11. Política de Seguridad

11.1 Del uso prohibido

- El sistema de correo electrónico no debe ser usado para la creación, ni distribución de mensajes:

    - ofensivos o perjudiciales tales como mensajes de racismo, discriminación de género, edad, incapacidad, orientación sexual, mensajes pornográficos, o cualquier otro tipo de ofensa no mencionada en este apartado.
    - reenvío de mensajes SPAM o HOAX, o con contenido que pueda resultar ofensivo o dañino para otros usuarios (virus, pornografía)
    - cadenas de correo.
    - archivos que infrinjan derechos de autor (textos, software, música, imágenes o cualquier otro), claves legales o ilegales de software.
    - para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.
    - No utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes.
    - Proselitismo político y/o religioso.

- Empleados quienes reciban algún correo con algún contenido mencionado anteriormente por parte de algún otro empleado de la UANL, debe de reportarse a la Centro Institucional de Atención a Tecnologías de Información (CIATI) en la Dirección de Tecnologías de Información de forma inmediata.

- No deberá tratar de acceder información a la que no tenga derecho de acceso, aun cuando esa información no se encuentre debidamente protegida por el propietario de la misma. El hecho de que alguna información no esté protegida no le da derecho a accederla, copiarla, modificarla o divulgarla. En caso de algún usuario detecte información no protegida tiene la obligación de reportarle a la Coordinación de Seguridad Informática.

11.2 Del uso personal

El uso de la cuenta @uanl.mx es para uso institucional, si usted requiere manejar información personal le sugerimos tener una cuenta de un proveedor externo.

11.3 De la cuenta

No deberá dar acceso a su cuenta a otras personas. Su cuenta y los recursos que con ella le han sido asignados son de uso individual. Usted es el responsable de todas las operaciones e intentos de acceso legal o ilegal que se hagan en su cuenta o a través de ella, así como todos aquellos correos electrónicos que provengan de la misma.

Se recomienda cambiar su contraseña por la menos una vez al año, cuyas características deben cumplir los lineamientos de contraseñas establecidos por la Dirección de Tecnologías de Información.

Una contraseña débil es una puerta a través de la cual usuarios no autorizados podrán tener acceso al servicio y poner en riesgo su comunicación en este medio, así como la imagen pública de la Universidad Autónoma de Nuevo León.

11.4. Envío de Información

Deberá contar con la precaución adecuada para no enviar información a destinatarios erróneos, ya que esta puede ser utilizada para un mal manejo y es imposible de recuperar o evitar que llegue a su destinatario una vez que ha sido enviado.

11.5 Generales.

El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia, al aceptarla, el buzón otorgado por la institución, el usuario se compromete a:

- Evitar el envío de respuestas con copia A TODOS los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios salvo cuando se trate de una respuesta que por su naturaleza y/o contenido, necesariamente requiera ser conocida por todos ellos.

- No se permite la utilización del buzón de correo electrónico para fines comerciales diferentes a los que sean relativos al interés institucional.

- Depurar periódicamente el contenido del buzón de entrada en el servidor para evitar que los mensajes permanezcan en él un tiempo excesivo que conduzca a la congestión o el bloqueo del mismo.

- Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red institucional.

- Utilizar siempre un lenguaje apropiado en sus comunicaciones.

- Se recomienda el uso del Manual de Estilo UANL para la redacción de sus correos electrónicos en sus comunicaciones institucionales.

- Utilizar su cuenta únicamente para fines laborales, investigación o para los estrictamente relacionados con las actividades propias de su trabajo.

- Si sospecha que su cuenta está siendo usada en forma ilegal por otra persona, cambie su contraseña de acceso de inmediato.

- Reportar todos los correos que considere sospechosos o que no han sido solicitados por usted a las cuentas institucionales de soporte al servicio donde se les dará el tratamiento adecuado.

- Deberá reportar la cuenta cuando ya no la necesite. Una cuenta en desuso es una puerta a través de la cual usuarios no autorizados pueden tener acceso a RedUANL o a la red de Internet adivinando la contraseña de entrada. Usted es responsable de la cuenta aun cuando ya no la esté usando. La notificación de cancelación de la misma lo releva de esta responsabilidad.

- Todas las cuentas pertenecientes a usuarios de honorarios, proyectos especiales u otros similares tendrán una vigencia en el tiempo. Cinco días hábiles antes del vencimiento de su vigencia, el interesado deberá solicitar su renovación ante el responsable de informática y evitar la cancelación de la cuenta.

- La Institución se reserva el derecho de enviar al usuario toda información que considere necesaria o pertinente para garantizar un adecuado flujo de información interna, dado que el buzón se considera un medio de comunicación institucional. En ningún caso la información oficial que la institución entregue a sus usuarios a través del correo electrónico puede catalogarse como Correo No deseado (SPAM).

- La Dirección de Tecnologías de Información filtrará los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final estará sujeta a que el resultado de la comprobación sea positivo.

- El incumplimiento por parte del usuario de una o más de las obligaciones arriba descritas, puede ocasionar la suspensión y posterior baja del sistema de su cuenta de correo electrónico. Esta medida puede tomarse incluso con carácter preventivo y sin aviso previo, si llegará a detectarse alguna actividad ilegal o peligrosa originada en el buzón del usuario.