ÚNICA

INSTITUCIÓN UNIVERSITARIA
COLOMBO AMERICANA

Políticas de Seguridad de la información – Manual

Bogotá D.C., Colombia - 2022

Manual de Políticas de Seguridad de la información ÚNICA

TABLA DE CONTENIDO

Alcance

Las políticas de seguridad de la información contenidas en este manual tienen como propósito garantizar la confidencialidad, integridad y disponibilidad de los activos de información gestionados por todos los procesos: estratégicos, misionales, y de apoyo de la Institución Universitaria Colombo Americana - ÚNICA, razón por la cual son de obligatorio cumplimiento por parte del personal administrativo, docentes, contratistas y, en general, las partes interesadas que generen, accedan o utilicen información de la Institución.

Objetivo general

Establecer las políticas que regulan la seguridad de la información en ÚNICA y presentar en forma clara y coherente los elementos que deben conocer, acatar y cumplir el personal administrativo, docentes, contratistas y en general las partes interesadas en la Institución.

Lineamientos

Las políticas contenidas en este manual se encuentran organizadas de acuerdo con los objetivos de control presentados en el Anexo A de la norma ISO27001.

Este Manual de Políticas de Seguridad de la información deberá ser revisado al menos una vez al año, durante las reuniones periódicas del Comité de Alta Gerencia, donde serán aprobadas por la dirección, publicadas y comunicadas al personal administrativo, docentes, contratistas y en general partes interesadas en ÚNICA.

El Comité de Alta gerencia está integrado por Rectoría, Vicerrectoría Académica, Dirección Financiera y Administrativa, Dirección de Comunicaciones, Dirección Jurídica y de Aseguramiento de la Calidad, Dirección de Comunicaciones y mercadeo, y Coordinación de Transformación digital.

Objetivo de control A5 - Políticas de la seguridad de la información.

Directrices:

a) ÚNICA, cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) y Protección de Datos Personales que le permite minimizar los impactos en la Institución por la materialización de riesgos de seguridad de la información y ciberseguridad, así como mantener un nivel aceptable de exposición al riesgo, garantizar la confidencialidad integridad y disponibilidad a lo largo del ciclo de vida de la información, crear un ambiente de cultura y conciencia de seguridad de la información, y mantener un proceso de mejora continua de protección de la información. El Sistema de Gestión de Seguridad de la información y Protección de Datos Personales de ÚNICA, incluye:

- Políticas y procedimientos en materia de seguridad de la información.
- Objetivos de control y controles aplicables.
- Gestión de los riesgos basados en una metodología de análisis, evaluación y tratamiento.
- Cultura de seguridad de la información en el personal administrativo, docentes, contratistas y en general partes interesadas en ÚNICA.
- Reporte y gestión de eventos e incidentes de seguridad.
- Gestión de la mejora continua del SGSI.

b) Por estas razones el Comité de Alta Gerencia se compromete a suministrar los recursos necesarios, como tiempo, equipo humano competente, y recursos económicos para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) y Protección de Datos Personales de ÚNICA.
c) El incumplimiento de las políticas aquí relacionadas traerá consigo las consecuencias legales, administrativas y disciplinarias, relacionadas con seguridad de la información y protección de datos personales, de acuerdo con lo establecido en el proceso disciplinario de ÚNICA.

Objetivo de control A6 - Organización de la seguridad de la información

Organización interna

Directrices:

a) ÚNICA contará con una estructura para controlar el desarrollo, la implementación y operación del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales, promoviendo iniciativas de seguridad de la información que sean pertinentes a la estructura, tamaño, objeto social y actividades de la Institución y contando con unas responsabilidades claramente asignadas y comunicadas a todos los niveles de la empresa. Para lo anterior ÚNICA contará con:

- Comité de Alta Gerencia: el cual tratará en su agenda los asuntos relacionados con el Sistema de Gestión de Seguridad de la información (SGSI) y Protección de Datos Personales, como son las estrategias para garantizar que el SGSI cumpla los lineamientos y los objetivos establecidos. Este comité está conformado por:
  - Rectora ÚNICA
  - Vicerrectoría Académica
  - Dirección Jurídica y de Aseguramiento de la Calidad
  - Dirección Financiera
  - Coordinación de Transformación digital
  - Dirección de Comunicaciones-

- **Responsable de Seguridad de la Información:** Será el **Coordinador de Transformación digital** quien tendrá la responsabilidad de administrar, promover, orientar, mantener, evaluar y tratar proactivamente el Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales.

b) Se deben mantener y documentar los contactos con autoridades (Policía, Bomberos, etc.), con el fin de contactar en caso de que se presente un incidente de seguridad de la información y que se requiera de asesoría externa.
c) Se debe mantener contacto con grupos de interés especializados en seguridad y privacidad de la información, con el fin de compartir e intercambiar conocimientos que permitan la mejora continua del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales.
d) Los proyectos que se desarrollen en ÚNICA deben contemplar una gestión de los riesgos de seguridad de la información asociados a éstos, lo cual incluye una identificación de los riesgos y la definición de la forma como serán tratados.
e) En cualquier caso, los proyectos desarrollados por ÚNICA deben estar alineados con las políticas de seguridad contenidas en el presente manual.

Política para dispositivos móviles

Directrices:

Las políticas de seguridad de la información para dispositivos móviles se establecen según el tipo del dispositivo, como sigue:

Teléfonos inteligentes personales que se usen en procesos institucionales:

a) El uso de teléfonos inteligentes está autorizado para todo el personal administrativo de ÚNICA, siempre y cuando se declare por parte del propietario en documento firmado que dicho dispositivo cuenta con antivirus instalado y se hace responsable de:
   - Instalar aplicaciones únicamente desde los repositorios oficiales.
   - Dar un manejo confidencial a la información almacenada o accedida desde dichos dispositivos.
   - Hacer un uso adecuado del internet según las políticas de navegación definidas en este manual.

Teléfonos inteligentes institucionales:

a) El personal administrativo que cuente con asignación de dispositivos móviles de ÚNICA es responsable de:
   - Gestionar información exclusivamente de ÚNICA en estos dispositivos.

- No se deberá gestionar información personal en los teléfonos institucionales.
- Cuidar de la seguridad física del teléfono celular.
- Proteger el dispositivo mediante contraseña de acceso.
- Instalar aplicaciones únicamente desde los repositorios oficiales.
- Dar un manejo confidencial a la información almacenada o accedida desde dichos dispositivos.
- Hacer un uso adecuado del internet según las políticas de navegación definidas en este manual.
- Ante la pérdida del celular, deberá realizar la respectiva denuncia ante la entidad competente y reportar inmediatamente el incidente, con el fin de que se cambien los accesos a las plataformas utilizadas.

Computadores y portátiles:

a) ÚNICA debe asignar equipos institucionales al personal administrativo. Dichos equipos contarán con sistema operativo y software antivirus licenciados, así mismo, los privilegios de administración sobre el equipo estarán restringidos mediante la configuración de un usuario administrador local.
b) En caso de requerirse el uso de equipos personales por parte del personal administrativo, deberá solicitarse la autorización por el jefe inmediato mediante el formato de control (este formulario deberá implementarlo el responsable de Seguridad de la Información). En cuyo caso el personal administrativo deberá declarar en documento firmado que dicho equipo cuenta con sistema operativo licenciado y se hace responsable de:
    - Instalar aplicaciones únicamente desde los repositorios oficiales.
    - Ejecutar su labor desde los recursos en la nube autorizados, como: Office 365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom, eltiempo.com.
    - Dar un manejo confidencial a la información almacenada o accedida desde dicho equipo.
    - Hacer un uso adecuado del internet según las políticas de navegación definidas en este manual.
    - Ante la pérdida del equipo portátil, deberá realizar la respectiva denuncia ante la entidad competente y reportar inmediatamente el incidente, con el fin de que se cambien los accesos a las plataformas utilizadas.

c) ÚNICA instalará el software de antivirus Institucional en los equipos personales autorizados.
d) ÚNICA verificará que los equipos autorizados cumplan las políticas establecidas y gestionará un inventario de éstos.
e) Cuando la labor contractual termine, el personal administrativo deberá declarar en documento firmado que se llevó a cabo el borrado de toda la información de ÚNICA que pudo haberse almacenado en el equipo personal.

Política de teletrabajo

Directrices:

a) El trabajo remoto está permitido en ÚNICA para su personal administrativo.
b) ÚNICA deberá garantizar la doble autenticación en los accesos remotos a los sistemas de información, aplicativos y servicios tecnológicos de la Institución.
c) El personal administrativo solo puede acceder a los sistemas de información, aplicativos y servicios que le han sido aprobados en teletrabajo, y en el horario laboral acordado por ÚNICA.
d) Toda información gestionada y que sea accedida remotamente por el personal administrativo debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.
e) Solo se podrá hacer uso de los repositorios dispuestos por ÚNICA. No está permitido el almacenamiento de información en el equipo personal.
f) Está prohibido instalar programas o software en los equipos suministrados por ÚNICA. El proceso de Gestión Tecnológica es el único autorizado para instalar o configurar software y equipos bajo licenciamiento.
g) El personal administrativo es responsable por el equipo de cómputo asignado y por los daños ocasionados por su mal uso.
h) Es responsabilidad del personal administrativo salvaguardar la información contenida en los diferentes recursos de información a los cuales accede, evitando compartir el acceso a dichos recursos con personas ajenas a ÚNICA
i) Está prohibido que el personal administrativo haga uso del equipo de cómputo asignado en sitios públicos o diferentes a los autorizados por ÚNICA.
j) El responsable de seguridad de la información verificará periódicamente el cumplimiento de las condiciones técnicas y de seguridad aquí establecidas, para los teletrabajadores que se encuentren activos.

Objetivo de control A7 - Seguridad de los recursos humanos

Seguridad de los recursos humanos

Directrices:

Antes de asumir el empleo

a) El responsable del proceso de Gestión del Talento Humano deberá incluir en el proceso de selección y contratación del personal administrativo, la verificación de antecedentes ante las siguientes entidades: Registraduría Nacional Del Estado Civil, Policía Nacional De Colombia, Policía Judicial, Fiscalía General De La Nación, Contraloría General De La República, Procuradora General De La Nación. Lo anterior con el fin de confirmar la

veracidad de la información suministrada y de esta forma validar la idoneidad y confiabilidad del recurso humano antes de su vinculación.

b) El proceso de Gestión del Talento Humano, deberá establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
c) Todo personal administrativo, debe firmar cláusulas en las que se establezca un acuerdo de confidencialidad y no divulgación de la información reservada de ÚNICA, lo cual deberá reposar en el expediente contractual del personal administrativo.
d) El proceso de Gestión del Talento Humano garantizará que, al momento de la vinculación, todo personal administrativo acepte el cumplimiento del Manual de Políticas de Seguridad de la Información, así mismo deberá firmar la autorización para el tratamiento de los datos personales según lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.

Durante la ejecución del empleo

e) El proceso de Gestión del Talento Humano deberá garantizar la capacitación y sensibilización sobre las políticas de seguridad de la información a todo el personal administrativo durante el proceso de inducción y reinducción.
f) El responsable de seguridad de la información debe evaluar que el personal administrativo haya entendido las políticas de seguridad de la información socializadas en el proceso de inducción y reinducción.
g) El personal administrativo deberá declarar en un documento firmado que leyó, entendió y se compromete a aplicar las políticas de seguridad de la información de ÚNICA.
h) Es responsabilidad del personal administrativo informar al responsable de seguridad de la información acerca de los incidentes de seguridad de la información que observe.
i) En el caso de presentarse una violación a la seguridad de la información por parte del personal administrativo o académico, el responsable establecido en el Reglamento de trabajo y reglamento docente deberá liderar la aplicación del proceso disciplinario según corresponda. Dicho proceso debe ser de conocimiento del personal administrativo de ÚNICA.
j) En caso de ausencias temporales del personal administrativo, debido a vacaciones o licencias, el proceso de Gestión del Talento Humano deberá notificar al responsable de tecnología para que sean desactivados los accesos físicos, tecnológicos y de sistemas de información a los cuales tenga acceso el funcionario en cuestión.
k) En el caso de que un empleado cambie de funciones, se debe informar al responsable de tecnología para que los accesos físicos, tecnológicos y de sistemas de información a los cuales tenga acceso sean actualizados de acuerdo con las nuevas funciones del personal administrativo Es responsabilidad del Jefe inmediato solicitar los accesos requeridos para el desarrollo de las nuevas funciones.

Terminación y cambio del empleo

l) El responsable de Talento Humano deberá informar inmediatamente al responsable de tecnología sobre la desvinculación del personal administrativo de ÚNICA para que sean retirados los accesos físicos, tecnológicos y de sistemas de información a los cuales tenga acceso el personal administrativo.
m) Es de responsabilidad del personal administrativo realizar la entrega de la información propia de ÚNICA a la que tenga acceso y certificar la eliminación de ésta de los dispositivos personales.
n) Se debe solicitar la devolución de los elementos asignados como carné, equipo de cómputo, celular, etc.

Toma de conciencia, educación y formación en seguridad de la información

Directrices:

a) El responsable de Talento Humano destinará los recursos suficientes y, a través del responsable de seguridad de la información, incluirá en el plan de capacitación de la Institución campañas de concienciación o sensibilización sobre políticas y procedimientos para lograr el entendimiento y toma de conciencia en seguridad de la información, y de esta manera, disminuir vulnerabilidades y amenazas relacionadas con el recurso humano.
b) El personal administrativo de ÚNICA demostrará su compromiso con el Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales por medio de la asistencia obligatoria a las campañas de concienciación o sensibilización cuando estas tengan lugar.
c) El responsable de seguridad de la información realizará la revisión de los resultados de las evaluaciones de las capacitaciones en seguridad de la información, para identificar oportunidades de mejora.
d) El proceso de Gestión del Talento Humano destinará los recursos suficientes y, a través del responsable de seguridad de la información, se asegurará de que se realizan procesos de sensibilización y concienciación a contratistas y terceros que presten sus servicios o tengan algún tipo de relación con ÚNICA según las necesidades identificadas en la evaluación de riesgos.
e) La sensibilización en seguridad de la información y protección de datos personales se debe realizar mínimo cada 3 meses.

Objetivo de control A8 - Gestión de activos

Identificación, clasificación y etiquetado de activos de información

Directrices:

a) ÚNICA, como propietario de los activos de información, mantendrá un inventario actualizado de activos de información y será responsabilidad de cada líder de proceso los activos de información a su cargo.
b) Los activos de información serán identificados y clasificados teniendo en cuenta los impactos que le pueden causar a ÚNICA por la pérdida de confidencialidad, integridad y disponibilidad. Así mismo serán clasificados de acuerdo con la ley 1581.
c) La información estará clasificada en: Uso Público, Uso Interno de ÚNICA, Uso Exclusivo del Proceso y Confidencial, la cual debe ser etiquetada por los responsables de la misma según lo establecido en el documento "Metodología de Identificación de Activos y Riesgos 08-02-2022".
d) Se debe revisar el inventario de activos y la matriz de análisis de riesgos de seguridad de la información al menos una vez al año.
e) ÚNICA proveerá los recursos necesarios para la aplicación de controles orientados a preservar la confidencialidad, la integridad y la disponibilidad de la información, de tal manera que permitan su correcto uso por parte del personal administrativo, docentes, contratistas y, en general, partes interesadas en ÚNICA que se encuentren autorizados y requieran de ella para la ejecución de sus actividades.
f) Todo líder de proceso será responsable de realizar la valoración de activos, y contenedores de información siguiendo la metodología junto con el responsable de seguridad de la información.
g) Todo personal administrativo deberá prevenir los riesgos a los que está expuesta la información, evitando la copia, divulgación, destrucción física o digital de la información sin previa autorización.
h) Todo personal administrativo deberá realizar la entrega formal de todos los activos de información físicos y electrónicos en el proceso de desvinculación.
i) Todo personal administrativo deberá evitar la duplicación de información con Datos personales y tratará en lo posible de consolidarla en el SharePoint Institucional.
j) El responsable de seguridad de información coordinará la revisión anual del inventario de activos de información para validar su clasificación y etiquetado.
k) En caso de requerirse la eliminación de activos de información, los responsables de los activos realizarán una disposición segura del activo de información de acuerdo con cada caso, dejando registro de evidencia y realizando la notificación al responsable de seguridad de la información.

Uso aceptable de activos

Directrices:

Todo el personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA tendrán a su disposición el uso de activos de información y recursos tecnológicos que los contienen, según las funciones laborales que así lo requieran. Para su uso, todo el personal acepta

y se acoge a las Políticas Seguridad de la información y las disposiciones relacionadas a continuación:

a) Toda cuenta de usuario es de uso personal e intransferible. El usuario será responsable de todas las acciones o transacciones efectuadas con su cuenta de usuario.
b) Los recursos se deben usar estrictamente para fines laborales. El personal administrativo no podrá hacer uso de estos recursos para transmitir, almacenar y/o procesar información que atente contra la propiedad intelectual, los derechos de autor o derechos de protección de datos personales.
c) El personal administrativo no debe realizar actividades que puedan degradar el desempeño de los recursos tecnológicos y, por ende, generar posibles pérdidas o daños en la información.
d) Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para el personal administrativo, docentes, contratistas y en general las partes interesadas en ÚNICA.
e) No está permitido el uso de cuentas personales para el almacenamiento o intercambio de información Institucional de ÚNICA.
f) Se debe proteger la información confidencial transmitida por correo electrónico mediante archivos Zip con contraseña, y la contraseña se debe comunicar por un canal de comunicación diferente.
g) Está prohibido acceder a páginas con contenido pornográfico y demás condiciones que degraden la condición humana y resulten ofensivas para el personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA. Así mismo, está prohibido acceder a juegos en línea, uso de redes sociales con fines diferentes a los laborales y queda prohibido el uso repositorios personales como Dropbox, Google Drive, OneDrive, WeTransfer para almacenar información institucional a menos que sea autorizado por el jefe directo.
h) Toda la información procesada y almacenada en los recursos de ÚNICA está asociada a la labor que desempeña el personal administrativo en desarrollo de sus funciones y cargos, por lo cual esta información es de carácter institucional. En este sentido, el personal administrativo debe abstenerse de almacenar y procesar información de carácter personal en los recursos provistos por ÚNICA.
i) Los usuarios no podrán copiar o distribuir software, cambiar las configuraciones de los recursos tecnológicos y deberán utilizar únicamente los programas y equipos autorizados por el responsable del proceso de Gestión Tecnológica, quienes son los autorizados para instalar o configurar software y equipos bajo licenciamiento.
j) La descarga, instalación o uso de software ilegal o sin licenciar será considerada como una violación a las políticas de seguridad de la información de ÚNICA.

Política de Gestión de Medios Removibles

Directrices:

a) Los medios removibles y las conexiones a dichos medios en los equipos de cómputo como memorias USB, unidades de CD/DVD y discos externos, entre otros, serán restringidos por parte del proceso de Gestión Tecnológica y en todos los equipos de la Institución, excepto para aquellos cargos que en desarrollo de sus funciones, requieran hacer uso de medios removibles, para lo cual deberán contar con la evaluación y aprobación del jefe directo y del responsable de la seguridad de la información, quienes realizarán la evaluación de riesgos a los que está expuesta la información.
b) El responsable del proceso de Gestión Tecnológica administrará una lista de aprobación (lista blanca) con los medios removibles autorizados y los respectivos responsables. Esta lista servirá como soporte en caso de presentarse incidentes, investigaciones o auditorías, entre otros, relacionados con la seguridad de la información.

Objetivo de control A9 - Control de acceso

Política de control de acceso

Directrices:

a) El responsable de Talento Humano debe suministrar y garantizar a los usuarios el cambio de contraseña para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol.
b) Las credenciales de acceso son de uso personal e intransferible.
c) Las conexiones remotas a los recursos de red deben establecerse mediante conexión VPN, la cual debe ser aprobada, registrada y monitoreada por el proceso de Gestión Tecnológica de ÚNICA.
d) El proceso de Gestión Tecnológica debe asegurar que las redes inalámbricas de la Institución cuenten con métodos de autenticación que eviten accesos no autorizados.
e) El proceso de Gestión Tecnológica debe realizar el cambio de contraseña de la red inalámbrica de la Institución periódicamente mínimo (3) veces al año.
f) El proceso de Gestión Tecnológica debe revisar que los equipos personales del personal administrativo, contratistas, proveedores o partes interesadas que se conecten a la red de datos de ÚNICA cuenten con sistema operativo licenciado y antivirus y únicamente podrán realizar las tareas para las que fueron autorizados.

Gestión de acceso de usuarios

Directrices:

a) El proceso de Gestión del Talento Humano debe definir un procedimiento que contemple la creación, actualización, activación e inactivación de cuentas de usuario.
b) El proceso de Gestión del Talento Humano suministrará los usuarios y contraseñas temporales, una vez el usuario ingrese deberá hacer cambio de la contraseña.
c) El proceso de Gestión del Talento Humano sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato.
d) Los usuarios creados no tienen permisos de administrador. Sólo se otorgan los privilegios de administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.
e) El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del personal administrativo, docentes, contratistas y en general las partes interesadas en ÚNICA.
f) El proceso de Gestión Tecnológica debe garantizar que los usuarios realicen el cambio de contraseña de acceso a los servicios tecnológicos cada vez que sea requerido.
g) El proceso de Gestión Tecnológica debe mantener un listado actualizado de las cuentas de administración de los recursos tecnológicos.
h) La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.

Responsabilidades de los usuarios

Directrices:

a) El responsable del proceso de Gestión Tecnológica debe garantizar que, en el ingreso a los servicios tecnológicos de la Institución, las contraseñas no sean visibles en texto claro.
b) La complejidad de la contraseña debe ser mínimo de 10 caracteres, y debe combinar mayúsculas, minúsculas, números y caracteres especiales.
c) Las contraseñas no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni que tengan que ver con la vida personal.
d) No se deberán repetir las últimas 3 contraseñas utilizadas en cada sistema o servicio tecnológico.
e) Las contraseñas deben cambiarse obligatoriamente cada 60 días, de lo contrario, la contraseña caducará y obligará a su cambio. Si el sistema no pide cambio de manera automática, el usuario deberá hacer dicho cambio voluntariamente.
f) Después de tres (3) intentos fallidos de ingreso de la contraseña el usuario se bloquea de manera inmediata y deberá esperar un tiempo de cinco (5) minutos para volver a intentar, o solicitar el desbloqueo al proceso de Gestión Tecnológica.
g) Debe cambiarse la contraseña si se ha detectado anomalía en la cuenta de usuario.
h) Las contraseñas no deben ser visibles en la pantalla al momento de ser ingresadas.

i) Las contraseñas no se deben registrar en papel, correo electrónico y/o archivos digitales a menos que se puedan almacenar de forma segura. El método de almacenamiento debe estar aprobado por el responsable de seguridad de la información.
j) Los administradores de los servicios tecnológicos deben cumplir con los lineamientos de contraseñas seguras indicados.
k) Los administradores de los servicios tecnológicos o sistemas de información deben custodiar de manera adecuada las credenciales de acceso.
l) El responsable del proceso de Gestión Tecnológica instalará una herramienta para el almacenamiento adecuado de credenciales de acceso de forma segura. Ej. KeePass.

Control de acceso a sistemas y aplicaciones

Directrices:

a) Los Directores administrativos deben aprobar la creación, modificación o desactivación de cuentas de usuario, roles y perfiles en sistemas de información, aplicativos y servicios, acogiéndose al procedimiento establecido para este fin.
b) El responsable del proceso de Gestión Tecnológica debe velar por que los servicios tecnológicos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles y perfiles para cada sistema de información.
c) Mientras el sistema o servicio tecnológico lo soporte, se deberá implementar autenticación por múltiple factor.
d) El administrador del sistema debe revisar los usuarios activos en el sistema de acuerdo con la matriz de roles y perfiles definida.
e) El proceso de Gestión Tecnológica debe asegurar que no se desplieguen en pantalla las contraseñas ingresadas en los sistemas.
f) Los repositorios autorizados para el almacenamiento de información en ÚNICA son: Office 365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom, elempleo.com.

Objetivo de control A10 - Criptografía

Política sobre el uso de Controles Criptográficos

Directrices:

a) Es deber de todo personal administrativo y docente, contratistas y, en general, las partes interesadas en ÚNICA, cifrar los activos de información clasificados como confidenciales o sensibles que sean transmitidos mediante canales de comunicación públicos. Esto se

puede lograr mediante el uso de archivos Zip con contraseña y la contraseña se debe comunicar por un canal de comunicación diferente.

b) Se deben generar claves criptográficas sólidas (TDES, AES-256) con una longitud de 256 bits como mínimo y garantizar que su distribución es independiente a la distribución de la información cifrada.
c) Se deben definir mecanismos seguros para el almacenamiento de las claves y realizar cambios periódicos de las claves.
d) Al realizar el cifrado de información, se debe mantener copia de las claves de cifrado en un lugar seguro de forma que la recuperación de la información cifrada sea factible en caso de ausencia temporal o permanente del custodio de ésta.
e) Las claves criptográficas de las que se tenga sospecha de exposición deben ser destruidas.
f) Se debe definir un tiempo de vida de las claves.
g) Se deben sustituir las llaves criptográficas tras su caducidad o compromiso.
h) Está expresamente prohibido revelar las claves privadas de cifrado de información a personal no autorizado.
i) Si se requiere el uso de controles criptográficos, se deben utilizar algoritmos robustos como: AES-256 (simétrico), RSA (asimétrico), SHA2 (funciones hash).
j) Está expresamente prohibido cifrar información con mecanismos no autorizados por ÚNICA.

Objetivo de control A11 - Seguridad física y del entorno

Áreas seguras

Directrices:

a) El acceso físico a las instalaciones ÚNICA se debe controlar mediante el diligenciamiento de una planilla de acceso, o contemplar la implementación de cámaras de seguridad que registre el ingreso de personal.
b) Se debe registrar el ingreso y retiro de dispositivos personales como computadores, cámaras y discos externos. Para el retiro de equipos Institucionales se debe contar con la autorización del jefe directo.
c) Las puertas y ventanas de las áreas deben permanecer cerradas y bloqueadas cuando no haya supervisión o cuando las áreas se encuentren sin la presencia de personal administrativo.
d) Los visitantes deben estar autorizados por el área responsable de la visita y deben estar acompañados en todo momento por personal administrativo de ÚNICA.
e) Siempre permanecerá una persona en las oficinas. De lo contrario, las oficinas quedarán con llave.
f) El responsable del proceso de Gestión SST debe suministrar extintores, la camilla y el botiquín de emergencia.

g) El proceso de Gestión SST debe establecer los planes de emergencia contra amenazas externas y ambientales.
h) Cabe resaltar que ÚNICA mantiene sus servicios tecnológicos en la nube por lo que no cuenta con centro de cómputo en sus instalaciones.

Equipos

Directrices:

a) El proceso de Gestión Tecnológica velará por que los equipos de cómputo, escáneres e impresoras estén situados en áreas protegidas para reducir el riesgo contra amenazas ambientales y acceso no autorizado.
b) El proceso de Gestión Tecnológica debe propender para que los equipos de cómputo portátiles se protejan mediante guayas para prevenir su pérdida.
c) El proceso de Gestión Tecnológica debe definir mecanismos de soporte y mantenimiento para los equipos de cómputo y equipos de red y debe llevar registro de éstos.
d) Cuando un equipo sea reasignado o retirado de servicio, el proceso de Gestión Tecnológica debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad.
e) El personal administrativo que tenga asignado un equipo portátil propiedad de ÚNICA debe asegurarlo con guaya. El equipo deberá ser entregado al proceso de Gestión Tecnológica una vez termine su vínculo contractual con la Institución.
f) El proceso de Gestión Tecnológica debe configurar como política general que todos los equipos de cómputo que se encuentren desatendidos se bloqueen automáticamente después de cinco (5) minutos de inactividad. De todas formas, si el control no aplica, el personal administrativo debe bloquear su pantalla cuando se levante de su puesto de trabajo o se retire de las oficinas de ÚNICA.

Política de escritorio y pantalla limpios

Directrices:

a) Todo el personal administrativo de ÚNICA deberá mantener protegida la información confidencial o sensible, objeto de su labor o propia de la Institución, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
b) El puesto de trabajo del personal administrativo deberá permanecer organizado y la información clasificada como confidencial o sensible, deberá guardarse bajo llave, mientras el personal administrativo responsable de ésta no esté trabajando con ella.

c) Los equipos de cómputo con información de ÚNICA, deberán conservar la pantalla libre de accesos directos a información clasificada como confidencial o sensible.
d) Los documentos que contengan información clasificada como confidencial o sensible, se deben retirar inmediatamente de las impresoras, fax, fotocopiadoras y escáneres.
e) Para evitar riesgo de pérdida o deterioro de la información que reposa en los puestos de trabajo, el personal administrativo deberá abstenerse de consumir alimentos o bebidas en dichos lugares.
f) Se debe tener control de la información en físico que se presta a otras áreas o que sale de las instalaciones de ÚNICA.
g) No se deben reutilizar o reciclar documentos impresos clasificados como confidenciales o sensibles. Estos deben ser destruidos de forma segura.

Objetivo de control A12 - Seguridad de las operaciones

Procedimientos operacionales y responsabilidades

Directrices:

a) El responsable del proceso de Gestión Tecnológica debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
b) El proceso de Gestión Tecnológica debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de sistemas de información, aplicativos y servicios tecnológicos, en el que se contemplen los impactos, se definan claramente los responsables de los cambios y se establezcan las actividades de Rollback (Deshacer cambio).
c) El responsable proceso de Gestión Tecnológica y el responsable de seguridad de la información deben evaluar, aprobar o negar la implementación de los cambios requeridos, teniendo en cuenta los posibles riesgos que se puedan presentar.
d) El responsable de los sistemas de información y de los servicios tecnológicos deben gestionar la capacidad, llevar a cabo proyecciones de crecimiento y alertar cuando dichas capacidades estén llegando a los límites establecidos.

Protección contra códigos maliciosos

Directrices:

a) ÚNICA contará con un antivirus Institucional que debe instalarse en todos los equipos institucionales y en aquellos equipos de uso personal autorizados en la Institución.

b) El proceso de Gestión Tecnológica debe garantizar que el software antivirus se mantenga actualizado con las últimas firmas y deberá monitorear las alertas generadas por dicho software en donde se encuentre instalado.
c) El proceso de Gestión Tecnológica debe definir los pasos para la detección, prevención y recuperación contra códigos maliciosos.
d) El responsable de seguridad de la información deberá generar cultura entre el personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA para prevenir ataques de software malicioso.
e) Se debe garantizar que la información sea escaneada por el software de antivirus. Así mismo, se debe escanear la información contenida y transmitida mediante correo electrónico.
f) El proceso de Gestión Tecnológica debe asegurar que no se pueda detener el software antivirus instalado en los equipos institucionales y en aquellos equipos de uso personal autorizados en la Institución.
g) El personal administrativo debe abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente, los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.
h) El personal administrativo, docentes, contratistas y, en general, partes interesadas en ÚNICA que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato al responsable de seguridad de la información con el fin de tomar las medidas correspondientes.

Copias de respaldo

Directrices:

a) El personal administrativo de ÚNICA ejecuta su labor desde los recursos en la nube autorizados, como Office 365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom, eltiempo.com. Dichos recursos garantizan alta disponibilidad de la información allí almacenada. Además, el personal administrativo no debe almacenar información en los equipos de cómputo, a menos que se garantice que una copia de la información está quedando almacenada en el OneDrive Institucional.
b) deben definir y documentar un procedimiento de copias de respaldo y restauración de la información más crítica almacenada de los recursos en la nube, donde se establezca el esquema de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.
c) Se deben llevar a cabo *backups* o copias de respaldo de la configuración e información crítica almacenada en sistemas de información y aplicaciones, las cuales deberán almacenarse en el OneDrive Institucional.
d) En caso de ser necesario, se deberá disponer de discos duros externos institucionales para llevar a cabo copias de respaldo de los equipos del personal administrativo. Los discos se deben mantener siempre en las instalaciones de ÚNICA.

e) El proceso de Gestión Tecnológica debe llevar a cabo pruebas de restauración de las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
f) Los líderes de procesos deben guardar la información en los recursos en la nube autorizados, como Office 365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom, eltiempo.com. La información que no se aloje en dichos recursos no será respaldada y cualquier pérdida de esta será responsabilidad del usuario.

Registro de eventos y seguimiento

Directrices:

a) El responsable del sistema o servicio tecnológico deberá parametrizar los registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas administrados.
b) El responsable del sistema o servicio tecnológico debe salvaguardar los registros de auditoría que se generen en los sistemas administrados
c) El responsable del sistema o servicio tecnológico deberá monitorear excepciones a los eventos de la seguridad de información.
d) El responsable del sistema o servicio tecnológico debe garantizar que los sistemas de información y servicios tecnológicos tengan configurada la misma zona horaria para facilitar futuras investigaciones.
e) También se deberán monitorear los registros de eventos realizados por los responsables de los sistemas o servicios tecnológicos.

Control de software operacional

Directrices:

a) El proceso de Gestión Tecnológica controlará la instalación de software no autorizado mediante la configuración de un usuario administrador local en los equipos Institucionales.
b) El proceso de Gestión Tecnológica configurará los equipos institucionales para que instalen actualizaciones de seguridad en los sistemas operativos automáticamente.
c) El proceso de Gestión Tecnológica definirá el listado de aplicaciones permitidas para estar instaladas en los equipos Institucionales.
d) El proceso de Gestión Tecnológica debe realizar de manera periódica una inspección del software instalado en los equipos Institucionales y debe desinstalar el software no autorizado.

Gestión De Vulnerabilidades Técnicas

Directrices:

a) El proceso de Gestión Tecnológica debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas y pruebas de penetración en los sistemas de información y servicios tecnológicos críticos.
b) El proceso de Gestión Tecnológica debe documentar, informar, gestionar y corregir las vulnerabilidades encontradas.

Objetivo de control A13 - Seguridad en las comunicaciones

Gestión de seguridad de las redes

Directrices:

a) El responsable de Gestión Tecnológica debe generar registros de navegación de los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de internet.
b) El responsable de Gestión Tecnológica debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos.
c) El responsable de Gestión Tecnológica debe proteger la red mediante el uso de dispositivos perimetrales, como firewalls.
d) El responsable de Gestión Tecnológica debe proteger el acceso a la red inalámbrica mediante el uso de protocolos fuertes de autenticación, como WPA2, así mismo, deberá cambiar la contraseña de acceso a la red inalámbrica periódicamente mínimo (3) veces al año.

Transferencia de información

Directrices:

a) Se garantizará la protección de la información confidencial y sensible de ÚNICA que sea transmitida o recibida entre personal administrativo, docentes, contratistas y en general partes interesadas, asegurando la conservación de las propiedades de confidencialidad, integridad y disponibilidad.
b) Se deberán implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de ÚNICA, contra interceptación, copiado, modificación y destrucción.
c) Cualquier intercambio de información con patrocinadores, aliados, convenios, contratistas, proveedores y partes interesadas debe quedar formalizado en un acuerdo de intercambio de información o cláusula del contrato determinando las condiciones y controles de seguridad que aseguren dicho intercambio de información. Dichas

condiciones y controles, deben ser validadas por el responsable de seguridad de información.

d) En caso de que una autoridad, ente regulador, de control, de vigilancia o judicial requiera la entrega de información, esta se llevará a cabo con la autorización del Comité de Alta Gerencia.
e) La información confidencial transmitida por correo electrónico deberá protegerse mediante archivos Zip con contraseña y la contraseña se debe comunicar por un canal de comunicación diferente.
f) Los mensajes de correo electrónico deben ir acompañados del siguiente *disclaimer* o descargo de responsabilidad: "Este mensaje y sus adjuntos se dirigen exclusivamente a su(s) destinatario(s), puede contener información confidencial o sensible que es para el uso exclusivo de la persona o entidad de destino. Si Ud., no es el destinatario indicado, queda notificado de que la lectura, utilización, divulgación y/o copia sin autorización expresa de ÚNICA está prohibida en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique inmediatamente por esta misma vía o al correo dir.comunicaciones@unica.edu.co y que proceda a su eliminación inmediata".

Acuerdos de confidencialidad o de no divulgación

Directrices:

a) Es obligación de todo el personal administrativo, docentes, contratistas y, en general, las partes interesadas que suscriben un contrato con ÚNICA, firmar el acuerdo de confidencialidad o no divulgación y es su deber entender, aceptar y generar un compromiso con el cumplimiento de las disposiciones contenidas en dicho acuerdo.
b) Todo personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA no debe participar en acciones (comentarios, publicaciones o imágenes en chat, redes sociales, sitios web, correos electrónicos, mensajería instantánea, medios de comunicación u otros) que dañen, difamen o afecten la reserva de la información o la imagen de la Institución.
c) La responsabilidad y la confidencialidad sobre datos personales a las que tenga acceso todo personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA deben quedar explicitas y aceptadas en un documento de acuerdo de confidencialidad o cláusula del contrato al momento de iniciar alguna relación contractual.

Objetivo de control A14 - Adquisición, desarrollo y mantenimiento de sistemas

Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de información

Directrices:

a) Todos los sistemas de información y/o aplicaciones que se adquieran o desarrollen deben tener una definición clara de los requerimientos funcionales, operacionales, especificaciones técnicas y criterios de aceptación, contemplando requerimientos de seguridad de la información. Este proceso deberá ser apoyado por el responsable de seguridad de la información y por el área usuaria que requiera la solución.
b) El responsable de Gestión Tecnológica debe asegurar que no se usen datos personales y sensibles en ambientes de prueba.
c) El responsable de Gestión Tecnológica debe asegurar que se asignen en los ambientes de producción los privilegios mínimos requeridos para el desarrollo de las actividades por parte del personal administrativo.
d) El responsable de Gestión Tecnológica debe asegurar que la autenticación de los usuarios en todas las aplicaciones se realice mediante múltiple factor de autenticación.
e) El responsable de Gestión Tecnológica debe controlar la asignación de permisos en los sistemas y aplicaciones según lo definido en el rol y/o perfil del usuario que ha sido solicitado y aprobado.
f) El responsable de Gestión Tecnológica debe establecer los controles para la validación de los datos de entrada, para su procesamiento, para su almacenamiento y para las salidas de los datos, todo de acuerdo con los requerimientos funcionales y los requerimientos para su administración.
g) El responsable de Gestión Tecnológica debe establecer en lo posible ambientes de desarrollo, prueba y producción por separado.
h) El responsable de Gestión Tecnológica debe garantizar que se ejecuten pruebas de vulnerabilidad técnica y de seguridad de la información para todo sistema o aplicación nuevo, antes de su entrada a producción.
i) El responsable de Gestión Tecnológica debe realizar mantenimiento periódico y planificado a los sistemas de información, para garantizar su correcto funcionamiento (depuración de usuarios, bases de datos, configuraciones, parámetros, entre otros y demás que puedan resultar en un incidente).
j) El responsable de Gestión Tecnológica debe controlar que los cambios en sistemas o aplicaciones tengan en cuenta la evaluación de los riesgos, se soporten en una definición de especificaciones, en pruebas de control de calidad y una adecuada gestión de su implementación que asegure la integridad del sistema.
k) El responsable de Gestión Tecnológica debe asegurar que todos los sistemas de información generen logs para seguimiento a las acciones y/o cambios ejecutados por los usuarios y administradores del sistema.
l) El responsable de Gestión Tecnológica debe asegurar que se gestionen adecuadamente los derechos de autor, la propiedad intelectual, y la confidencialidad del sistema.
m) El responsable de Gestión Tecnológica debe establecer lineamientos para la supervisión y seguimiento a las actividades de desarrollo seguro contratado, incluido la garantía de uso de técnicas de programación seguras y la implementación de condiciones de seguridad del ambiente de desarrollo, control y seguridad para los controles relacionados con las

versiones del Sofware que se está implementando, todo lo cual debe quedar inmerso en las cláusulas o especificaciones técnicas del contrato a ejecutar.

Objetivo de control A15 - Relación con los proveedores y terceros

Política de la seguridad de la información para las relaciones con proveedores y terceros

Directrices:

a) ÚNICA debe establecer los criterios para la selección de proveedores y terceros, relativos a la experiencia, reputación, capacidad, adecuadas a las necesidades de la Institución y del bien o servicio a adquirir.
b) ÚNICA debe llevar a cabo un análisis de la información de la información que requiere el proveedor y/o tercero con el fin de establecer los criterios de acceso a los activos de información de la institución, a los sistemas de información, aplicativos, redes, etc., así mismo, deberá definir los requisitos de seguridad para procesar, almacenar, comunicar o suministrar información y, por último, deberá definir los planes o acciones de tratamiento para prevenir la materialización de los riesgos identificados.
c) Los acuerdos con los proveedores y terceros deben ser formalizados antes del inicio de las actividades con el proveedor.
d) ÚNICA debe definir como mecanismo de control en las relaciones contractuales un acuerdo de confidencialidad sobre la información obtenida bien sea por acceso físico o lógico y/o que haya sido entregada directamente por ÚNICA en el desarrollo de las actividades, con el fin de prevenir los riesgos de divulgación de información a la que tengan acceso, e incluir cláusulas que indiquen que dichos proveedores o terceros no están autorizados para utilizar los recursos de información, tecnología y conexión de red de la Institución para propósitos diferentes a los necesarios para el cumplimiento del objeto contractual suscrito.
e) Los proveedores o terceros no están autorizados a ejecutar ningún cambio sobre los recursos tecnológicos o la desactivación de controles de seguridad sin contar con la autorización formal de ÚNICA.
f) Los proveedores o terceros que acceden a la gestión, transformación o transmisión de la información de ÚNICA, deben conocer, aceptar y cumplir las políticas de seguridad de la información definidas.
g) ÚNICA realizará revisiones periódicas para verificar el cumplimiento de los acuerdos establecidos entre las partes.

Objetivo de control A16 - Gestión de incidentes de seguridad de información

Gestión de incidentes y mejoras en la seguridad de la información

Directrices:

a) ÚNICA debe asegurar que los eventos o incidentes de seguridad que se presenten con los activos de información, contenedores y recursos tecnológicos de información sean comunicados y atendidos oportunamente, empleando el procedimiento definido.
b) Todo el personal administrativo, docentes, contratistas y en general las partes interesadas en ÚNICA deben reportar al responsable de seguridad de la información en el menor tiempo posible eventos o incidentes que afecten la confidencialidad, integridad o la disponibilidad de la información, así como la violación a las políticas de seguridad.
c) Se debe llevar un cuadro control de los incidentes que se presenten en materia de seguridad de la información o protección de datos personales, relacionando como mínimo: fecha, incidente, actividades de contención, planes de acción para que no se vuelvan a presentar los incidentes.
d) El responsable de seguridad de la información estará encargado de catalogar los incidentes según el procedimiento definido asegurando una respuesta rápida y eficiente.
e) El responsable de seguridad de la información deberá investigar y proponer la solución más efectiva para los incidentes notificados, implementando las acciones necesarias para prevenir su reincidencia.
f) El responsable de seguridad de la información deberá escalar los incidentes de acuerdo con su criticidad, manteniendo registro del proceso de investigación y preservando la evidencia que sea recolectada como probatoria en procesos legales.
g) El responsable de seguridad de la información debe contar con una base de datos de los incidentes y eventos presentados que permita identificar los incidentes recurrentes o de alto impacto, al igual que una base de conocimiento con la información de la evaluación y la solución de cada caso que permita tomar acciones para reducir su tiempo de respuesta.
h) El responsable de seguridad de la información documentará las lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información; estas deben ser socializadas a los interesados conservando la respectiva confidencialidad.
i) El personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA, que se encuentren responsables después según los resultados de la investigación del incidente, asumirán las consecuencias legales, administrativas y disciplinarias, incluyendo lo establecido en la ley, relacionadas con seguridad de la información y protección de datos personales, y de acuerdo con lo establecido en el proceso disciplinario de ÚNICA.

Política de Recolección de Evidencias

Directrices:

a) ÚNICA establecerá un procedimiento de recolección de evidencia digital que aplicará una vez se ha identificado un incidente de seguridad de la información con el fin de realizar

investigaciones de informática forense que deriven en acciones legales o investigaciones disciplinarias.

b) El responsable de seguridad de información será el encargado de coordinar las actividades necesarias para la recolección de evidencia digital para, de acuerdo con las circunstancias, realizar el contacto con proveedores externos.
c) Deberán mantenerse los contactos apropiados con autoridades pertinentes para atender emergencias y recolectar evidencia de manera técnica, tales como el ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) o CCP (CAI Virtual de la Policía Nacional).

Objetivo de control A17 - Aspectos de seguridad de información en la continuidad del negocio

Política de la continuidad de la seguridad de la información

Directrices:

a) ÚNICA cuenta con recursos en la nube autorizados, como: Office 365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom, eltiempo.com, los cuales garantizan alta disponibilidad de la información allí almacenada. Además, se tiene permitido el trabajo remoto para todo el personal administrativo.
b) ÚNICA deberá contar con un Plan de Continuidad del Negocio que garantice la recuperación de los procesos y sistemas de información más críticos.
c) Estos planes deben incluir condiciones de seguridad de la información en las etapas de recuperación y retorno a la normalidad.
d) Se deberán llevar a cabo pruebas periódicas al Plan de Continuidad del Negocio, y se deberán documentar los resultados de dichas pruebas.

Objetivo de control A18 - Cumplimiento

Cumplimiento de Requisitos Legales y Contractuales

Directrices:

a) ÚNICA, a través del responsable de seguridad de la información, se asegurará de hacer la continua revisión, identificación, documentación y cumplimiento de las disposiciones legales y requisitos en materia de seguridad de la información aplicables a la Institución, con el fin de mitigar riesgos ocasionados por incumplimientos legales o contractuales.

Política de Privacidad y Protección de Información de Datos Personales

Directrices:

a) ÚNICA velará por la protección de datos personales dando cumplimiento a las disposiciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios, estableciendo los controles necesarios para asegurar la información que la Institución conozca y almacene del personal administrativo, docentes, contratistas y, en general, partes interesadas, y velará porque dicha información únicamente sea utilizada para las funciones propias de la Institución y no sea publicada, revelada o entregada a terceras partes sin autorización.
b) Todo el personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA que administren datos personales deberán conservar estricta confidencialidad de éstos.
c) La responsabilidad y confidencialidad sobre datos personales debe quedar explicita y aceptada por el personal administrativo de ÚNICA en una cláusula del contrato al momento de iniciar la relación contractual.
d) Los responsables de los recursos tecnológicos, deberán procurar o implementar los mecanismos apropiados sobre los sistemas para el control de los datos personales que permitan conservar su confidencialidad e integridad.
e) Se deberá contar con los procedimientos adecuados para la recolección, almacenamiento, uso, circulación y supresión o disposición final de la información personal incluyendo los requisitos para obtener la autorización de los titulares, la atención de peticiones de titulares para el acceso, la actualización y corrección de datos personales, la conservación y eliminación de información personal; igualmente, para dar cumplimiento a las obligaciones frente a la SIC – Superintendencia de Industria y Comercio.

Derechos de propiedad intelectual

Directrices:

a) ÚNICA velará porque el software instalado en los recursos tecnológicos cumpla con todos los requerimientos legales y de licenciamiento aplicables referente a derechos de autor y propiedad intelectual, así mismo, propenderá al cumplimiento por parte del personal administrativo, docentes, contratistas y, en general, partes interesadas, que hagan uso de los recursos tecnológicos.
b) El responsable del proceso de Gestión Tecnológica deberá garantizar que todo el software esté protegido por derechos de autor y posea su licencia de uso o, en su defecto, sea software de libre distribución y uso, para lo cual contará con un inventario del software permitido en la Institución e implementará controles para la instalación de software autorizado únicamente.
c) El responsable del personal administrativo de ÚNICA debe cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software y la reproducción no autorizada es una violación a la ley.

Revisión de la Seguridad de la Información

Directrices:

a) El Comité de Alta Gerencia verificará el cumplimiento de políticas, procedimientos, objetivos y de la implementación de controles de seguridad de información definidos para ÚNICA, a través de los resultados de las auditorias planificadas, los seguimientos periódicos y los resultados de las métricas establecidas, con la finalidad de abordar iniciativas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de los activos de información.

Seguimiento y control de las políticas (monitoreo)

La política general y las políticas específicas de seguridad de la información, deben ser revisadas por el responsable de la seguridad de la información de manera periódica como mínimo una vez al año o cuando se presenten cambios significativos que requieran de su actualización.

Aprobación

Versión	Fecha	Aprobó
01	25/05/2022	Sala General - Acuerdo 06 del 25 de mayo de 2022 (Acta 48)

Nota: Esta política hace parte integral del Acuerdo 06 del 25 de mayo de 2022 de la Sala General.