Ministerio de Educación Pública

Hacia una ciudadanía digital segura y responsable

Políticas de uso de tecnologías digitales en los ambientes de aprendizaje a distancia

¿Qué debe hacer para proteger su identidad digital?

Para proteger su identidad digital, su privacidad y la confidencialidad de sus correos electrónicos, debe tomar en cuenta lo siguiente:

- Utilice la cuenta de correo electrónico MEP y el Microsoft Teams exclusivamente para actividades académicas y educativas.
- Evite el envío de correos electrónicos que incluyan información confidencial, como contraseñas, números de tarjetas de crédito o débito, pines u otros datos de identificación.
- Elija contraseñas seguras y evite utilizar palabras de fácil identificación. Las contraseñas seguras incluyen al menos 8 caracteres, una combinación de mayúsculas y minúsculas, al menos un número entre 0-9 y un símbolo.
- Guarde su contraseña en un lugar seguro, que solo usted pueda ubicar. Además, evite utilizar la misma contraseña en todas las cuentas, sitios web u otra aplicación. Esta es una práctica riesgosa que pone en peligro su privacidad. Recuerde no escribir las contraseñas en un papel y mucho menos guardarlas en su billetera, cartera o libreta de contactos.

- Evite dejar abierta su sesión o que otras personas utilicen su correo personal. Cuando finalice su sesión de trabajo verifique que su cuenta se cerró correctamente.
- Digite su contraseña cada vez que ingresa al correo u otra aplicación. Trate de no guardar la contraseña en los dispositivos para ingresar de manera directa. Con esto se evita que otras personas tengan acceso directo a sus aplicaciones: Outlook, Skype, Zoom, Teams, Facebook, Instagram, entre otras.
- Revise periódicamente el correo electrónico institucional habilitado como medio oficial de comunicación y de acceso a la plataforma Microsoft Teams. Ingrese para descargar las lecturas, realizar las actividades y participar en las videoconferencias programadas por cada persona docente y profesionales a cargo de los diversos servicios.
- Utilice el correo electrónico y plataforma Teams para establecer contacto con las personas docentes.
- Solicite a la persona docente el cronograma de trabajo para participar en las actividades establecidas.
- Utilice el espacio personal en la nube (One Drive), para almacenar las evidencias de trabajos, tareas o proyectos.

¿Cuáles son las prácticas seguras y preventivas que construyen la reputación digital de cada persona?

- Evite compartir archivos, anuncios, con contenido que podría ser amenazador, abusivo, malicioso, agraviante, difamatorio, vulgar, obsceno, pornográfico, invasivo de la privacidad, y cualquier otro que genere responsabilidad disciplinaria estudiantil, civil o penal.
- Utilice la tecnología sin perjuicio de otras personas. Por ejemplo:
    - Suplantar la identidad de una persona o institución.
    - Utilizar imágenes o videos de personas sin autorización.
    - Hacer público contenidos sin autorización.
- Publique archivos que no contengan virus o cualquier otro código, archivos o programas diseñados para interrumpir, destruir o limitar la funcionalidad de cualquier software, hardware o equipo de computación y telecomunicaciones.

- Utilice un lenguaje respetuoso al comunicarse por cualquier medio con las personas docentes o personal institucional.
- Ejecute e instale únicamente las aplicaciones desde un origen legítimo como la tienda oficial de aplicaciones del dispositivo.
- Asegúrese de revisar las instrucciones detenidamente y brindar únicamente los permisos que sean necesarios cuando instale aplicaciones móviles. De lo contrario, estaría aceptando la extracción de información de usuario, por ejemplo: dar permisos de acceso a mensajes de texto/SMS, cámara, ubicación, contactos, micrófono, otros.
- Mantenga actualizados sus dispositivos y cualquier software o aplicaciones móviles que utilice. Las actualizaciones tienen como objetivo brindar mayor seguridad.
- Consulte a una persona mayor de edad o alguien que le pueda orientar sobre cómo actuar cuando reciba mensajes de contactos desconocidos. Se recomienda no abrir los enlaces o hipervínculos que algún contacto desconocido envíe por mensajería de texto o correo electrónico. Una buena práctica es no atender llamadas o mensajes de números telefónicos desconocidos o correos sospechosos.
- Verifique que los mensajes enviados por personas conocidas no contengan información sospechosa, podría significar que la lista de contactos y la cuenta de correo electrónico del remitente están comprometidas. Busque contactar a la persona por otros medios y describa y alerte del correo que ha recibido, confirme si es legítimo.
- Revise con cuidado los mensajes en los que se pide realizar acciones comprometedoras, por ejemplo: “¡Cuidado! Han intentado entrar a su cuenta. Vamos a bloquear su cuenta por 2 días si no sigue estos pasos”. Estos mensajes deben eliminarse y nunca responderse.
- Evite caer en este tipo de amenazas, y como precaución, se puede cambiar la contraseña de su correo institucional, esta opción la puede gestionar en la dirección: https://www.mep.go.cr/correo-mep
- Conecte su equipo a una red con internet segura, para que el sistema operativo, las aplicaciones y, especialmente el antivirus, cuenten con las actualizaciones correspondientes.

- Utilice fuentes oficiales y confiables para informarse, desconfíe de cadenas de mensajes donde no se proporcione datos válidos y no se referencie la fuente.
- Ingrese a las siguientes direcciones electrónicas para conocer acerca de comportamientos inadecuados y acciones que puede aplicar en diversas situaciones
    - Protocolos de actuación en situaciones de violencia en los Centros Educativos, acceda a través del enlace: http://www.mep.go.cr/protocolos/index.html
    - Ruta para denunciar el sexting, grooming y sextorsión, acceda a través del enlace: https://ementores.org/caja-de-herramientas/descargables/rutapara-denunciar-el-sexting-grooming-y-sextorsion
    - Crianza tecnológica, Viviendo la Ciudadanía Digital, acceda a través del enlace: https://crianzatecnologica.paniamordigital.org/
- Recuerde que en Costa Rica se cuenta desde el 2012, con la Ley de Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048, la cual debe ser conocida por todas las personas que usan dispositivos electrónicos, para que, de esta forma, en el momento en que se sientan vulnerables o que están siendo víctimas de algún tipo delito informático, puedan denunciarlo por la línea confidencial del Organismo de Investigación Judicial: 800-8000645.

¿Qué debe hacer para interactuar correctamente en los ambientes virtuales?

- Evite la redacción de textos en mayúscula, en los blogs, foros, correos, diarios, chat y wikis. Hacerlo de esta forma es como si estuviera gritando. (~~¿HOLA COMO ESTAS?~~).
- Utilice un lenguaje apropiado, respetuoso y amigable. Es importante realizar comentarios libres de insultos o que descalifiquen las posiciones de otras personas.
- Use con moderación los símbolos o emoticones () y si los utiliza, recuerde editar el texto alternativo, es decir, ¿cómo describiría de forma sencilla y concreta, ese símbolo o emoticón a una persona ciega?

- Redacte los mensajes sin abreviaturas. Por ejemplo: porque (xq), que (q), debe (db), se (c).
- Recuerde utilizar un lenguaje claro, de lectura fácil, para que sea accesible a la mayor cantidad de personas.
- Utilice negrita, cursiva o comillas para destacar un texto. Se recomienda no utilizar textos de diversos colores o usar subrayado (se puede confundir con un enlace web).
- Informe en el mensaje o contenido del correo cuando se adjunta uno o varios archivos (Ejemplo: adjunto los documentos solicitados).
- Revise los mensajes antes de enviarlos para verificar que son comprensibles.
- Verifique que el título del asunto tenga correspondencia con el contenido del mensaje.
- Utilice el chat para hacer consultas o comentarios relacionados con el tema que se desarrolla, no para iniciar conversaciones con otras personas participantes. También se utiliza el chat para anunciar que necesita retirarse un momento de la actividad.
- Sea puntual al ingresar en las salas de videoconferencia o chat, preferiblemente algunos minutos antes de la hora indicada.
- Revise que durante la videoconferencia el micrófono y la cámara estén apagados y cuide habilitarlos solamente cuando se requiera.
- Utilice el chat para pedir la palabra y abrir el micrófono para hablar cuando la persona que administra la videoconferencia lo indique.
- Elija un lugar para trabajar donde, en la medida de lo posible, no tenga interferencias en la comunicación.
- Cuando el anfitrión o moderador de la videoconferencia dé las indicaciones de que finaliza, despídase del grupo, preferiblemente por el chat.