UANL.
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

DOI-049
REV. 07-03/23

Dirección General de Tecnologías y Desarrollo Digital

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA SERVICIOS

Índice

Contenido

Alcance

Esta política aplica a todas aquellas personas que interactúan con los servicios ofrecidos dentro del alcance de ISO 20000, por la Dirección General de Tecnologías y Desarrollo Digital de la Universidad Autónoma de Nuevo Leon.

Objetivo

Asegurar que los servicios ofrecidos por la Dirección y que se encuentran dentro del Alcance de ISO 20000, cubren los principios básicos de seguridad: Confidencialidad, Integridad y Disponibilidad, y así cumplir con los requerimientos legales y/o contractuales respecto a la protección de información.

Responsabilidades

Puesto/Rol	Responsabilidades
Coordinador de Seguridad	• Responsable de la elaboración, revisión y evaluación de la política de seguridad de la información. • Responsable de convocar a reuniones cuando existan cambios significativos en el entorno de la certificación, las circunstancias de negocio, las condiciones legales o el medio ambiente técnico y que es probable que tenga un impacto de la información o por lo menos una vez al año.
Dueños de servicio	• En conjunto con el coordinador de Seguridad se establecen los lineamientos requeridos para cubrir los requisitos mínimos de seguridad de la política. • Establecer, monitorear y mantener los controles que soportarán los lineamientos específicos de su servicio. • Cumplir con las políticas definidas por la Dirección.
Dueño del Subproceso de Mejora Continua	• Dar seguimiento a las mejoras que se deriven del análisis de las políticas de seguridad.
Dueño del Subproceso de Administración de la Continuidad	• En conjunto con el coordinador de Seguridad establecen la asociación entre análisis de riesgos y los controles que dan soporte a la presente política.
Usuario del servicio	• Cumplir las políticas de seguridad de la Dirección.

POLÍTICAS GENERALES PARA SERVICIOS

Del uso del servicio

Los servicios en general no deben ser usados para:

- Creación o 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.
- Para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.
- Utilización de identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes u otro tipo de comunicación.
- Proselitismo político y/o religioso.
- No utilizar el servicio con fines comerciales y/o diferentes a los que sean relativos al interés institucional.

Del tratamiento de información

Con respecto al uso de la información en los servicios:

- No deberá tratar de manipular información a la que no tenga derechos de acceso, aún y 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 de accederla, modificarla o divulgarla. En caso de que algún usuario detecte información no protegida tiene la obligación de reportarle al dueño del servicio o al coordinador de seguridad.
- 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 enviada o transmitida.
- Toda aquella información que por su clasificación sea considerada como confidencial deberá ser tratada con responsabilidad, otorgar el acceso a la misma deberá estar respaldado mediante un acuerdo de confidencialidad.

Del uso de la cuenta

Para aquellos servicios que por su naturaleza de funcionamiento y como medida de control de acceso se ha establecido una cuenta de usuario se establecen las presentes clausulas generales:

- No deberá dar a acceso a su cuenta a otras personas. Su cuenta y los recursos que con ella han sido asignados son de uso individual/institucional. Usted es el responsable de todas las operaciones e intentos de acceso legal e ilegal que se hagan en su cuenta o a través de ella.
- Se recomienda cambiar su contraseña por lo menos dos veces al año, cuyas características deben cumplir los lineamientos 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 y/o servicio, así como la imagen pública de la Universidad Autónoma de Nuevo León.

El usuario es el único responsable por el buen uso de su cuenta del servicio. En consecuencia, al aceptarla, el usuario se compromete a:

- 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.
- Utilizar su cuenta únicamente para fines laborales, investigación o para los temas estrictamente relacionados con las actividades propias de su trabajo o actividad académica.
- Si sospecha que su cuenta está siendo usada de forma ilegal por otra persona, cambie o solicite a su dependencia el cambio de su contraseña de acceso de inmediato (usuario) y/o notifique inmediatamente al administrador de servicio a través de una solicitud de servicio al Centro de Ayuda.
- 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 información confidencial o privada. Usted es responsable de la cuenta aún y cuando ya no la esté usando. La notificación de cancelación de la misma lo releva de esta responsabilidad.

POLÍTICAS PARTICULARES POR SERVICIOS

En el presente apartado se establecen aquellas condiciones particulares que adicionalmente a lo ya declarado en otras políticas de seguridad (DOI-099), deberán considerarse para los diferentes servicios que están en el alcance de esta política.

CONDICIONES PARTICULARES PARA EL SERVICIO DE CORREO ADMINISTRATIVO

- Reenvío de mensajes SPAM o HOAX, o con contenido que pueda resultar ofensivo o dañino para otros usuarios (malware, pornografía).
- Envió de cadenas de correo.
- Envió de archivos que infrinjan derechos de autor (textos, software, música, imágenes o cualquier otro), claves legales o ilegales de software.

Usuarios quienes reciban correo con algún contenido mencionado anteriormente, deberán reportarse al correo reportar.spam@uanl.mx de forma inmediata o bien, al Centro de Ayuda.

- 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.
- Al aceptar la cuenta 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.
    - Todas las cuentas pertenecientes a usuarios honorarios, proyectos especiales u otros similares tendrán una vigencia en el tiempo. Antes del vencimiento de su vigencia, el interesado deberá solicitar su renovación ante el responsable de informática y evitar la cancelación de su cuenta.
    - La institución se reserva el derecho de enviar al usuario toda información que considera 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 General de Tecnologías y Desarrollo Digital 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.

INCUMPLIMIENTO DE LAS CONDICIONES GENERALES DE LA POLÍTICA

El incumplimiento por parte del usuario de una o más de las obligaciones arriba descritas, puede ocasionar la cancelación temporal o permanente de su acceso al servicio, a su vez se notificará al responsable de la dependencia para que aplique las sanciones adicionales que correspondan. Esta medida puede tomarse incluso con carácter preventivo y sin previo aviso, si llegara a detectarse alguna actividad ilegal o inapropiada originada por el usuario.