Dirección de Tecnologías de Información

Política General de Seguridad de la Información para Servicios

Versión 3.0

Fecha: *09/03/2018*

Generales			
Descripción	Es un documento define los lineamiento para el control de la seguridad de la información manejada por la Junta Directiva de TI.		
Propósito	El propósito de esta política es dar a conocer al lector los lineamientos a cumplir por todos los usuarios en materia de seguridad de la información y coadyuvar al cumplimiento.		
Propietario del Documento	Coordinador de Seguridad	Organización	Dirección de Tecnologías de Información
Fechas de la revisión del documento	09/03/2018	Fecha de próxima Revisión	08/03/2019

Autorizado Comité Directivo de Seguridad		
Fecha	**Nombre y puesto**	**Firma**
09/03/2018	Dr. Alberto Zambrano Elizondo Director de Tecnologías de Información	
09/03/2018	M.A. Tomas Rodriguez Elizondo Subdirector de Proyectos y Servicios	
09/03/2018	Ing. Noel A. Hortiales Corona Subdirector de Computo y Software	
09/03/2018	Ing. Gerardo Treviño Barrera Subdirector de Sistemas Administrativos	
09/03/2018	Ing. Jesus Cuauhtemoc Valero Cantú Subdirector de Telecomunicaciones	
09/03/2018	Ing. Joaquin Huante Hernandez Subdirector de Sistemas Académicos	
09/03/2018	Lic. Gerardo Bernal Carranza Coordinador de Seguridad Informática	
09/03/2018	Ing. Diego Vidal Luna Rodriguez Administrador de Seguridad	
09/03/2018	Lic. Erick Hiram Tapia Martinez Responsable de Seguridad de la Red	

Autorizado dueños de servicios			
Fecha	**Responsable del servicio**	**Servicio**	**Firma**
09/03/2018	M.A. Sara Ivette Rodulfo Hdz Coordinadora de Plataforma Tecnológica	Comunidad	
		Correo Administrativo	
09/03/2018	Lic. Dagoberto Salas Zendejo Coordinador de Sistemas de Bibliotecas	Administración Integral de Bibliotecas	
09/03/2018	Lic. Jose Joel Silva Zamarripa Coordinador de Sistemas Informáticos de Enseñanza-Aprendizaje	Enseñanza y Aprendizaje en Línea	

09/03/2018	Lic. Abel Castro Garcia Coordinador de Sistemas de Información para la Calidad	Gestión de Calidad	
09/03/2018	M.A. Samuel Efren Garcia Gonzalez Coordinador de Sistemas de RH	Recursos Humanos y Nominas	
09/03/2018	M.C. Mayra Silva Almanza Coordinador de Servicios Web	Portal UANL	
09/03/2018	Ing. Jaime Zamarripa Cervantes Responsable Programador Analista	SIASE Recursos Humanos	
09/03/2018	Ing. Juan Jesus Villarreal Garcia Responsable de Operación de Telefonía	Red Telefónica Institucional (UANL)	
09/03/2018	M.C. Humberto Jorge Orozco Barron Coordinador de Red de Servicios Integrados	Internet	
09/03/2018	Ing. Juan Javier Quiroga Garza Coordinador de Soporte a Sistemas	Digitalización de Documentos	
09/03/2018	M.A. Martin Daniel Ortiz Galvan Coordinador de Sistemas de Información Ejecutiva	Generación de Indicadores Ejecutivos	
09/03/2018	Victor Adiel Reyna Villarreal Responsable de Sistemas Escolares	SIASE Servicio Social	
		SIASE Unibolsa	
09/03/2018	Lic. Pamela Rocio Reyna Santoy Responsable Analista Programador	SIASE Tutorias	
		SIASE Prácticas Profesionales	
09/03/2018	Tec. Manuel Rodriguez Morales Coordinador de Servicios Audiovisuales	Videoconferencia	
09/03/2018	Sergio Eduardo Rocha Mendoza Coordinador Sistemas de Sorteos	Soporte a Sorteos	
09/03/2018	M.I. Linda Lisbeth Gaxiola Lucio Coordinador de Desarrollo e Implementación de Sistemas	Administración H. Consejo	

Historial de Versiones			
Versión	Fecha de Actualización / Creación / Revisión	Responsable de Actualización / Creación / Revisión	**Resumen de Cambios**
V1.0	29/08/2013	Lic. Gerardo Bernal Carranza	Generación de Plantilla.
V3.0	06/02/2018	Lic. Gerardo Bernal Carranza	Generación de Plantilla nueva para restructuración de política.

Contenido

1 Introducción

La información es uno de los activos más importantes de **la Universidad Autónoma de Nuevo León,** es esencial que todos entiendan el valor de la información y su responsabilidad individual y colectiva para protegerlo, **la Universidad Autónoma de Nuevo León** debe ser capaz de demostrar que ha ejercido la debida diligencia en la protección de la información y de este modo puede defender su derecho a la información, tomar las medidas legales apropiadas, hasta incluso remitir el asunto a las autoridades gubernamentales para un enjuiciamiento legal.
Además, el valor de la vida privada de un individuo se mantiene en alta estima y se compromete a gestionar y proteger la información de identificación personal como se establece en esta política.
Además, reconoce la necesidad de establecer políticas de seguridad y privacidad, así como prácticas para cumplir los requisitos legales vigentes, así como prepararse adecuadamente para cumplir razonablemente con las leyes y reglamentos.
Por último, la **Universidad Autónoma de Nuevo León** reconoce que, con el fin de apoyar las operaciones de la institución, tendrá que equilibrar su seguridad y los esfuerzos de privacidad con sus objetivos de negocio generales.

2 Alcance

Esta política aplica a todas aquellas personas que interactúan con los servicios ofrecidos por la Dirección de Tecnologías de Información de la Universidad Autónoma de Nuevo Leon.

3 Responsabilidades

Puesto/Rol	Responsabilidades
Dueño del Subproceso de Seguridad de la Información	• 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 coordinación el dueño del subproceso de seguridad establecer 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 en este documento.
Analista de Seguridad	• Si existe un rol establecido para el servicio apoyará al dueño de servicio en el monitoreo y detección de incidentes de seguridad para el servicio.
Dueño de Subproceso de Portafolio de Servicios	• Hacer las recomendaciones de acuerdo al proceso que tenga a cargo.
Dueño del Subproceso de Mejora Continua	• Hacer las recomendaciones de acuerdo al proceso que tenga a cargo.
Dueño del Subproceso de Administración de la Continuidad	• En coordinación con el dueño del subproceso de seguridad establecer la asociación entre análisis de riesgos y los controles que dan soporte a la presente política.
Usuario del servicio	• Cumplir las políticas definidas en este documento.

4 Definiciones

UANL. - Universidad Autónoma de Nuevo León.

Terceros. - Se refiere a cualquier empresa, institución académica o de investigación, proveedores o entidades de gobierno u organizaciones externas que necesitan establecer una relación con la UANL.

CIATI. - Centro Institucional de Atención en Tecnología de Información, se trata del centro principal de contacto de la Dirección de Tecnologías de Información a través del cual se brindan la atención a los principales servicios de la Dirección.

DTI. - Dirección de Tecnologías de Información.

5 Objetivos

Asegurar que los servicios ofrecidos por la DTI 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.

6 Aplicabilidad

La presente política aplica para todos aquellos servicios certificados en el alcance de la certificación ISO 20000.

7 Principios clave de privacidad

La UANL emplea los siguientes principios de privacidad de la información para conducir el uso de los servicios ofrecidos por la DTI:

- Información de identificación del personal puede ser compartida para cubrir requerimientos legales como órdenes emitidas por un juez, requerimientos de licencias o propósitos similares, además de que dicho requerimiento haya sido aprobado por la oficina del Abogado General.
- Terceros pueden acceder a la información de identificación del personal solo por medio de un acuerdo de confidencialidad para proteger la adecuada confidencialidad, integridad y disponibilidad de dicha información. Dicho acuerdo deberá ser validado por la oficina del Abogado General de la UANL, la DTI proporcionará una guía para la utilización y gestión de los acuerdos de confidencialidad.
- Todos los usuarios de los cuales la institución recopile información de identificación personal deberán de ser informados a través del correspondiente aviso de privacidad que establece La Unidad de Transparencia de la UANL (http://transparencia.uanl.mx).
- Los usuarios serán informados de cómo su información de identificación personal será recolectada usada y compartida.
- Todos los usuarios serán provistos de un medio razonable de actualización de sus datos de identificación personal.
- La UANL considerará las restricciones de costo y funcionalidad para lograr un riesgo aceptable con respecto a las actividades de privacidad y seguridad de la información
- Todos los usuarios podrán ejercer los derechos a acceso, rectificación, cancelación y oposición (ARCO) de acuerdo a como lo establece la Ley Federal de Protección de Datos Personales y El Reglamento de Transparencia y Acceso a la Información de la Universidad Autónoma de Nuevo León.

8 Principios clave de seguridad

Para soportar las premisas básicas y objetivos establecidos, la UANL emplea los siguientes principios de seguridad para conducirse:

- Siempre que sea factible la información será marcada de tal manera que demuestre la propiedad de la UANL, como símbolos que pueden incluir, etiquetas de clasificación, etiquetas de activo fijo, notas de derecho de autor, marca comercial, firma digital, etc.
- La información protegida y confidencial no podrá ser revelada a terceros sin el debido consentimiento de la UANL y a través de un acuerdo claramente establecido, siguiendo lo previamente establecido para acuerdos de confidencialidad.
- La UANL se esforzará por mejorar sus sistemas y procesos de seguridad siguiendo las mejoras prácticas y estándares de seguridad.

9 Clasificación de la información

Para clasificar un activo de información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

- **Información Confidencial**

  Se considera información confidencial respecto a los servicios ofrecidos por la DTI a la información de carácter técnico como lo son nombres de equipo, configuraciones de red, seguridad, respaldo, software y aplicaciones, información de configuración del sistema, además de toda aquella información clasificada como tal dentro de El Reglamento de Transparencia y Acceso a la Información de la Universidad Autónoma de Nuevo León.

- **Información protegida**

  Se considera información protegida a toda aquella información de los servicios ofrecidos por la DTI para la que se requiera una cuenta y contraseña, como lo es toda información que influye en el flujo de trabajo de los usuarios autorizados. Además, toda aquella información que es necesaria para dar seguimiento/mantenimiento al servicio como: información de proyectos, planes de trabajo, proceso de certificación, procedimientos, evaluaciones de seguridad, políticas internas, etc.

- **Información Pública**

  Se considera información pública a toda aquella información de los servicios ofrecidos por la DTI para la que no se requiere cuenta y contraseña y que está disponible a través del portal Web del servicio, así como cualquier información de consulta e intercambio entre instituciones nacionales e internacionales con las cuales se tiene colaboración.

10 Análisis y Gestión de Riesgos

La DTI a través de la administración de continuidad establece la gestión y análisis de riesgos de los diferentes servicios establecidos por el alcance de la política.

Este proceso identifica los riesgos asociados a los servicios y/o sus componentes con el fin de establecer los controles de seguridad de información administrativos y técnicos que nos permitan preservar la confidencialidad, integridad y accesibilidad de los servicios y a su vez cumplir con los objetivos de la gestión de la seguridad de información.

Los controles de seguridad de la información son apropiadamente documentados en el DOI-050 Controles de Seguridad como parte del proceso de gestión de la seguridad. Y como parte de la gestión y análisis de riesgos de los diferentes servicios se realiza un análisis de riegos documentado en RC-SER-07-101 así como análisis de impacto al negocio documentado en RC-SER-07-100.

11 Política de Seguridad

11.1 Políticas generales

Las siguientes serán consideradas cláusulas generales que aplican a todos los servicios del alcance de esta política:

11.1.1 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.

11.1.2 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.

11.1.3 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 CIATI.
- 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.

11.2 Políticas particulares por servicios

En el presente apartado se establecen aquellas condiciones particulares que adicionalmente a lo ya declarado en la sección de general deberá tenerse en cuenta para los diferentes servicios que están en el alcance de esta política.

11.2.1 Condiciones particulares para el servicio Enseñanza y Aprendizaje en Línea (NEXUS)

Adicional a lo establecido en las clausulas generales del uso del servicio, Enseñanza y Aprendizaje en Línea (NEXUS) no debe ser usado para:

- Cargar o distribuir archivos que infrinjan derechos de autor (textos, software, música, imágenes o cualquier otro), claves legales o ilegales de software.

La Dirección de Tecnologías de información filtrará los archivos que sean cargados por los usuarios del sistema para verificar la ausencia de virus. La carga definitiva de todo archivo estará sujeta a que el resultado de la comprobación esté libre de virus.

11.2.2 Condiciones particulares para el servicio Gestión de Calidad

Adicional a lo establecido en las clausulas generales del uso de la cuenta, las cuentas de Gestión de Calidad:

- Todas las cuentas de los usuarios generados de manera manual como son las cuentas con terminación @uanl.edu.mx son responsabilidad de la dependencia.

11.2.3 Condiciones particulares para el servicio Red Telefónica Institucional (UANL)

El servicio de la red telefónica es distinto en su forma de entrega y gestión, las siguientes son sus condiciones particulares no exceptuando aquello que pueda aplicar en las clausulas generales.

Del uso prohibió del servicio.

- El servicio de la red telefónica de la UANL 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, acoso, difamación, calumnia, mensajes pornográficos, creencias y prácticas religiosas, creencias políticas o cualquier otro tipo de ofensa no mencionada en este apartado.
- Empleados quienes reciban alguna llamada con algún contenido mencionado anteriormente deberá reportarse a la Dirección de Tecnologías de Información de forma inmediata.
- La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario responsable, sin perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.
- No utilizar identidades ficticias o pertenecientes a otros usuarios para la realización de llamadas.
- No utilizar el aparato telefónico y/o clave telefónica para fines comerciales diferentes a los que sean relativos al interés institucional.

Del uso adecuado

- El uso de la red telefónica UANL deberá ser única y exclusivamente por empleados vigentes de la Universidad Autónoma de Nuevo León.
- Con el fin de asegurar la aplicación del buen uso de la red de telefonía UANL se deben seguir los pasos necesarios para cumplir con las siguientes premisas:
  - **Validación de privilegios en la red telefónica**:
    - El director o responsable de la dependencia deberá validar a su criterio que tipo de privilegio le otorgara a la persona a quien desean darle acceso a una clave telefónica, esto para realizar llamadas específicamente del trabajo que realice a su cargo.
    - Los niveles de privilegio de los códigos de acceso telefónico son los siguientes:
      a) Llamadas locales.
      b) Llamadas a celular.
      c) Llamadas larga distancia nacional.
      d) Llamadas larga distancia mundial.

  - **Alta, Cambio o Baja de claves telefónicas**
    - Para realizar un alta de una(s) claves(s) telefónica(s) se deberá de mandar un oficio firmado de director a director, indicando el nombre completo de la persona, así como el privilegio que va a contener dicha clave que están requiriendo.
    - Para la realización de un cambio de una(s) clave(s) telefónica(s) se deberá de mandar un oficio firmado de director a director, indicando que tipo de cambio se realizará, por ejemplo, un cambio de código o cambio de privilegio.
  - **Monitoreo de la actividad de los usuarios**
    - Para monitorear la actividad de los usuarios en el uso de las claves telefónicas se deberá de solicitar por parte del director o responsable vía un oficio solicitando la validación de la(s) clave(s) telefónica(s) o extensión(es) que soliciten monitorear para validar la actividad de llamadas que estuvieron realizando y así los responsables o el director de la dependencia tomen acciones con los usuarios plasmados en dicho reporte.

- **Suspensión del servicio de red telefónica**
  - En dado caso que se le encuentre a un usuario haciendo mal uso de alguna clave telefónica, se le suspenderá la clave dándola de baja por un tiempo indefinido mientras su director o responsable considere otorgarle de nuevo este privilegio.

- **Del uso personal**
  - El uso de la red telefónica UANL deberá ser única y exclusivamente para la realización o recepción de llamadas con fines institucionales o de trabajo relacionado a la UANL y no para uso o beneficio personal.
- **De la clave telefónica de acceso a la red telefónica publica**
  - No deberá compartir su clave telefónica a otras personas. Su clave telefónica es de uso personal. Usted es el responsable de todas las operaciones e intentos de acceso legal e ilegal que se hagan en su clave telefónica o a través de ella.
- **Del mal trato y daño intencional al aparato telefónico**
  - En caso de ser dañado intencionalmente el equipo, se hará acreedor a una sanción que designaran las autoridades correspondientes, así como el robo del aparato.
- **Del intento de acceso a los equipos de control y administración de los teléfonos**
  - No se deberá intentar tener acceso a los equipos de control y administración de la red telefónica, así como el intento de hacer cambios en configuraciones o modificaciones.

11.2.4 Condiciones particulares para el servicio de Correo Administrativos

Adicional a lo establecido en las clausulas general respecto al uso del servicio, el servicio de Correo Administrativo no debe ser usado para:

- Re-envió 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 por parte de algún otro empleado de la UANL, debe reportarse al Centro Institucional de Atención a Tecnologías de Información (CIATI) en la Dirección de Tecnologías de Información de forma inmediata.

Usuarios quienes reciban correo con algún contenido mencionado anteriormente o que por sospecha o duda de su legitimidad lo consideren sospechoso y/o provengan de un remitente desconocido deberá reportar a través de los canales de seguimiento oficiales.

Además de lo establecido en las clausulas generales, también se deberán atender las siguientes para el servicio de Correo Administrativo:

- 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.
- Se recomienda el uso del Manual de Estilo UANL para la redacción de sus correos electrónicos en sus comunicaciones institucionales.
- Todas las cuentas pertenecientes a usuarios 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 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 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.

11.2.5 Condiciones particulares para el servicio de Administración Integral de Bibliotecas (CODICE)

Para el servicio de Administración Integral de Bibliotecas (CODICE) se consideran las siguientes clausulas particulares respecto a las cuentas además lo que previamente estipulado en las generales:

- Todas las cuentas administrativas tendrán una vigencia en el tiempo de un año. El sistema CODICE le notificará cuando esté próxima a vencer, para lo cual el interesado deberá solicitar la renovación a través de una solicitud de servicio al CIATI dirigida al administrador de CODICE para evitar la cancelación de la cuenta. La vigencia de las cuentas de los usuarios finales es responsabilidad de la biblioteca.

11.2.6 Condiciones particulares para el servicio SIASE Recursos Humanos

Para el servicio de SIASE Recursos Humanos se consideran las siguientes clausulas respecto a las cuentas de servicio, adicionales a las establecidas en general:

- Todas las cuentas administrativas tendrán una vigencia de un año. Para lo cual el interesado deberá solicitar la renovación a través de una solicitud de servicio al CIATI dirigida al dueño del servicio para evitar la cancelación de la cuenta. La vigencia de las cuentas de los usuarios finales es responsabilidad de la dependencia.

11.2.7 Condiciones particulares para el servicio Portal UANL

Para el servicio de Portal UANL se considera de manera adicional las siguientes clausulas respecto a las cuentas:

- En caso de que el personal responsable de sitios web de las dependencias sea dado de baja, el director de la dependencia deberá notificar a la Dirección de Portal Web para que sea eliminada su cuenta de manera definitiva.

- En caso de los usuarios finales, éstos no requieren de cuenta de acceso y la información a la que pueden acceder es pública y abierta a través de Portal UANL www.uanl.mx.

11.2.8 Condiciones particulares para el servicio SIASE Tutorías

Para el servicio de SIASE Tutorías se consideran las siguientes clausulas respecto a las cuentas de servicio, adicionales a las establecidas en general:

- Todas las cuentas administrativas tendrán una vigencia de un año. Para lo cual el interesado deberá solicitar la renovación a través de una solicitud de servicio al CIATI dirigida al dueño del servicio para evitar la cancelación de la cuenta. La vigencia de las cuentas de los usuarios finales es responsabilidad de la dependencia.

11.2.9 Condiciones particulares para el servicio SIASE Prácticas Profesionales

Para el servicio de SIASE Prácticas Profesionales se consideran las siguientes clausulas respecto a las cuentas de servicio, adicionales a las establecidas en general:

- Todas las cuentas administrativas tendrán una vigencia de un año. Para lo cual el interesado deberá solicitar la renovación a través de una solicitud de servicio al CIATI dirigida al dueño del servicio para evitar la cancelación de la cuenta. La vigencia de las cuentas de los usuarios finales es responsabilidad de la dependencia.

11.2.10 Condiciones particulares para el servicio SIASE Unibolsa

Para el servicio de SIASE Unibolsa se consideran las siguientes clausulas respecto a las cuentas de servicio, adicionales a las establecidas en general:

- Todas las cuentas administrativas tendrán una vigencia de un año. Para lo cual el interesado deberá solicitar la renovación a través de una solicitud de servicio al CIATI dirigida al dueño del servicio para evitar la cancelación de la cuenta. La vigencia de las cuentas de los usuarios finales es responsabilidad de la dependencia.

11.2.11 Condiciones particulares para el servicio SIASE Servicio Social

Para el servicio de SIASE Servicio Social se consideran las siguientes clausulas respecto a las cuentas de servicio, adicionales a las establecidas en general:

- Todas las cuentas administrativas tendrán una vigencia de un año. Para lo cual el interesado deberá solicitar la renovación a través de una solicitud de servicio al CIATI dirigida al dueño del servicio para evitar la cancelación de la cuenta. La vigencia de las cuentas de los usuarios finales es responsabilidad de la dependencia.

11.2.12 Condiciones particulares para el servicio Digitalización de Documentos

Adicional a lo estipulado en las condiciones generales, las siguientes clausulas son particulares para el servicio Digitalización de Documentos:

- El uso del servicio es exclusivamente para el resguardo y administración de documentos para los que fue diseñado y configurado con fines institucionales. Por lo cual deberá abstenerse de cargar cualquier archivo

no contemplado como lo son textos, software, música, imágenes o cualquier otro contenido no estipulado en el catálogo de servicio.

11.2.13 Condiciones particulares para el servicio de Videoconferencia

El servicio de videoconferencia es distinto en su forma de entrega y gestión, las siguientes son sus condiciones particulares no exceptuando aquello que pueda aplicar en las clausulas generales.

Del uso prohibido del servicio.

- El servicio de videoconferencia (UANL) 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, acoso, difamación, calumnia, mensajes pornográficos, creencias y prácticas religiosas, creencias políticas o cualquier otro tipo de ofensa no mencionada en este apartado.
- La violación de esta obligación origina automáticamente la suspensión del servicio y puede ser causa de sanciones al usuario responsable, sin perjuicio de las responsabilidades que eventualmente puedan surgir ante la ley.
- Si durante el enlace reciben algún tipo de contenido mencionado anteriormente al equipo de videoconferencia deberá reportarse a la Dirección de Tecnologías de Información de forma inmediata.
- No utilizar identidades ficticias o pertenecientes a otros usuarios para la realización de videoconferencias
- No utilizar el equipo de videoconferencia para fines comerciales diferentes a los que sean relativos al interés institucional.

Del uso adecuado

- El uso de videoconferencia deberá ser única y exclusivamente por empleados vigentes de la Universidad Autónoma de Nuevo León. (responsables de informática)
- Con el fin de asegurar la aplicación del buen uso de videoconferencia se deben seguir los pasos necesarios para cumplir con las siguientes premisas:
  - **Alta, Cambio o Baja de salas de videoconferencia**
    - Para realizar un alta de una sala de videoconferencia se deberá de mandar un oficio firmado de director a director, indicando la información requerida para dar de alta en la red de Videoconferencia de la UANL, así como el nombre completo de la persona responsable de dicha sala
    - Para la realización de un cambio de una sala de videoconferencia se deberá de mandar un oficio firmado de director a director, indicando que tipo de cambio se realizará
  - **De la actividad de los usuarios**
    - No establecer comunicaciones con desconocidos o que no estén dentro de nuestra lista de contactos.
    - Verificar la identidad de los contactos por otros medios, sobre todo cuando se va a iniciar una videoconferencia por primera vez con ellos.
    - Utilizar perfiles de usuario con autenticación mediante contraseña segura, para evitar el acceso por usuarios no autorizados.
    - Mantener actualizado el software de los sistemas de videoconferencia.
    - Deshabilitar la compartición de contenido por defecto. Habilitar solo cuando sea necesario.
    - Deshabilitar la recepción de video por defecto. Habilitar solo cuando sea necesario.

- Cubrir la cámara cuando el sistema no está en uso. También, configurar la cámara para que, al comenzar una videoconferencia, muestre una imagen neutra que no muestre información comprometida, en caso de establecer una conexión errónea.
- Apagar o silenciar los micrófonos cuando el sistema no está en uso.
- Concienciar y formar a los usuarios sobre la necesidad de aplicar estas precauciones de seguridad. El responsable de la dependencia deberá validar a su criterio para saber qué audiencia estará en la sala donde se realice la videoconferencia.

◦ **Del uso personal**
- El uso del equipo de videoconferencia deberá ser única y exclusivamente para la recepción de enlaces de videoconferencias con fines institucionales o de trabajo relacionado a la UANL y no para uso o beneficio personal.

◦ **Del intento de acceso a los equipos de videoconferencia**
- No se deberá intentar hacer cambios en configuraciones o modificaciones.

11.2.14 Condiciones particulares para el servicio Soporte a Sorteos

Las siguientes premisas son consideradas particulares para el servicio Soporte a Sorteos respecto a las cuentas:

- Las cuentas de acceso al servicio serán otorgadas exclusivamente a personal de Promotora de Eventos para la Siembra Cultural, toda aquella solicitud ajena a este requisito deberá ser evaluada por la DTI en conjunto con Promotora de Eventos.

11.3 Del 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, en forma independiente de las sanciones especificas a que se haga acreedor por la infracción cometida. 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.

11.4 Del incumplimiento de condiciones particulares de las políticas

Adicional a los incumplimientos de las condiciones generales existen ciertas condiciones particulares o específicas de algunos servicios que se mencionan a continuación.

Respecto al servicio Gestión de Calidad

- En usuarios administrativos, adicionalmente a lo antes descrito, el administrador del sistema KAIZEN informará al responsable de la dependencia a fin de que éste emita la sanción correspondiente.

Respecto al servicio de la Red Telefónica Institucional (UANL)

- 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 extensión telefónica y/o clave de acceso telefónico. Esta medida puede tomarse incluso con carácter preventivo y sin aviso previo, si llegará a detectarse alguna actividad ilegal o peligrosa originada en la extensión y/o clave telefónica del usuario.

Respecto al servicio de Administración Integral de Bibliotecas (CODICE)

- En usuarios administrativos, adicionalmente a lo antes descrito, el administrador del sistema CODICE informará al responsable de biblioteca a fin de que éste emita la sanción correspondiente.

Respecto al servicio de Videoconferencia

- Suspensión del servicio de videoconferencia

  En dado caso que se le encuentre a un usuario haciendo mal uso del equipo de videoconferencia, se le suspenderá el enlace por un tiempo indefinido mientras su director o responsable considere otorgarle de nuevo este privilegio.

- Del mal trato y daño intencional al aparato de videoconferencia

  En caso de ser dañado intencionalmente el equipo, se hará acreedor a una sanción que designaran las autoridades correspondientes, así como el robo del aparato.

12 VIGENCIA

La presente política tiene vigencia de un año, es responsabilidad del Dueño del Subproceso de Seguridad de la Información su actualización que deberá ser revisada y aprobada por el comité de seguridad.