Universidad Autónoma de Bucaramanga

protegernos

Oficina de seguridad de la información **UNAB**

RECOMENDACIONES GENERALES DE SEGURIDAD DE LA INFORMACIÓN PARA EMPLEADOS Y ESTUDIANTES UNAB.

Aplicar las buenas prácticas de seguridad es un deber de todos.

Las herramientas de cómputo, especialmente aquellas que podemos llevar a todos lados nos permiten un acceso continuo a la información y a su vez nos permiten compartir información de nuestra autoría. Sin embargo, esta actividad no está libre de amenazas de seguridad.

Es necesario aplicar el sentido común y observar las pautas dadas para proteger la información, las estaciones de trabajo y las redes de datos. Recuerda que se debe garantizar la seguridad de la información de los titulares que han autorizado a la UNAB el tratamiento de sus datos personales.

Todos estamos obligados a: mantener la seguridad de la información, a observar la ley de habeas data, las buenas prácticas de seguridad y las políticas institucionales de seguridad de la información de la Universidad.

unab
VIGILADA MINEDUCACIÓN

Recomendaciones de uso del correo UNAB.

La cuenta de correo electrónico UNAB debes usarla como tu dirección de contacto principal para: las comunicaciones internas, los servicios en la universidad y como el usuario de ingreso a las plataformas de aprendizaje. El uso de los servicios de correo electrónico de la universidad mejora la seguridad de las comunicaciones.

Si recibes un correo electrónico enviado a otro destinatario, informa al remitente sobre la dirección incorrecta. Recuerda que estás obligado a mantener el contenido del mensaje como confidencial.

Los mensajes de correo electrónico pueden contener programas malignos o dirigirte a sitios que contienen malware. No abras mensajes si no estás seguro de su origen. También puedes recurrir a la oficina de Seguridad de la Información para obtener más instrucciones.

Ten cuidado al compartir tu dirección de correo electrónico. Evita usar la dirección de correo electrónico de la UNAB en foros en línea y redes sociales. Utiliza una cuenta de correo electrónico diferente para uso personal.

Los mensajes de correo electrónico generalmente se transmiten en un formato sin cifrar, por lo que los mensajes confidenciales se deben cifrar por separado antes de enviarlos.

Utilizar claves seguras y mantenerlas en secreto.

Utiliza tu usuario y contraseña UNAB para iniciar sesión en los sistemas de la universidad. Mantén tu identificación de usuario y contraseña tan seguros como tu tarjeta bancaria y tu código PIN.

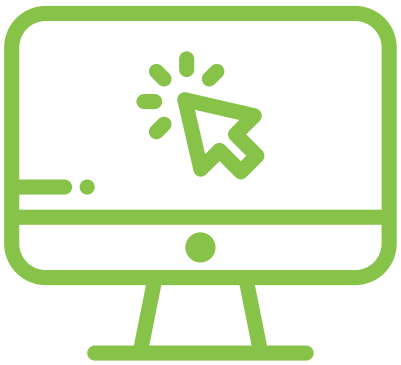
Cuando recibas una nueva contraseña emitida por el soporte de CATIC UNAB, cámbiala inmediatamente por una que solo tú conozcas. Cambia tu contraseña regularmente por lo menos cada 3 meses y siempre que tengas alguna duda de que ha sido revelada a otra persona. En general se debe tener en cuenta que las contraseñas o los pines de acceso a los sistemas no deben cumplir años, a mayor tiempo de uso mayor peligro de exposición.

Tú eres responsable de todas las actividades realizadas con tu ID de usuario. Nunca le entregues tu contraseña a nadie más; ni siquiera a los administradores del sistema. Si alguien solicita tu contraseña, definitivamente es para un propósito malicioso.

Elige tu contraseña cuidadosamente. Una buena contraseña no es tan fácil de recordar, pero difícilmente otros podrán descubrirla. No utilices palabras que se usen comúnmente o que de alguna manera estén conectadas contigo. Una buena contraseña está compuesta por: una letra mayúscula, un número, un símbolo especial y una longitud de mínimo 8 caracteres.

Elige diferentes contraseñas para los servicios de la UNAB y cualquier servicio externo; de esta manera, al exponerse la contraseña del servicio externo no se comprometería la seguridad del sistema universitario.

Recuerda, las contraseñas en los sistemas de información no se deben prestar y menos aún recibirlas en préstamo.



Usa de forma responsable los PCs de la UNAB.

Siempre que te ausentes de tu puesto de trabajo no olvides bloquear tu equipo de cómputo. Esto evita el uso no autorizado de los sistemas que estás manejando.

La instalación de software en los PCs de la UNAB está prohibida y también técnicamente impedida. Si necesitas una determinada aplicación ponte en contacto con el Centro de Atención en Tecnologías de Información y Comunicaciones - CATIC para obtener ayuda.

Cuando produzcas o edites textos u otros materiales, recuerda guardar tus cambios regularmente. De esta manera, no perderás todo el trabajo realizado en caso de una falla técnica.

Guarda todos los datos importantes en un directorio o carpeta que hayas creado para tal fin. Si eres un funcionario de la UNAB recuerda que puedes utilizar el área de almacenamiento por dependencia para guardar tu información de trabajo.

En el caso de utilizar los PCs en préstamo o los PCs de las aulas no olvides llevarte la información cuando termines de usar el PC. Estos equipos son para el uso de toda la comunidad académica.

Cuidado con la ingeniería social y otras estafas.

No confíes en todos los correos electrónicos que recibes. El campo del remitente puede no indicar la fuente real del mensaje. Las aplicaciones de malware pueden enviar mensajes sin la participación del usuario. No abras archivos de fuentes desconocidas, asegúrate de conocer el remitente.

Ten cuidado con el phishing, es decir, mensajes en donde te solicitan que compartas tu usuario y contraseña o que los ingreses en un sitio web enviado por el remitente. Recuerda que los administradores de la UNAB nunca solicitan tu usuario y su contraseña. En caso de que suceda, no entregues tu información e informa inmediatamente a la oficina de Seguridad de la Información de la UNAB.

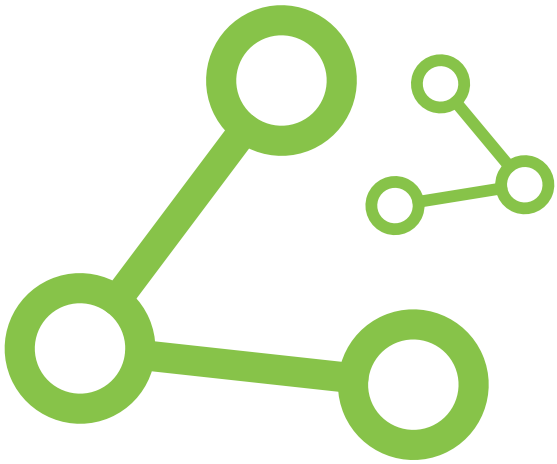
Comprueba siempre la dirección de destino real antes de hacer clic en un enlace.

Ten mucho cuidado con los enlaces recibidos a través de los mensajes de correo electrónico.

Los anuncios y las cadenas enviadas al correo electrónico sin tu consentimiento considéralos maliciosos. Nunca respondas a tales mensajes; solo márcalos como SPAM. Si una oferta parece demasiado buena para ser cierta, probablemente es maliciosa; no la tomes.

Además del correo electrónico, también puedes encontrar otras formas de intento de engaño, por teléfono o en redes sociales. Ten cuidado con las fotomultas, notificaciones de embargos o mensajes inesperados de los remitentes que se hacen pasar por administradores del sistema.

Si en una llamada de tu banco te piden tu número de tarjeta de crédito completo o tu clave de acceso ten por seguro que la llamada es maliciosa y si a ello se agrega la solicitud del código de seguridad de la tarjeta, puedes tener certeza absoluta ¡cuelga!



Utiliza los servicios en línea y los medios sociales sabiamente.

Piensa antes de compartir información personal en varias plataformas en línea como Facebook, Instagram, WhatsApp, entre otras. Después de cargarla, como una foto o tus datos personales, puede ser imposible de eliminar permanentemente de la web.

Ten cuidado con las ventanas emergentes y los anuncios. El malware se propaga eficientemente a través de las redes sociales y los servicios en línea. ¡Haz clic con cuidado! No uses servicios en línea que no se sientan confiables.

Muchos servicios en línea se implementan en forma de servicios en la nube, lo que significa que la información proporcionada por los usuarios solo se almacena en los servidores del proveedor de servicios. Los servicios en la nube conllevan muchos riesgos de seguridad de la información que se deben tener en cuenta. Antes de registrarte como usuario del servicio, siempre verifica los términos y condiciones relacionados con la protección de los datos personales y la divulgación de los mismos a terceros.

Ten cuidado con los datos personales: piensa detenidamente qué información compartes y con quién la compartes. Tú estás a cargo de compartir tu información personal, pero la información personal de otros solo puede ser compartida por su titular. Nunca compartas información de otra persona sin su consentimiento.

En las redes sociales es fácil fingir ser alguien que no se es. No seas demasiado crédulo con respecto a las cosas que lees en Internet.

Recuerda las buenas reglas de comportamiento en el correo electrónico y las comunicaciones en línea. Por ejemplo, los comentarios fuertes publicados en un panel de discusión pueden dañar tu reputación más adelante cuando solicites un trabajo.

No agregues datos de ubicación a las fotos que publiques en línea. Deshabilita la funcionalidad GPS de tu cámara o elimina el sello de ubicación de las fotos antes de publicarlas. No es bueno que desconocidos sepan tanto de ti.

Verifica la configuración de privacidad de tu perfil de usuario. Controla quién puede acceder a tu información y ajústala cuando sea necesario.

Mantén tu propio PC funcional y saludable.

Tú eres el administrador de sistemas de tu propio computador. Monitorea su funcionalidad y garantiza la seguridad adecuada de la información de acuerdo con las siguientes instrucciones:

- Si el PC está conectado a una red, debe protegerse con un firewall y un software antivirus.
- No instales ninguna aplicación de software que realmente no necesites. Instala todas las actualizaciones de seguridad.
- Crea un usuario administrador y otro restringido y navega con el usuario restringido. Los derechos de administrador solo deben usarse para realizar tareas de nivel de administrador como: instalación de software, creación de otras cuentas, etc.
- Realiza copias de respaldo de tus archivos de forma regular. Mantén las copias de seguridad fuera de tu computador.
- No deseches los computadores, los teléfonos inteligentes o las unidades USB sin antes haber destruido la información.

También mantén seguros tus dispositivos móviles.

Los teléfonos, tabletas y otros dispositivos móviles deben protegerse con tanto cuidado como los computadores.

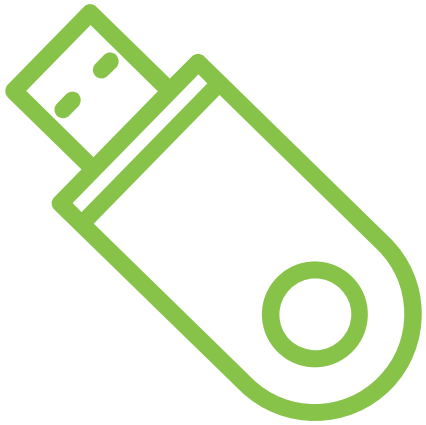
No abras mensajes que provienen de remitentes desconocidos o que parezcan sospechosos, por ningún motivo. Pueden contener malware con la capacidad para enviar mensajes a tu nombre, robar tus datos personales o causar otros tipos de daños.

Protege tus dispositivos móviles contra robo. Establece una clave o código de seguridad además del código PIN para evitar que personas ajenas accedan a tus datos.

Desactiva las conexiones inalámbricas Bluetooth y WLAN cuando no las necesites. Recuerda también realizar copias de respaldo de los datos importantes almacenados en tus dispositivos móviles. Elimina tus datos cuando deseches el dispositivo.

No instales ninguna aplicación de software que realmente no necesites. Solo descarga e instala software de distribuidores autorizados.

Considera cuidadosamente si debes compartir tus datos de ubicación en los servicios en línea.

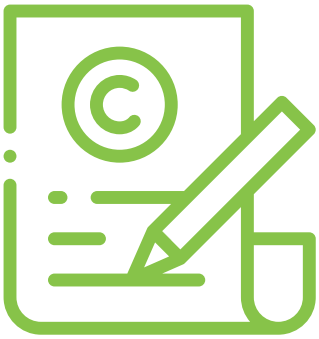


Ten cuidado con tus unidades USB.

No utilices una unidad USB como el principal o único almacenamiento de archivos, aunque sea una herramienta práctica para transferir datos y realizar copias de seguridad. Una unidad USB puede dañarse o perderse fácilmente.

Si tienes la intención de guardar datos confidenciales en una unidad USB, almacénalos de forma cifrada. Ten cuidado con las unidades USB de otros usuarios ya que pueden contener una aplicación de malware que se activa automáticamente para controlar tu computador, robar o dañar tu información.

Si encuentras una unidad USB de alguien en las instalaciones de la universidad no la uses, llévala a la oficina de objetos perdidos sin verificar su contenido.



Observa los derechos de autor y las licencias de software.

Asegúrate de tener las licencias requeridas para las aplicaciones que instales en tu computador. No instales software no licenciado.

Lee las pautas de la Biblioteca para conocer los términos y condiciones de uso de los materiales de la biblioteca electrónica.

Las películas y los materiales musicales están cubiertos por derechos de autor. No descargues ni compartas dicho material en línea sin el debido permiso del propietario de los derechos de autor.

unab
VIGILADA MINEDUCACIÓN

Universidad
Autónoma de
Bucaramanga

protegernos

Oficina de seguridad de la información **UNAB**