VICEMINISTERIO ADMINISTRATIVO
DIRECCIÓN INFORMÁTICA DE GESTIÓN
"Educar para una nueva ciudadanía"

CIRCULAR

DVM-A-DIG-001-2020

De: Jose Sandí Zuñiga
Director

JOSE MANUEL SANDI ZUÑIGA (FIRMA)
Firmado digitalmente por JOSE MANUEL SANDI ZUÑIGA (FIRMA)
Fecha: 2020.04.20 09:48:51 -06'00'

Para: Despacho Ministra de Educación
Despacho Viceministra Académica
Despacho Viceministra de Planificación y Coordinación Regional
Directores y Directoras Regionales de Educación
Supervisores y Supervisoras de Circuitos Escolares
Directores y Directoras de Centros Educativos Públicos
Funcionarios de Oficinas Centrales
Funcionarias y funcionarios en general
Ministerio de Educación Pública

V.B.: Steven González Cortés
Viceministro Administrativo

STEVEN GONZALEZ CORTES (FIRMA)
Firmado digitalmente por STEVEN GONZALEZ CORTES (FIRMA)
Fecha: 2020.04.20 13:01:15 -06'00'

Fecha: 20 de abril de 2020

Asunto: Recomendaciones sobre manejo de la seguridad en los equipos tecnológicos.

Estimados (as) funcionarios (as):

La organización operativa del Ministerio de Educación Pública se fundamenta en la Política Curricular, en la Política Educativa y en la Política en Tecnologías de la información y Comunicación. De esta última, se toma como principio de trabajo el eje denominado: Gestión de la seguridad de las Tecnologías de Información, desde el cual se justifica cada una de las orientaciones descritas a continuación, enfocadas en salvaguardar la integridad de quienes conforman la comunidad educativa nacional.

1) **Uso adecuado del correo institucional y la información confidencial**

El uso del correo institucional es primordial, dado que el proveedor del servicio de correo electrónico provee al Ministerio de Educación Pública una plataforma con protocolos de seguridad como lo son el uso de certificados digitales y configuraciones de seguridad, mediante la cual es viable la trazabilidad de los mensajes que son recibidos, para efectos de establecer un seguimiento del remitente. Condiciones que el usuario no podría obtener con una cuenta personal.

Desde esta perspectiva, se ofrecen las siguientes medidas para el uso del correo y protección de la contraseña y otros datos confidenciales:

- El Uso del correo MEP es exclusivo para comunicaciones relacionadas con el ámbito laboral y académico, en el caso de las personas estudiantes.
- Evite el envío de correos electrónicos que incluyan información confidencial, como contraseñas, números de tarjetas de crédito o débito, pines u otros métodos de identificación.
- No utilice la misma contraseña para todas las cuentas, sitios web, otros.
- Disponga contraseñas seguras, evite usar palabras de fácil identificación. Contraseñas seguras incluyen al menos 8 caracteres, una combinación de mayúsculas y minúsculas, al menos un número entre 0-9 y un símbolo.
- Cambios de contraseña periódicos.
- No revele su clave de red institucional y correo electrónico institucional, esta información es personal y confidencial.
- Si el equipo lo utiliza más de una persona, cree sesiones de usuario diferentes para evitar que otras personas accedan a información personal y sensible.
- Cierre siempre la sesión cuando termine su tarea en la aplicación.
- No marque la opción de guardar su contraseña cuando ingresa a una aplicación, ya sea en el celular, computadora, tablet o cualquier dispositivo electrónico, pues al tener guardada la clave, la aplicación inicia sin su autenticación y por ende si su equipo es extraviado, entonces cualquiera puede tener acceso con solo encenderlo, como las aplicaciones, Outlook, Skype, Zoom, Teams, Facebook, Instagram, entre otros.
- Es mejor digitar la contraseña, con esto ejercitará el cerebro y siempre la recordará.
- Nunca escriba sus contraseñas en un papel y mucho menos guardarlas en su billetera, cartera, o libreta de contactos.

El Ministerio de Educación Pública, ni ningún ente Estatal, **nunca**, le solicitará datos de este tipo por correo electrónico o por ninguna aplicación.

2) Medidas personales para la protección del teléfono inteligente, tableta o computador.

- Solo ejecute e instale 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.

3) Acciones preventivas ante posibles intentos de estafas

Muchas de las estafas que se producen actualmente son conocidas como **phishing** (técnicas de suplantación de identidad y engaño, para ganar confianza de la víctima), las cuales se realizan mediante mensajes de correo electrónico, llamadas telefónicas, mensajes de texto, entre otros; cuyo objetivo es engañar a la persona usuaria, para proporcionar información confidencial, o inducir a seguir vínculos o datos adjuntos maliciosos.

Algunas estafas a partir de la suplantación de identidad (Phishing) pueden disfrazarse con mensajes de lo que parecen ser fuentes legítimas; como un banco, una institución oficial. El mensaje puede indicar que inicie sesión con su dirección de correo electrónico y contraseña, pero **cuidado** porque puede estar brindando información en un sitio web falso. Tome en cuenta que las estafas pueden estar disfrazadas de mensajes de correo electrónico provenientes de personas conocidas en los contextos personal, laboral y social o incluso familiares, esto para hacerlo caer en la trampa más fácilmente. En algunos de estos correos es posible que soliciten seguir un vínculo, abrir o descargar un archivo adjunto. Ante esta situación se recomienda tomar en cuenta lo siguiente:

- Si recibe un mensaje que parece sospechoso, siga este procedimiento:
    - Coloque el cursor sobre el vínculo que fue enviado al correo sin presionar el mismo, esto le permitirá observar el nombre de la entidad que remite, en otra ventana del navegador busque el nombre del sitio web y compruebe que el remitente sea real o conocido.
    - Busque el sitio web legítimo en lugar de hacer clic en un vínculo en el mensaje de correo electrónico.

- Asegúrese que el URL (URL es una dirección de Internet que, al ser encontrada y visualizada por un **navegador**, muestra un recurso de información al usuario) inicie con https y que tenga un candado.

- Si recibe un mensaje de un contacto conocido, pero contiene información sospechosa, podría significar que la lista de contactos y la cuenta de correo electrónico del remitente están comprometidas. Busque contactar al remitente por otros medios y describa y alerte del correo que ha recibido, confirme si es legítimo.

- Otra táctica utilizada en mensajes fraudulentos es intimidar al usuario, y forzar a realizar lo que están solicitando, por ejemplo: “**¡Cuidado! Han intentado entrar a su cuenta. Vamos a bloquear su cuenta en 2 días si no sigue estos pasos.**” Estos mensajes deben eliminarse y nunca responderse.

- Para evitar caer en este tipo de amenazas, y como precaución, se puede cambiar la contraseña de su correo institucional, esta opción la puede gestionar desde https://www.mep.go.cr/correo-mep.

4) Recomendaciones generales de seguridad para el trabajo a distancia

- En la red local del hogar, es recomendable cambiar la contraseña de la clave WIFI y del router, esto evita que otras personas que no tengan la contraseña puedan ingresar a la red.
- Nunca utilice aplicaciones en el celular o en la computadora, o tableta donde deba colocar datos confidenciales (números de cuenta, pines, contraseñas), en sitios con redes abiertas como por ejemplo: restaurantes, centros comerciales y otros.
- Hacer uso de sistemas operativos (Windows) sin la debida licencia del fabricante hace que no se pueda actualizar el mismo con frecuencia y de la forma correcta, lo que repercutirá en bajos niveles de seguridad sobre el equipo.
- Cualquiera que sea el software que se utilice para realizar video conferencias, asegúrese de que esté actualizado a la última versión.
- No se una a reuniones donde no conoce al anfitrión y/o participantes o la invitación no provenga de una fuente confiable.

- El dispositivo que utilice para realizar tareas del trabajo, no debe estar expuesto a que lo puedan utilizar otras personas, cierre sesiones de correo electrónico y de otras aplicaciones siempre que no las esté utilizando.
- Periódicamente realice respaldo de su información. Ante desastres o infecciones de cualquier tipo de virus es importante tener un plan B. Utilice dispositivos externos para realizar el respaldo (por ejemplo: disco duro extraíble, dispositivos de memoria USB, o la misma nube OneDrive).
- Es responsabilidad de cada persona, contar con un antivirus fiable y actualizado en cada uno de los dispositivos personales.
- Si utiliza dispositivos institucionales, debe conectarse a una red con internet segura, para que el sistema operativo, las aplicaciones y, especialmente el antivirus, cuenten con las actualizaciones correspondientes.
- En general, es una buena práctica no atender llamadas o mensajes de texto de números desconocidos, o cualquier otro que parezca sospechoso.

- Los enlaces o hipervínculos en mensajes de texto, se deben evitar si no son de fuentes confiables.

- Utilice fuentes oficiales y confiables para informarse, desconfíe de cadenas de mensajes donde no se proporcione datos válidos y no se referencie la fuente.

Como recomendación final, se le recuerda que en Costa Rica contamos, desde 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 usen dispositivos electrónicos, para que, de esta forma, en el momento en que crean o 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.

Atentamente,

Dirección de Informática de Gestión
San José, Edificio Rofas, 4to piso
Teléfono: 2256-8880
Correo electrónico: *direccioninformatica@mep.go.cr*