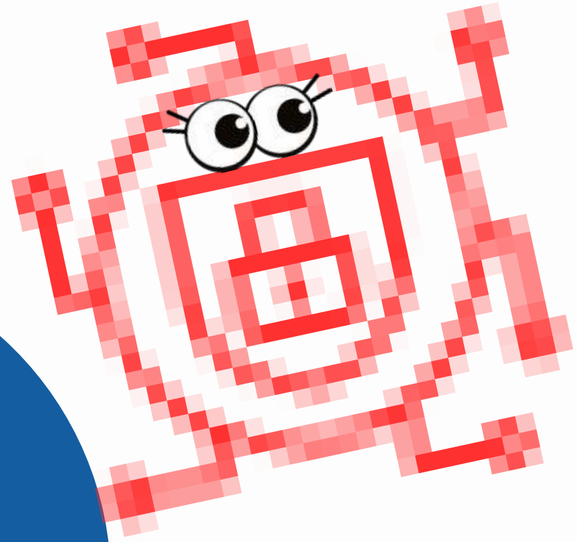
El uso de los equipos de cómputo será destinado única y exclusivamente para apoyar las funciones que son propias de la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA y en beneficio de la misma.





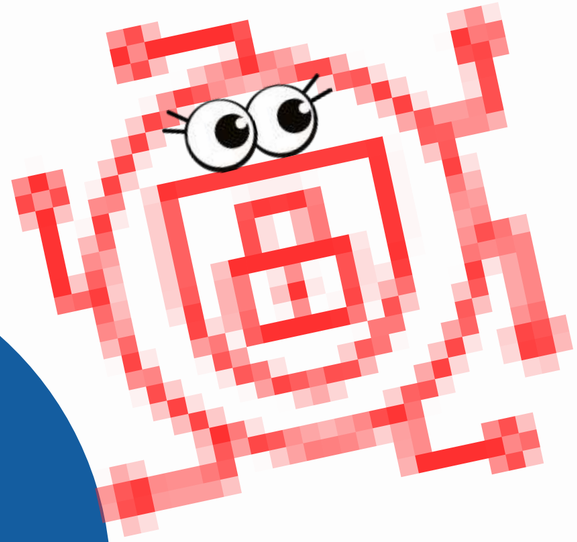
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

El equipo de cómputo no se debe operar fumando o consumiendo alimentos o bebidas.



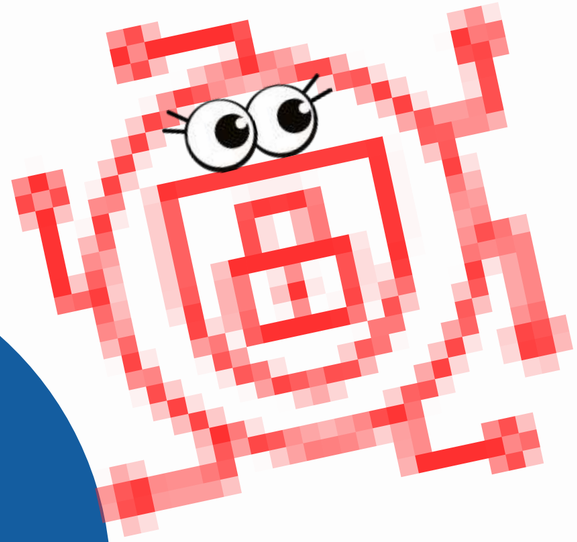
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

El equipo de cómputo debe estar conectado a la red eléctrica implementada por la E.S.E.



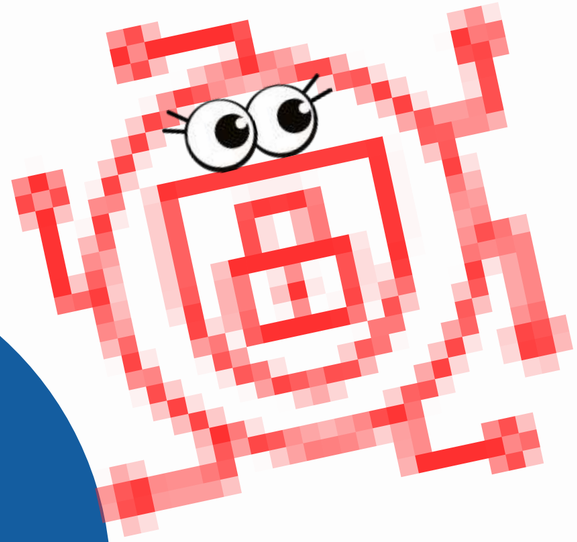
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

Si el usuario se ausenta de su puesto de trabajo por un tiempo superior a quince (15) minutos, el equipo de cómputo debe mantenerse protegido con una contraseña.

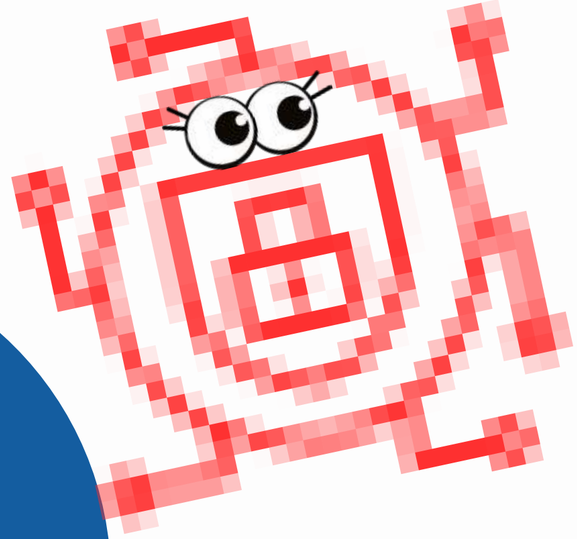


UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

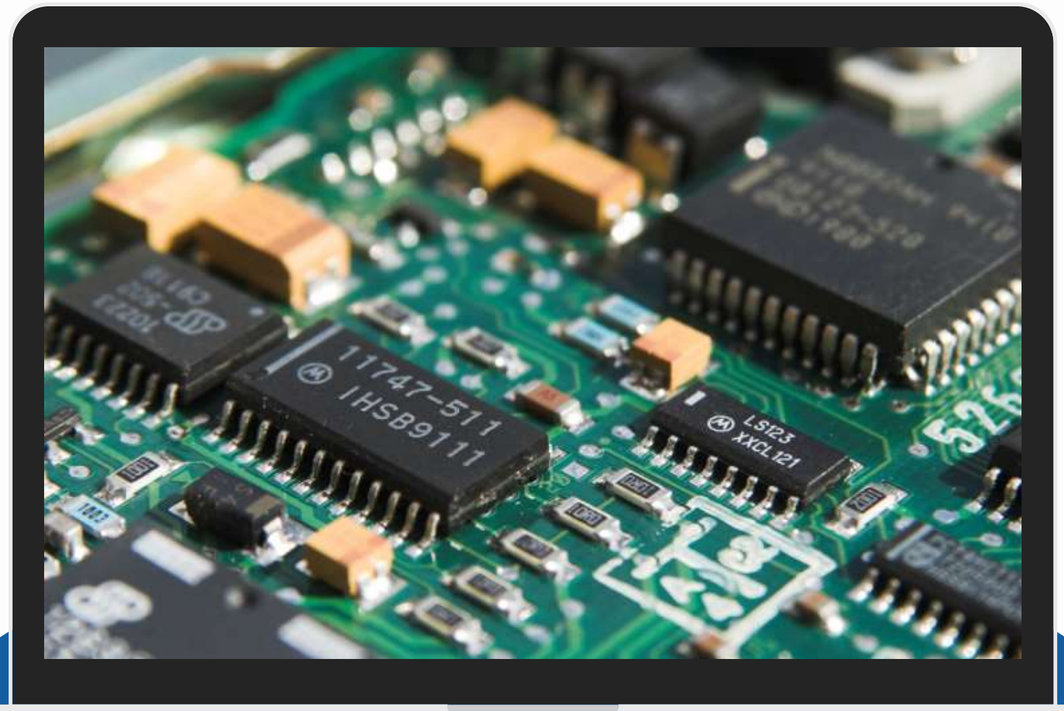
Queda estrictamente prohibido la instalación de cualquier programa no autorizado por la Dirección TICS.

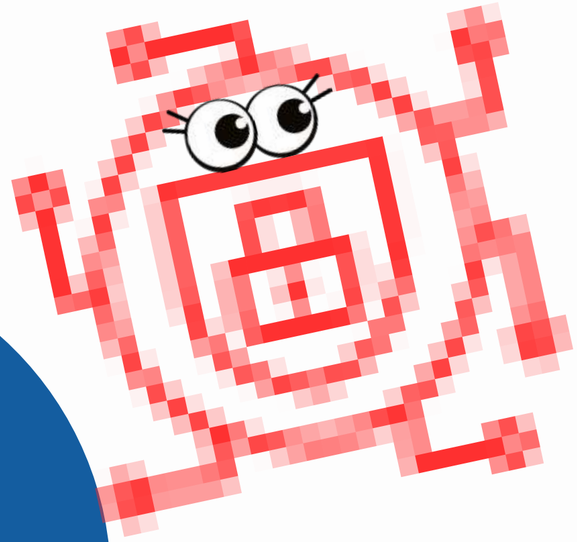


El cambio y/o movilidad de los equipos de cómputo solo podrá hacerse por personal de Recursos Físicos (Activos Fijos – Mantenimiento), una vez sea notificado, con oportunidad y autorizado por la Dirección TICS de la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA mediante oficio de acuerdo al procedimiento establecido.



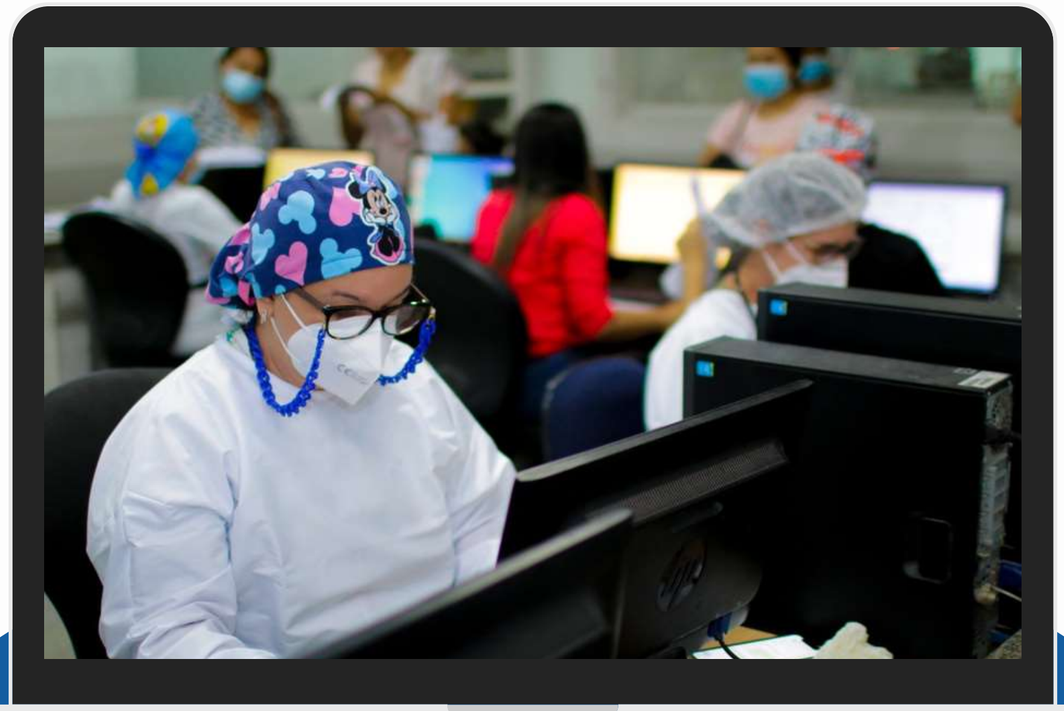
Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área de Dirección TICS.

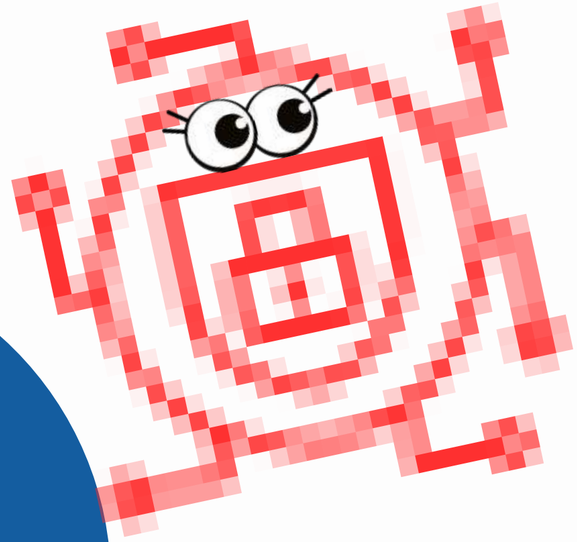




UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

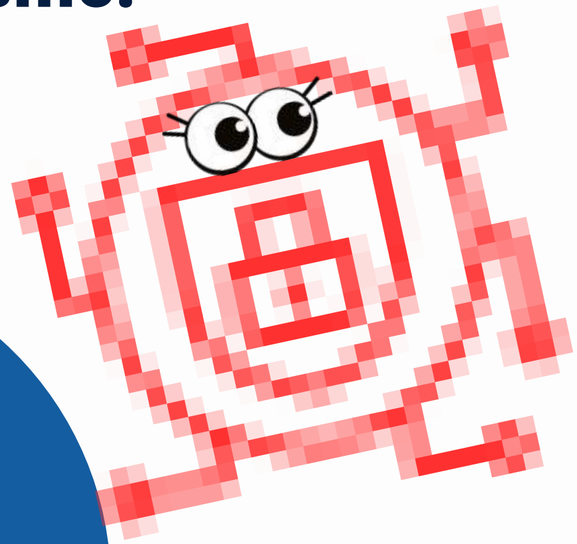
Ningún usuario podrá cambiar la configuración establecida por la Dirección TICS en los equipos de cómputo.

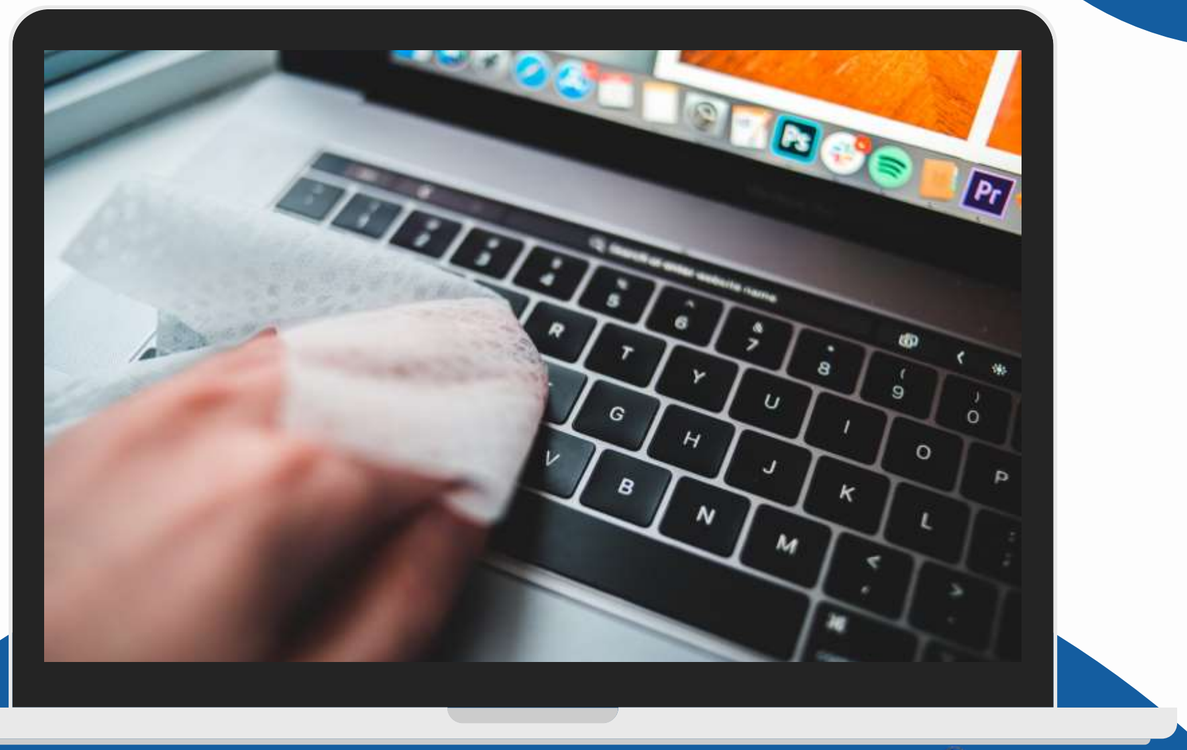




UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

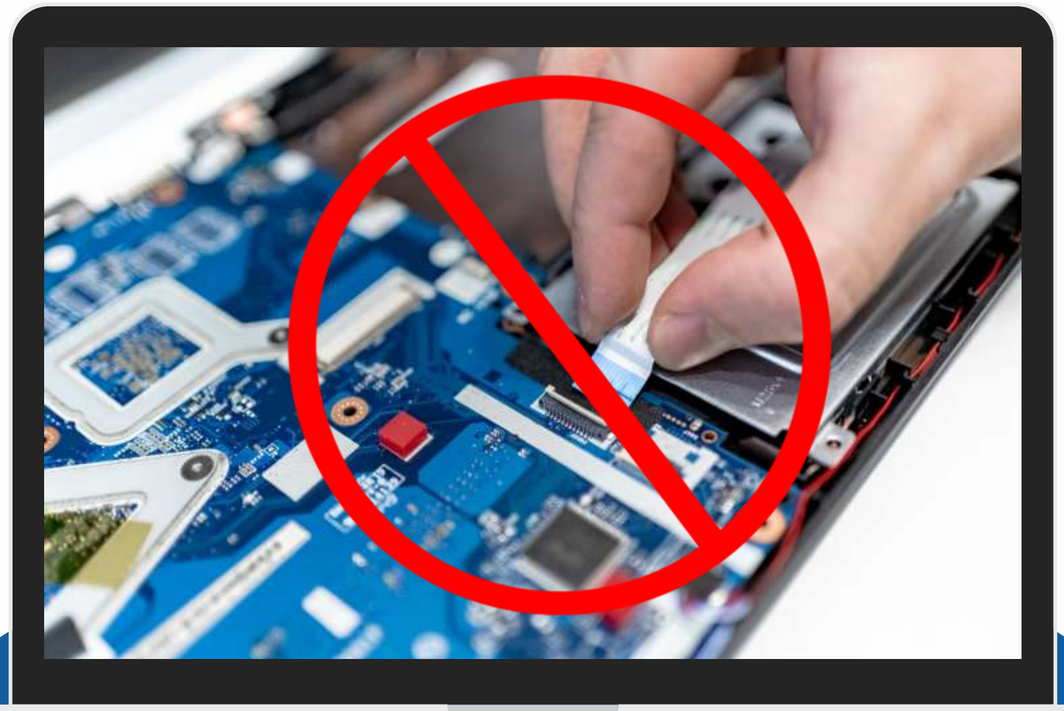
Todos los escritorios o mesas de trabajo tanto real como virtual, deben permanecer limpios, con fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

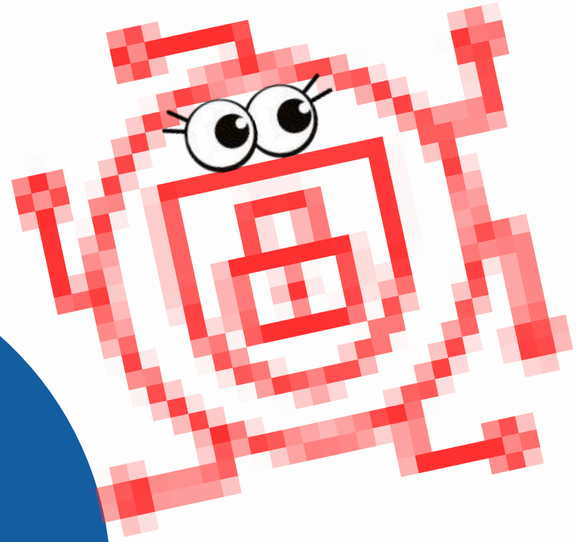




UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

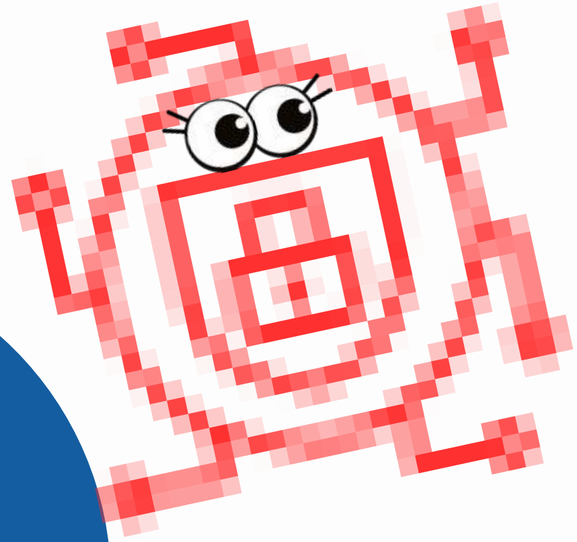
Ningún usuario podrá abrir físicamente los equipos de cómputo asignados para actualizar y/o realizar cambios no autorizados.





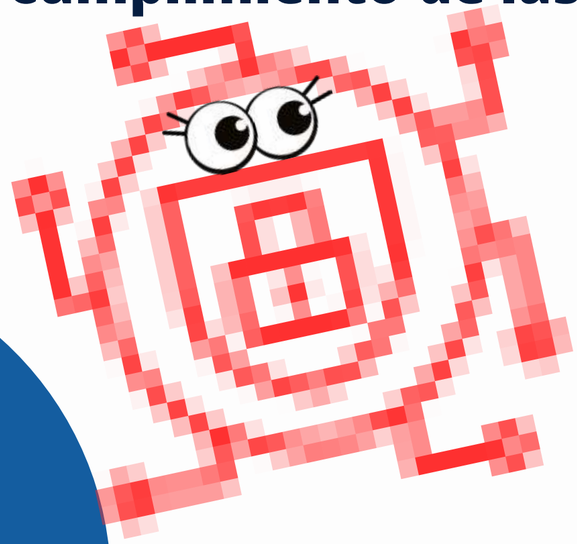
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

Queda prohibido el ingreso a las instalaciones de la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA, equipos de cómputo para su utilización, sin previo registro en la Dirección TICS.



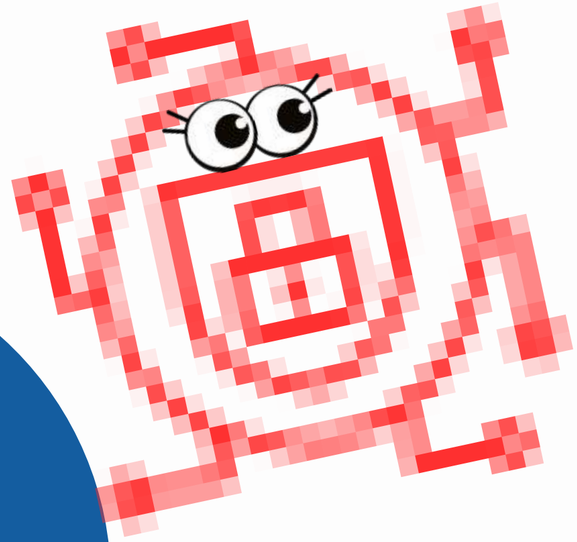
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

El uso de medios extraíbles para almacenamiento de información como DVD, CD-ROM, memoria USB, discos externos se deberá efectuar de manera racional y únicamente como herramienta de trabajo. Está totalmente prohibido el uso de estas herramientas para almacenar información con fines distintos al cumplimiento de las funciones.

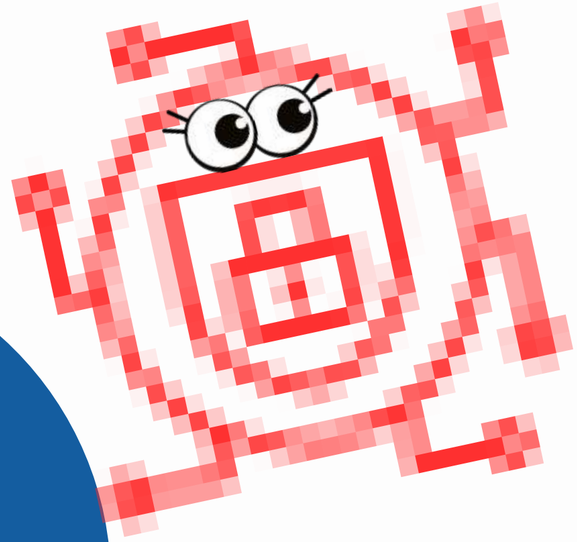


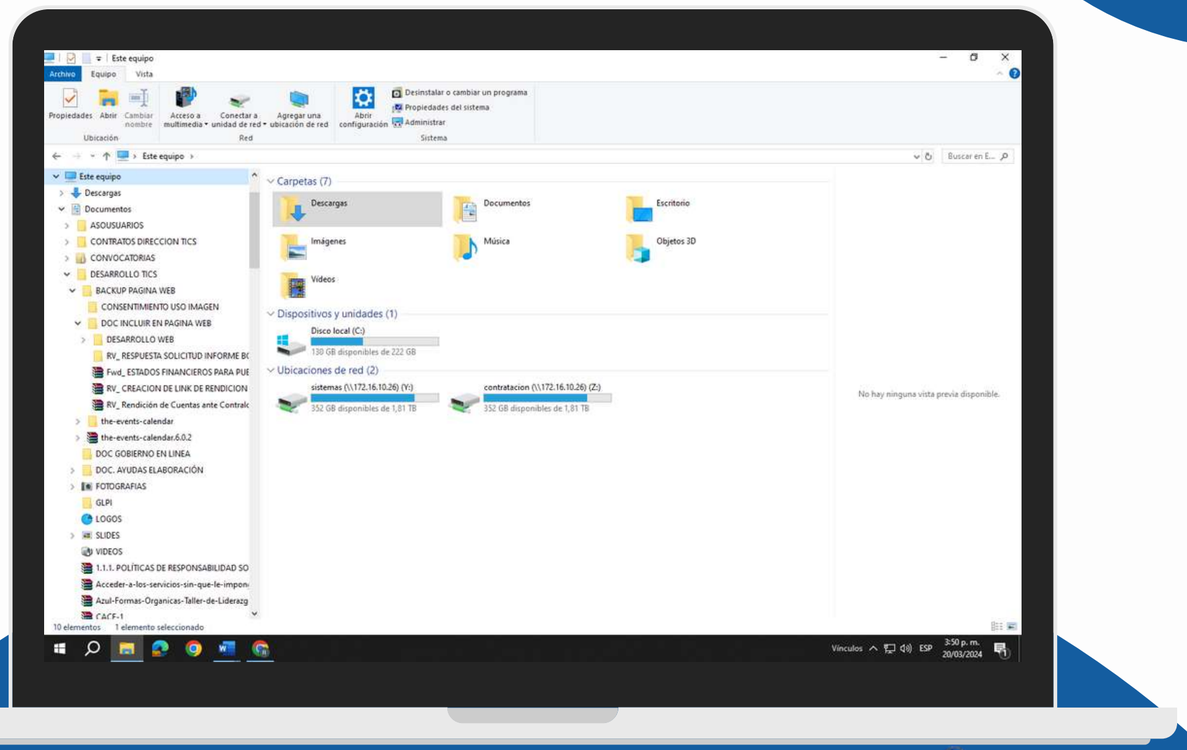
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

El usuario utilizará para la impresión de sus informes solo la impresora asignada por la Dirección TICS.



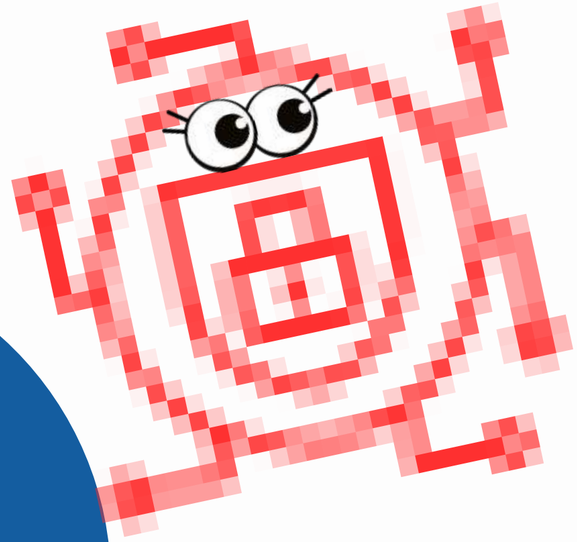
Por ningún motivo los usuarios podrán hacer uso de los medios instaladores de programas adquiridos, la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA, no permitirá el uso de instaladores y copias de software propiedad de la E.S.E. para beneficio personal.



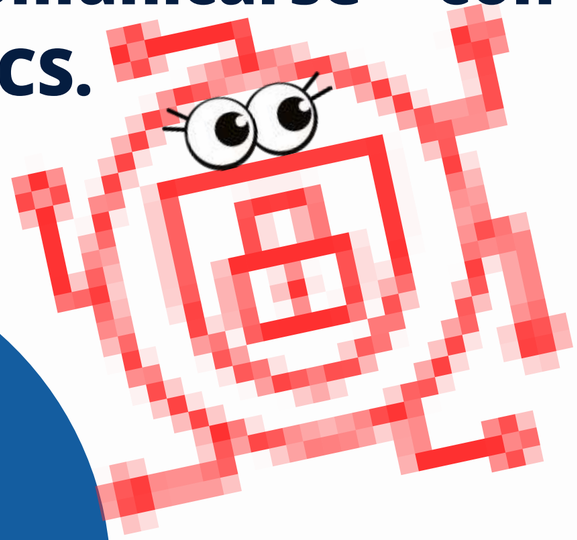


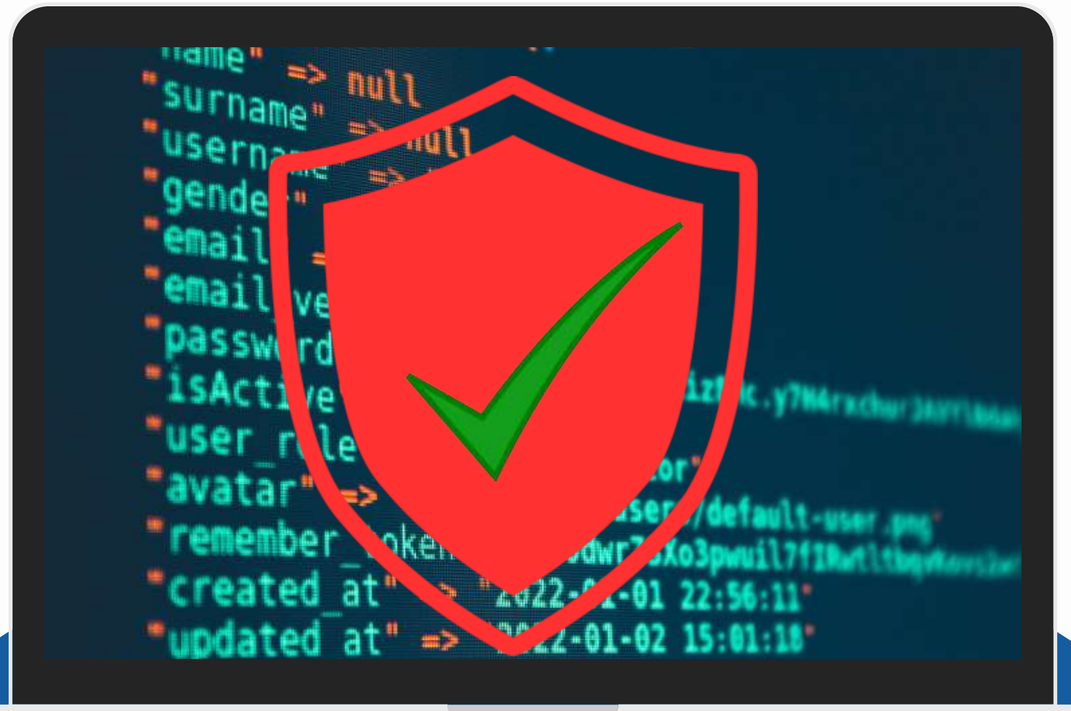
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

Todo archivo de origen externo debe ser pasado por el antivirus antes de su utilización.



Si los usuarios sospechan que hay infección por un virus, deben utilizar la herramienta antivirus instalada en sus equipos para desinfectarlo. En caso de que no funcione o persista en inconveniente, el usuario debe comunicarse con la Dirección TICS.

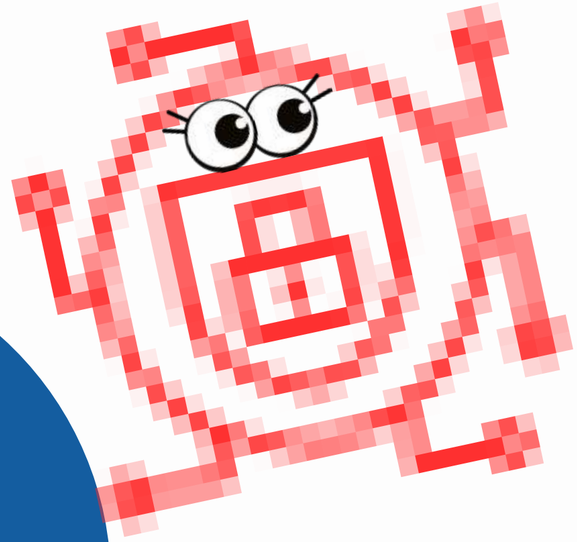




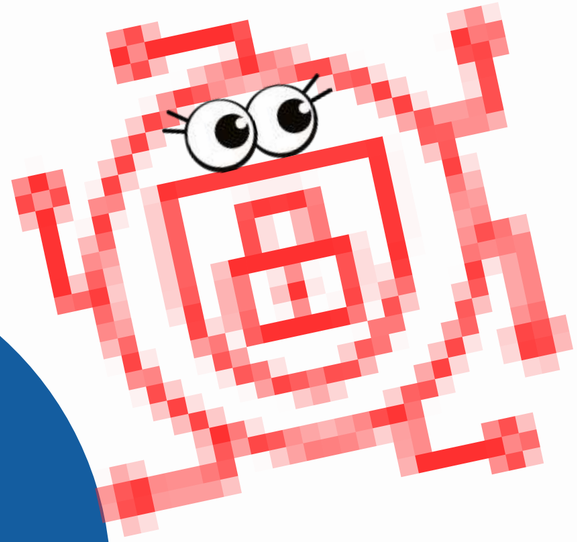
El ingreso de equipos (laptops, notebooks, iPad, etc.) a las instalaciones de la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA, debe ser autorizado por la Dirección TICS y registrado en la entrada. Para el caso de los computadores portátiles que van a ser utilizados con el fin de conectarse a la red de la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA, estás deberán contar con una licencia de protección antivirus legal, Software legal principalmente para Sistemas Operativos Windows y Paquetes de Office, Factura y/o manifiestos de importación del equipo y licencias, de lo contrario la Dirección TICS no autorizará el ingreso del equipo a las instalaciones.

UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

Todo equipo portátil perteneciente a la E.S.E. UNIVERSITARIA DEL ATLÁNTICO UNA, que salga de las instalaciones de la E.S.E. debe tener autorización de la Dirección TICS para su retiro. Los usuarios que utilicen estos medios en lugares públicos deben cumplir con los lineamientos para la seguridad del equipo, de manera que no se pierda, modifique o sea sustraída información contenida en ellos por descuidos.

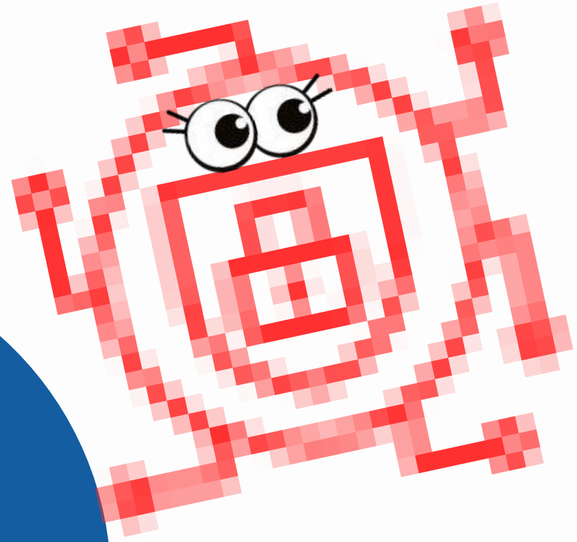


El equipo de cómputo no debe ser utilizado para fines personales.



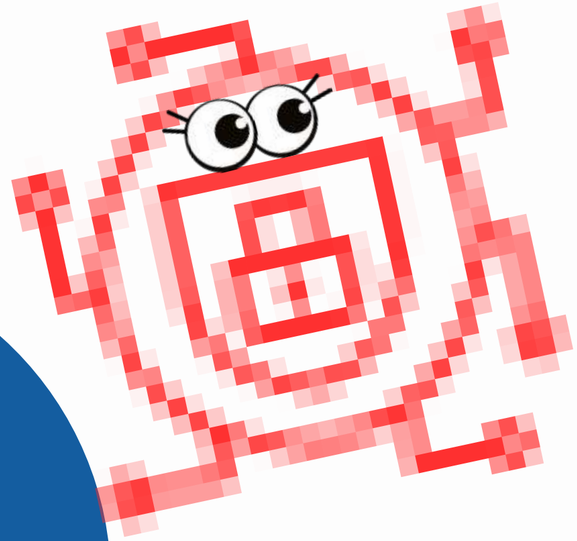
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

La Dirección TICS proveerá el servicio de Internet para ser compartido entre el personal y de acuerdo con los cargos establecidos.

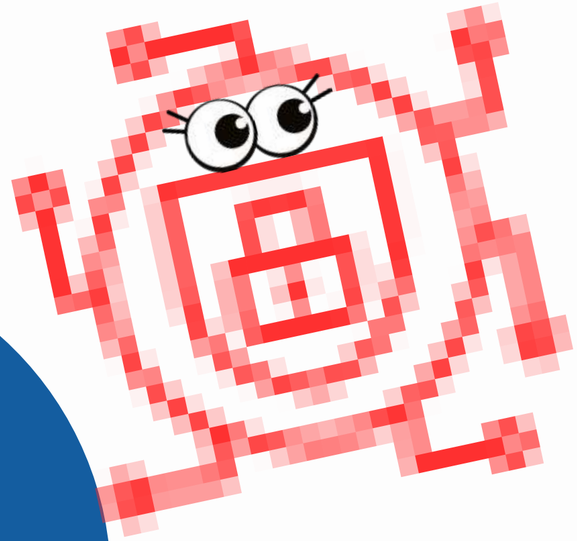


UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

El usuario del Servicio de Internet sólo podrá utilizar este servicio para el acceso a páginas seguras, confiables y que son para beneficio de la organización.



No se permite a los usuarios navegar por páginas denominadas perjudiciales para la compañía como páginas de sexo, pornografía, juegos, mensajería instantánea web, y otras



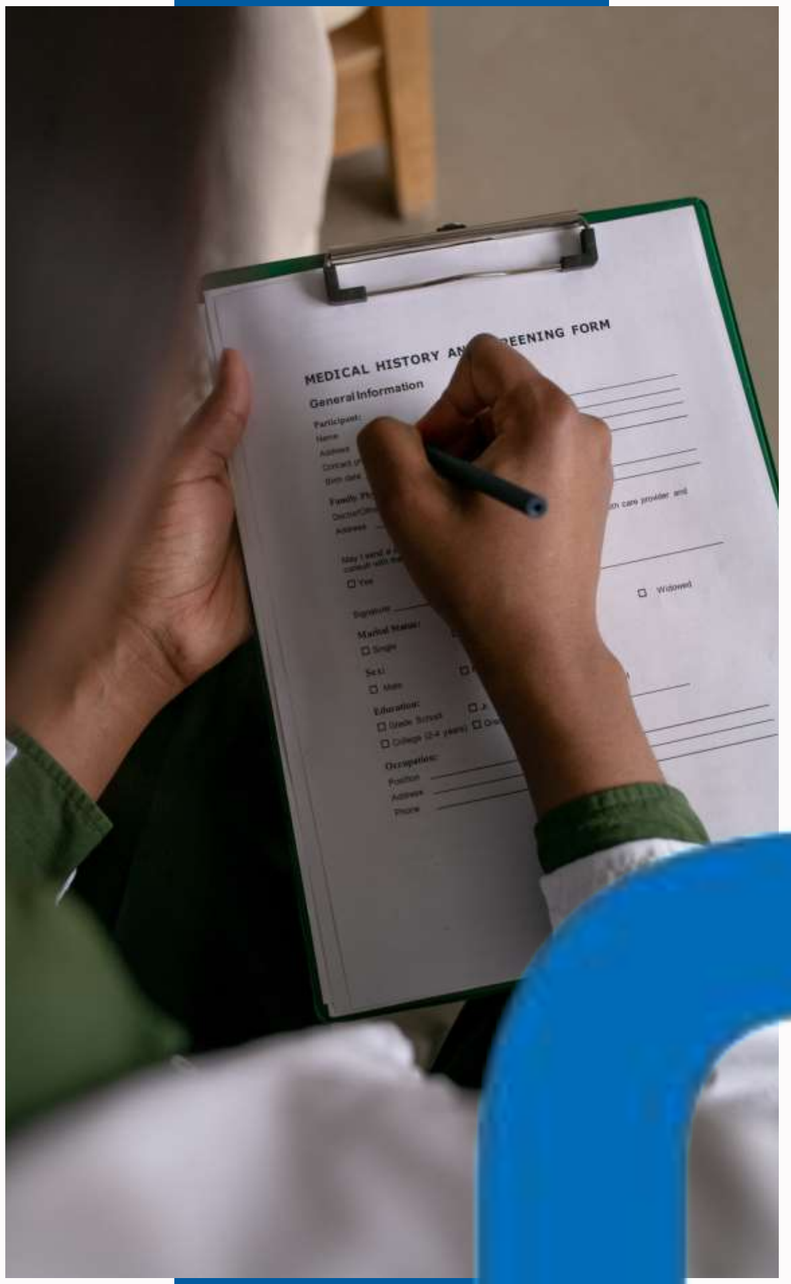
UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

USO RESPONSABLE DE LAS COMUNICACIONES Y LAS REDES SOCIALES

Objetivos

- Comprender la importancia del uso responsable de las comunicaciones y redes sociales.
- Identificar buenas prácticas y conductas éticas en el entorno digital.
- Conocer las implicaciones legales y profesionales del uso inadecuado de las redes sociales.

- **Privacidad** del Paciente: Proteger la confidencialidad y privacidad de la información del paciente.
- **Reputación** Profesional: Mantener una imagen profesional adecuada.
- **Ética** Médica: Adherirse a los principios éticos de la profesión médica.
- **Legalidad**: Evitar implicaciones legales que puedan surgir por el mal uso de la información.



1 Proteger la Información del Paciente:

La Constitución Política de 1991 señala en su artículo 15: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre y el Estado debe respetarlos y hacerlos respetar (...)”

Proteger la Información del Paciente:

La Historia Clínica: Es un documento privado, sometido a reserva, que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley. Por lo tanto, las fotografías tomadas a los pacientes, incluso si estos las han autorizado, hacen parte de la historia clínica y de los documentos legales, técnicos, científicos y administrativos pertinentes en los procesos de atención.

El secreto profesional implica que no es ético ni lícito revelar información sin una justa causa, ya que pertenece al ámbito íntimo de su titular. La revelación del secreto profesional es procedente en los siguientes casos:

1. Al enfermo, en aquello que estrictamente le concierne y convenga;
2. A los familiares del enfermo, si la revelación es útil al tratamiento;
3. A los responsables del paciente, cuando se trate de menores de edad o de personas mentalmente incapaces;
4. A las autoridades judiciales o de higiene y salud, en los casos previstos por la ley;
5. A los interesados, cuando por defectos físicos irremediables o enfermedades graves infectocontagiosas o hereditarias, se ponga en peligro la vida del cónyuge o de su descendencia.

EN LA LEY 23 DE 1981 DE ÉTICA MÉDICA EN COLOMBIA, LOS ARTÍCULOS QUE SE REFIEREN AL USO DE IMÁGENES DE LOS PACIENTES INCLUYEN:

ARTÍCULO 33

Uso de Imágenes del Paciente

El uso de imágenes (fotografías, vídeos, etc.) de los pacientes en la práctica médica, con fines de diagnóstico, tratamiento, investigación o docencia, está condicionado al consentimiento expreso del paciente o de sus representantes legales. La imagen debe utilizarse de manera que no permita la identificación del paciente, salvo que exista un consentimiento explícito para ello.

ARTÍCULO 34

Secreto Profesional

El artículo también es aplicable al uso de imágenes, ya que el secreto profesional incluye toda la información obtenida en el ejercicio de la profesión médica, lo cual comprende las imágenes del paciente. La revelación de estas imágenes está sujeta a las mismas condiciones de confidencialidad y autorización que cualquier otra información sensible.

Artículo 35

Historias Clínicas

Aunque se refiere a la información contenida en la historia clínica, este artículo abarca cualquier documentación incluida en la misma, lo cual podría incluir imágenes. Estas están sujetas a la misma privacidad y condiciones de revelación que el resto de la información clínica.

ARTÍCULO 36

Comunicación de Diagnósticos

Este artículo enfatiza la prudencia en la comunicación de información clínica, lo cual se extiende al uso y divulgación de imágenes médicas, asegurando que se compartan solo con el consentimiento adecuado y dentro de los límites éticos y legales establecidos.

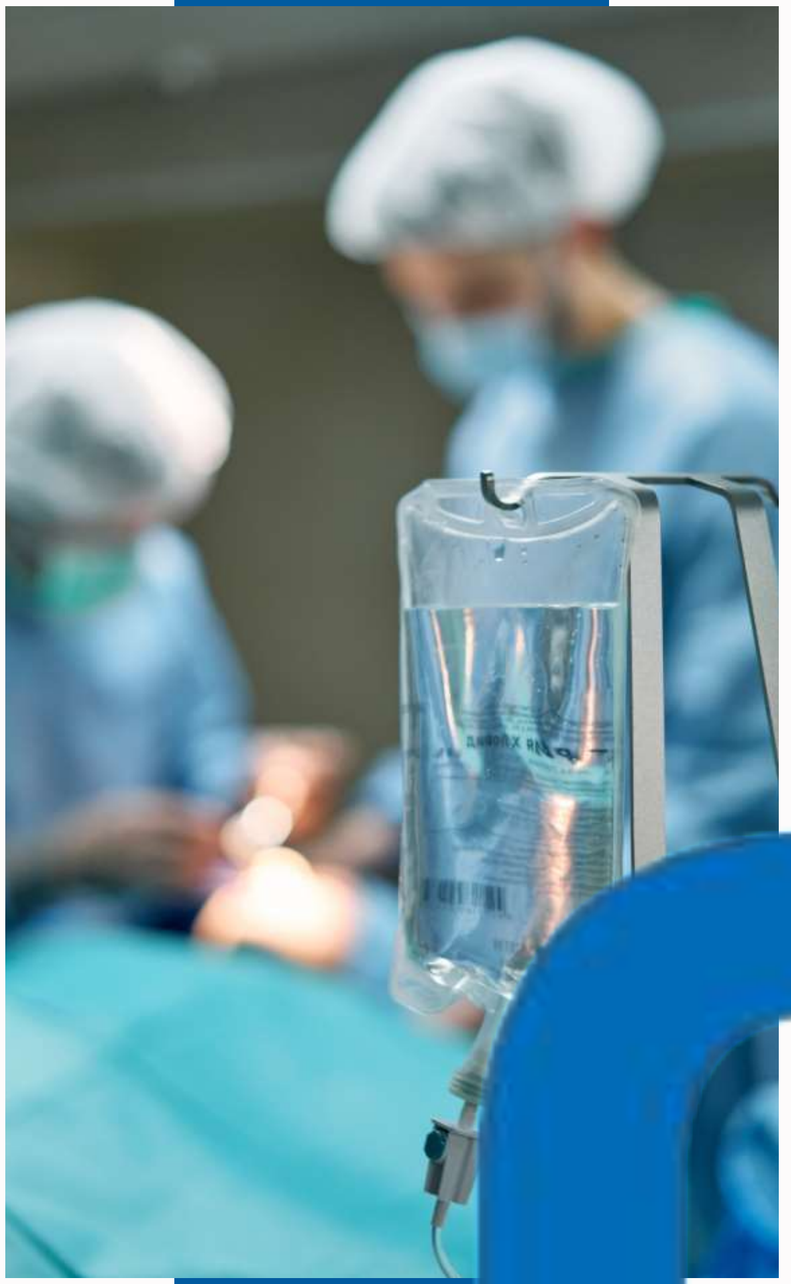
ARTÍCULO 46

Publicaciones Médicas

Cuando se utilicen imágenes de pacientes en publicaciones científicas o académicas, debe asegurarse la anonimización de las mismas, salvo que el paciente haya dado su consentimiento explícito para ser identificado. Además, cualquier uso debe ser estrictamente con fines de beneficio público, educativo o científico.

TENER EN CUENTA

- No compartir detalles específicos sobre pacientes en redes sociales.
- Despersonalizar cualquier información clínica utilizada con fines educativos. *Anonimizar* las imágenes para que la persona fotografiada no sea identificable.
- Conocer y seguir las políticas Tratamiento de datos personales de la E.S.E. UNA y Ley Estatutaria 1581 de 2012.



UNA e.s.e | UNIVERSITARIA DEL ATLÁNTICO

DIRECCIÓN TICS

En cuanto a la publicación de imágenes de LA E.S.E. UNA en cualquiera de sus 5 sedes, aunque no salga ninguna persona en ellas, se precisa la autorización de la Dirección TICS

La publicación de estas imágenes sin el consentimiento adecuado puede resultar en sanciones administrativas y penales, indemnizaciones por daños y perjuicios, y vulneración de derechos al honor, intimidad y protección de datos personales. El cumplimiento de estas normativas es crucial para mantener la ética y profesionalismo.

Mantener una Imagen Profesional:

- Publicar contenido que refleje profesionalismo y respeto.
- Evitar publicaciones polémicas o inapropiadas que puedan dañar la imagen profesional.
- Separar la vida personal y profesional en redes sociales.

Consejos para un Uso Responsable:

- Configurar la Privacidad: Utilizar las configuraciones de privacidad para controlar quién ve las publicaciones.
- Pensar Antes de Publicar: Reflexionar sobre el impacto potencial de cada publicación.
- Evitar Discusiones Sensibles: No involucrarse en debates controversiales que puedan comprometer la profesionalidad.

Adherirse a la Ética Médica:

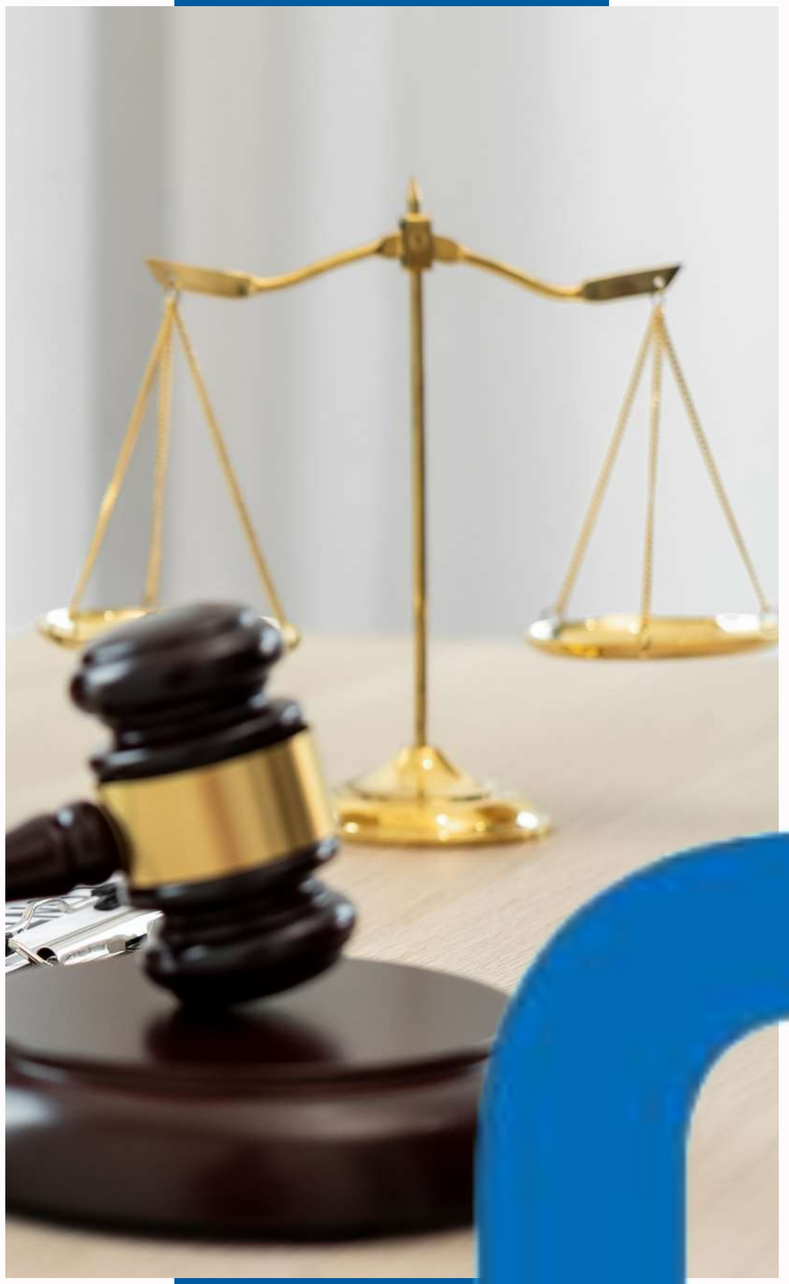
- Ser honesto y transparente en la comunicación digital.
- Respetar los derechos y la dignidad de los pacientes y colegas.
- No difundir información falsa o engañosa.

El profesionalismo, que incluye entre otros aspectos el respeto por la privacidad de los pacientes (22-24), constituye una de las seis competencias básicas que deben desarrollar y mantener los estudiantes de Medicina durante el pregrado y la residencia, y los médicos en su ejercicio profesional.

La Asociación Médica Mundial ha promulgado la Declaración de Helsinki como una propuesta de principios éticos que sirvan para orientar a los médicos y a otras personas que realizan investigación médica en seres humanos. enuncia proposiciones éticas que deben tener carácter universal, por tanto aplicables en todo el mundo: si un ensayo no es ético en Massachusetts por esta razón, tampoco lo es en Barranquilla.

Implicaciones del Uso Inadecuado:

- Disciplinarias: Posibles sanciones por parte de instituciones médicas y educativas.
- Legales: Demandas y acciones legales por violaciones de privacidad.
- Profesionales: Daño a la reputación y futuras oportunidades de empleo.



UNA e.s.e UNIVERSITARIA DEL ATLÁNTICO
DIRECCIÓN TICS

LA CALIDAD DE LA PERSONA SE NOTA DESDE EL SALUDO