



Política del Sistema de Gestión de Seguridad de la Información




Bogotá D.C., Colombia – 15 de diciembre de 2023

Contenido

1. Objetivo.....	3
2. Alcance	3
3. Definición	3
4. Normas y políticas	3
5. Lineamientos.....	4
5.1 Políticas de la Seguridad de la Información.....	5
5.1.1 Implementación de la política	6
5.1.1.1 Aspectos relacionados con la Toma de conciencia, educación y formación en seguridad de la información.....	6
5.1.1.2 Aspectos relacionados con el proceso de Talento Humano.....	7
5.1.1.3 Aspectos relacionados con la Gestión de activos de información	8
5.1.1.4 Aspectos relacionados con la realización de proyectos Administrativos, Financieros o Académicos.....	9
5.1.1.5 Aspectos relacionados con el acceso a los servicios de red y sistemas de información.....	9
5.1.1.6 Aspectos relacionados con el manejo del correo electrónico.....	11
5.1.1.7 Aspectos relacionados con el manejo de dispositivos móviles	11
5.1.1.8 Aspectos relacionados con el trabajo remoto	13
5.1.1.9 Aspectos relacionados con la Gestión de Medios Removibles	13
5.1.1.10 Aspectos relacionados con la Seguridad Física y del Entorno.....	13
5.1.1.11 Aspectos relacionados con la organización del escritorio y pantalla asignada..	14
5.1.1.12 Aspectos relacionados con la Seguridad de las operaciones	15
5.1.1.13 Aspectos relacionados con la Seguridad en las Comunicaciones.....	17
5.1.1.14 Aspectos relacionados con la adquisición, desarrollo y mantenimiento de sistemas	18
5.1.1.15 Aspectos relacionados con los proveedores y terceros	19
5.1.1.16 Aspectos relacionados con la gestión de incidentes de seguridad de información	19
5.1.1.17 Aspectos relacionados con el Cumplimiento	20
6 Control de cambios.....	22
7 Revisión y Aprobación.....	22



 <p>Vigilada MinEducación</p>	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 3 de 22

1. Objetivo

Establece las políticas que regulan la seguridad de la información en ÚNICA y presenta en forma clara y coherente los elementos que el personal administrativo, los docentes, los contratistas y, en general, las partes interesadas deben conocer, acatar y cumplir para garantizar la confidencialidad, integridad y disponibilidad de la información gestionada por los procesos institucionales.

Con estas políticas se espera consolidar una cultura de ciberseguridad, reducir el impacto de los riesgos de seguridad de la información y mantener actualizadas las directrices de acuerdo con la normatividad vigente aplicable a la Institución.

2. Alcance

Las políticas de seguridad de la información contenidas en este manual aplican a 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, los docentes, los contratistas y, en general, por las partes interesadas que generen, accedan o utilicen información de la Institución.

3. Definición

- **Sistema de Gestión de Seguridad de la Información - SGSI:** es un conjunto de políticas de administración de la información. De acuerdo con la ISO/IEC 27000 n SGSI consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.
- **Ciclo de gestión PHVA:** ciclo de gestión definido por Deming PHVA Planear – Hacer – Verificar – Actuar, es una estrategia de mejora continua y usada para implementar cambios. No es un proceso que se ejecuta una sola vez, sino un espiral continuo que busca mejorar los procesos e iteraciones.
- **Gestión de Salud y Seguridad en el Trabajo -SST:** busca permanente la prevención y promoción de la salud en el trabajo y la identificación del origen de las enfermedades profesionales y de los accidentes de trabajo.
- **Activos de información:** es aquella información que resulta fundamental para la organización. Los activos de información pueden ser archivos, bases de datos, contratos, acuerdos, documentación del sistema, manuales de los usuarios, informes, etc. y estos se son contenidos en aplicaciones, servidores, medios físicos, las personas, archivador, etc.

4. Normas y políticas


- Decreto 1360 de 1989. Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen

las entidades de certificación y se dictan otras disposiciones.

- Ley 599 de 2000. Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático, protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.
- Acuerdo 060 de 2001. Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1341 de 2009. Marco General del Sector de TIC. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones-TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Ley 1437 de 2011. Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013. Por la cual se reglamenta parcialmente la Ley 1581 de 2012 para la protección de datos personales.
- Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- Decreto 1074 de 2015. Del ministerio de Comercio, Industria y Turismo. Capítulo 26 Registro Nacional de Bases de Datos
- Decreto 1078 de 2015. Ministerio de Tecnologías de la Información y las comunicaciones. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Decreto Reglamentario Único 1081 de 2015 - Decreto 103 de 2015. Reglamento sobre la gestión de la información pública.
- Decreto Número 115 del 29 de junio de 2017. Por el cual se modifica el artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 – Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Amplía el plazo de inscripción de las Bases de Datos en el Registro Nacional de Bases de Datos

5. Lineamientos

ÚNICA, cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) 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 de la información, crear un ambiente de cultura y conciencia de seguridad de la información, y mantener un proceso de

 <p>Vigilada MinEducación</p>	<p>POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 5 de 22

mejora continua de protección de la información.

Para la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información SGSI se contempla el ciclo de gestión definido por Deming PHVA Planear – Hacer – Verificar – Actuar, el cual se basa en la realización constante de 4 pasos que describimos a continuación:

- Planear (Definir el SGSI): Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de la Institución.
- Hacer (Implementar y operar el SGSI): Implementar la política, los controles, procesos y procedimientos del SGSI.
- Verificar (hacer seguimiento y revisar el SGSI): Evaluar y en donde sea aplicable, medir el desarrollo de la política, reportar los resultados para su revisión e identificar los aspectos a mejorar.
- Actuar (mantener y mejorar el SGSI): Empezar acciones preventivas y correctivas con base en los resultados de la implementación del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

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.
- 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.

5.1 Políticas de la Seguridad de la Información.

ÚNICA, se compromete a preservar la confidencialidad, disponibilidad e integridad, de sus activos de información, protegiéndolos contra amenazas internas y externas, mediante la implementación del Sistema de Gestión de Seguridad de la Información y la metodología para la gestión del riesgo, manteniendo la mejora continua; adicionalmente a cumplir con las disposiciones constitucionales y legales aplicables a la institución, así como las disposiciones internas, relacionadas con la seguridad de la información.

- Estructura para la implementación:

ÚNICA cuenta 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 SGSI que permite promover las iniciativas de seguridad de la información que sean pertinentes a la estructura de la institución, y cuenta con unas responsabilidades claramente asignadas y comunicadas a los colaboradores de la Institución.

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 6 de 22

La estructura definida se describe a continuación:

- El Comité de Desarrollo Institucional es el responsable de revisar y aprobar las modificaciones realizadas a la Política del Sistema de Gestión de Seguridad de la Información, así como de garantizar su divulgación a los colaboradores (personal administrativo y docentes de UNICA), contratistas y, en general, partes interesadas en la Institución.
- El Comité de Desarrollo Institucional que, al abordar en su agenda los asuntos relacionados con la Política del Sistema de Gestión de Seguridad de la Información (SGSI) y la Política de Protección de Datos Personales, cuenta con la participación de:
 - Rectoría UNICA
 - Vicerrectoría Académica
 - Dirección de Planeación y Aseguramiento de la Calidad
 - Dirección Financiera y Administrativa
 - Dirección de Innovación y Desarrollo Tecnológico
 - Coordinación de Tecnología
 - Dirección de Comunicaciones y Mercadeo
- El Comité de Desarrollo Institucional 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 UNICA.
- El responsable de Seguridad de la Información es el Coordinador de Tecnología quien tiene 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.
- Sumado a esto, la Institución ha definido una serie de actividades y responsables frente a la identificación de los riesgos de seguridad de la información y la gestión de los incidentes de seguridad de la información los cuales se encuentran descritos en los documentos:
 - El “Instructivo Evaluación de Riesgos de Seguridad de la Información I-GT-01” contiene la identificación, valoración de los riesgos definidos por la Institución, así como, las acciones para su aceptación y seguimiento.
 - El “Instructivo Gestión de Incidentes de Seguridad de la Información I-GT-02” contiene las orientaciones para la identificación, valoración y seguimiento de los incidentes de seguridad de la información presentados en la Institución.

5.1.1 Implementación de la política

Para la implementación de esta política la Institución ha definido una serie de directrices que contemplan el cumplimiento normativo administrativo y disciplinario en materia de seguridad de la información que se describen a continuación:

5.1.1.1 Aspectos relacionados con la Toma de conciencia, educación y formación en seguridad de la información






- a) El Coordinador de Tecnología debe incluir 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 Coordinador de Tecnología realiza la revisión de los resultados de las evaluaciones de las capacitaciones en seguridad de la información para identificar oportunidades de mejora.
- c) El Coordinador de Tecnología promueve la realización de actividades de sensibilización y concienciación en temas de Seguridad de la Información a contratistas y terceros que prestan sus servicios o tengan algún tipo de relación con ÚNICA, según las necesidades identificadas en la “Matriz de Evaluación de Riesgos de Seguridad de la Información F-GT-01”.
- d) La sensibilización en seguridad de la información y protección de datos personales se debe realizar mínimo cada 6 meses a través de campañas de divulgación.

5.1.1.2 Aspectos relacionados con el proceso de Talento Humano

- Antes de asumir el empleo
 - a) El proceso de Gestión de Talento Humano realiza la verificación de antecedentes ante las siguientes entidades: Registraduría Nacional del Estado Civil, Policía Nacional de Colombia, Contraloría General de la República y Procuraduría General de la Nación, 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. La Asistente Administrativa realiza esta verificación en el proceso de selección y contratación del personal administrativo y docente.
 - b) El proceso de Gestión del Talento Humano debe establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
- Proceso de Vinculación
 - a) Todo colaborador, debe firmar cláusulas en las que se establezca un acuerdo de confidencialidad y no divulgación de la información reservada de ÚNICA, lo cual se incluye en el contrato laboral.
 - b) El proceso de Gestión del Talento Humano debe garantizar la capacitación y sensibilización sobre la Política del Sistema de Gestión de Seguridad de la Información a todo el personal administrativo durante el proceso de inducción y reinducción, según lo establecido Ley 1581 de 2012 y sus decretos reglamentarios, y su compromiso queda firmado en el formato de inducción.
 - c) El Coordinador de Tecnología debe evaluar que los colaboradores hayan entendido la política de seguridad de la información socializada en el proceso de inducción y reinducción a través de una entrevista o prueba escrita.

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 8 de 22

- Durante la vinculación laboral
 - a) Es responsabilidad del colaborador informar al Coordinador de Tecnología los incidentes de seguridad de la información que observe.
 - b) En el caso de presentarse una violación a la seguridad de la información por parte del colaborador, el responsable establecido en el Reglamento de Trabajo y el Reglamento Docente debe liderar la aplicación del proceso disciplinario según corresponda. Dicho proceso debe ser de conocimiento de los colaboradores de ÚNICA.
 - c) En el caso de que un colaborador cambie de funciones, se debe informar al Coordinador 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. Es responsabilidad del jefe inmediato del colaborador solicitar los accesos y ajustes requeridos para el desarrollo de las nuevas funciones.
 - d) Los colaboradores deben tener en cuenta los demás lineamientos descritos en esta Política requeridos para el buen desarrollo de sus funciones.

- Terminación y cambio del empleo
 - a) El responsable de Talento Humano debe informar inmediatamente al Coordinador de Tecnología sobre la desvinculación de un colaborador de ÚNICA para que sean retirados los accesos físicos, tecnológicos y de sistemas de información a los cuales tenga acceso.
 - b) Es de responsabilidad del colaborador realizar la entrega de la información propia de ÚNICA a la que tenga acceso y garantizar la eliminación de ésta de los dispositivos personales.
 - c) Se debe solicitar la devolución de los elementos institucionales asignados como carné, equipo de cómputo, celular, etc., de acuerdo con el “Listado de Entrega de Equipos - dispositivos F-GT-04”.

5.1.1.3 Aspectos relacionados con la Gestión de activos de información

- a) Los activos de información se identifican y clasifican teniendo en cuenta los impactos que le pueden causar a ÚNICA por la pérdida de confidencialidad, integridad y disponibilidad, como se observa en la “Matriz de Activos de Información F-GD-01”, de acuerdo con la Ley 1581.
- b) ÚNICA mantiene la Matriz de Activos de Información F-GD-01 actualizada y es responsabilidad de cada líder de proceso los activos de información a su cargo.
- c) El Director de Planeación y Aseguramiento de la Calidad y el Coordinador de Tecnología anualmente deben revisar la Matriz de Activos de Información y la Matriz de Riesgos de Seguridad de la Información y realizar las actualizaciones requeridas.
- d) ÚNICA promueve 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 de los colaboradores, contratistas y, en general, partes interesadas en ÚNICA que se encuentran autorizados y requieren de ella para la ejecución de sus actividades.
- e) Todo líder de proceso es responsable de realizar la valoración de activos, y

contenedores de información siguiendo la metodología definida, y el Director de Planeación y Aseguramiento de la Calidad y el Coordinador de Tecnología deben acompañar el proceso.

- f) Todo colaborador debe prevenir los riesgos a los que está expuesta la información, evitando la copia, divulgación, destrucción física o digital de la información sin previa autorización.
- g) Todo colaborador debe realizar la entrega formal de todos los activos de información físicos y electrónicos en el proceso de desvinculación.
- h) En caso de requerirse la eliminación de activos de información, los responsables de los activos realizan la disposición segura del activo de información de acuerdo con lo previsto en los procedimientos de gestión documental y activos de información.
- i) Todo colaborador, contratista y, en general, las partes interesadas en ÚNICA tienen a su disposición el uso de activos de información y los recursos tecnológicos que los contienen, de acuerdo con sus funciones o responsabilidad.
- j) Todos los colaboradores aceptan y se acogen a las Políticas de Seguridad de la Información que se encuentran en este documento.

5.1.1.4 Aspectos relacionados con la realización de proyectos Administrativos, Financieros o Académicos


- a) Los proyectos que se desarrollan 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 basados en la Matriz de Evaluación de Riesgos de Seguridad de la Información F-GT-01.
- b) En cualquier caso, los proyectos desarrollados deben estar alineados con las políticas de seguridad contenidas en el presente documento.

5.1.1.5 Aspectos relacionados con el acceso a los servicios de red y sistemas de información

- a) La Rectoría, la Vicerrectoría Académica y los Directores de área aprueban 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) Los procesos de Gestión del Talento Humano y de Tecnología definen la creación, actualización, activación e inactivación de cuentas de usuario.
- c) El Coordinador de Tecnología debe velar por que los servicios tecnológicos estén debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta los roles (estudiante, colaborador, docente o administrador) y perfil para cada sistema de información según el registro de roles definido.
- d) El Coordinador de Tecnología debe asegurar que las redes inalámbricas de la Institución cuenten con métodos de autenticación que eviten accesos no autorizados.
- e) El Coordinador de Tecnología debe suministrar y garantizar a los colaboradores el cambio de contraseña para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados por el jefe inmediato, según su perfil y

rol.

- f) El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos es personal e intransferible. Toda cuenta de usuario es de uso personal e intransferible. El usuario es responsable de todas las acciones o transacciones efectuadas con su cuenta de usuario.
- g) 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.
- h) El Coordinador de Tecnología debe realizar el cambio de contraseña de la red inalámbrica de la Institución periódicamente mínimo una (1) vez al año.
- i) El Coordinador de Tecnología debe revisar que los colaboradores, contratistas, proveedores o partes interesadas que se conecten a la red de datos de ÚNICA cuenten con sistema operativo licenciado y antivirus y únicamente puedan realizar las tareas para las que fueron autorizados.
- j) El Coordinador de Tecnología debe mantener un listado actualizado de las cuentas de administración de los recursos tecnológicos: licencias, cuentas Zoom, software, computadores.
- k) El Coordinador de Tecnología define la estructura del acceso teniendo en cuenta lo siguiente:
 - Las contraseñas no deben ser visibles en la pantalla al momento de ser ingresadas.
 - La complejidad de la contraseña debe ser mínimo de 10 caracteres, y debe combinar mayúsculas, minúsculas, números y caracteres especiales.
 - No se debe repetir las últimas 3 contraseñas utilizadas en cada sistema o servicio tecnológico.
 - Las contraseñas para los sistemas operativos se deben cambiar obligatoriamente cada 6 meses.
 - Las contraseñas para los equipos como computadores se deben cambiar cada 6 meses.
- l) El Coordinador de Tecnología debe gestionar una herramienta para el almacenamiento adecuado de credenciales de acceso de forma segura. Ej., KeePass.
- m) Las contraseñas no se deben registrar en papel, correo electrónico y/o archivos digitales a menos que se puedan almacenar de forma segura.
- n) Se debe cambiar la contraseña si se ha detectado anomalía en la cuenta de usuario.
- o) Los colaboradores al crear contraseñas no deben usar palabras comunes que se pueden encontrar en diccionarios, ni que estén relacionadas con la vida personal de los mismos.
- p) Está prohibido acceder a páginas con contenido pornográfico y demás condiciones que degraden la condición humana y resulten ofensivas para el personal administrativo, los docentes, contratistas y, en general, para las partes interesadas en ÚNICA. Así mismo, está prohibido acceder a juegos en línea y el uso de redes sociales con fines diferentes a los laborales.
- q) Toda la información procesada y almacenada en los recursos de ÚNICA está asociada a la labor que desempeña el colaborador en desarrollo de sus funciones y cargos, por lo cual esta información es de carácter institucional. En este sentido, los colaboradores se deben abstener de almacenar y procesar información de carácter

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 11 de 22

- personal en los recursos provistos por ÚNICA.
- r) Los usuarios no pueden copiar o distribuir software, cambiar las configuraciones de los recursos tecnológicos y deben utilizar únicamente los programas y equipos autorizados por el Coordinador de Tecnología, quien es el autorizado para instalar o configurar software y equipos bajo licenciamiento.
 - s) La descarga, instalación o uso de software ilegal o sin licenciar es considerada como una violación a las políticas de seguridad de la información de ÚNICA.
 - t) Los recursos se deben usar estrictamente para fines laborales. Los colaboradores no pueden 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.
 - u) Los colaboradores no deben realizar actividades que puedan degradar el desempeño de los recursos tecnológicos y, por ende, generar posibles pérdidas o daños en la información.
 - v) El administrador del sistema debe revisar los usuarios activos en el sistema de acuerdo con la matriz de roles y perfiles definida.


5.1.1.6 Aspectos relacionados con el manejo del correo electrónico

- a) 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 características que degraden la condición humana y resulten ofensivas para el personal administrativo, docentes, contratistas y, en general, para las partes interesadas en ÚNICA.
- b) No está permitido el uso de cuentas personales para el almacenamiento o intercambio de información Institucional de ÚNICA.
- c) 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 (cuentas externas).
- d) Los mensajes de correo electrónico deben ir acompañados del siguiente *disclaimer* o descargo de responsabilidad:
“Este mensaje electrónico y sus anexos contienen información de la Institución Universitaria Colombo Americana – ÚNICA, de carácter confidencial y para uso exclusivo de la persona o institución de destino. Si recibes esta información por error, por favor, elimínala y contacta de inmediato a su remitente, al teléfono o e-mail señalados en la firma del correo. La copia, reproducción, difusión o cualquier uso indebido de esta información está prohibida y es penalizada por la Ley”.
- e) Los colaboradores al dar respuesta a un correo electrónico deben revisar la necesidad de incluir o no, el histórico de la comunicación manteniendo la confidencialidad de los temas analizados al interior de la institución.

5.1.1.7 Aspectos relacionados con el manejo de dispositivos móviles


Los aspectos relacionados con el manejo de dispositivos móviles se establecen según el tipo del dispositivo, como sigue:



 Vigilada MinEducación	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 12 de 22

- Teléfonos inteligentes personales que se usan en procesos institucionales:
El uso de teléfonos inteligentes está autorizado para todos los colaboradores de ÚNICA, siempre y cuando se declare por parte del propietario, en el formato “Acuerdo de Acceso a Sistemas y Datos desde Dispositivos Personales” F-GT-05, que dicho dispositivo cuenta con las actualizaciones más recientes del sistema operativo 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.
 - Dar un manejo confidencial al uso de las contraseñas del dispositivo.
 - Hacer un uso adecuado del internet según las políticas de navegación definidas en este manual.
 - Mantener los dispositivos con las últimas versiones de software.

- Computadores y portátiles:
 - a) El Coordinador de Tecnología cuenta con privilegios de administrador local para el desarrollo de sus funciones.
 - b) El Coordinador de Tecnología asigna a los colaboradores equipos institucionales que cuentan con un sistema operativo y un software antivirus licenciados.
 - c) El Coordinador de ÚNICA debe verificar, cuando se estime necesario, que los equipos institucionales autorizados cumplen las políticas establecidas y debe reportar cualquier novedad en el formato de “Control de Inventario de Tecnología F-GT-06”.
 - d) En caso de requerirse el uso de equipos personales por parte de los colaboradores se procede a diligenciar el “Acuerdo de Acceso a Sistemas y Datos desde Dispositivos Personales F-GT-05”, en el que se indica que dicho equipo cuenta con sistema operativo licenciado y que el colaborador se hace responsable de:
 - e) Instalar aplicaciones únicamente desde los repositorios oficiales.
 - f) 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.
 - g) Si la Institución adquiere nuevos recursos de almacenamiento, su uso será informado y autorizado a través de correo electrónico.
 - h) Dar un manejo confidencial a la información almacenada o accedida desde dicho equipo.
 - i) Dar un manejo confidencial al uso de las contraseñas del computador o portátil personal.
 - j) Hacer un uso adecuado del internet según las políticas de navegación definidas en este manual.
 - k) Mantener los dispositivos actualizados con las últimas versiones de software.
 - l) Ante la pérdida del equipo portátil, se debe 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.
 - m) Cuando la labor contractual termine, el colaborador debe declarar en el formato asignado que se llevó a cabo el borrado de toda la información de ÚNICA que pudo

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 13 de 22

haberse almacenado en el equipo personal.

5.1.1.8 Aspectos relacionados con el trabajo remoto


- a) El trabajo remoto está permitido en ÚNICA para los colaboradores de acuerdo con lo definido con la Rectoría.
- b) ÚNICA debe garantizar la doble autenticación en los accesos remotos al Office 365 de uso Institucional.
- c) Los repositorios autorizados para el almacenamiento de información en ÚNICA son: Office365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom y elempleo.com. Si la Institución adquiere nuevos recursos de almacenamiento, su uso será informado y autorizado a través de correo electrónico. No está permitido el almacenamiento de información en el equipo personal.
- d) Está prohibido instalar programas o software en los equipos suministrados por ÚNICA. El Coordinador de Tecnología es el único autorizado para instalar o configurar software y equipos bajo licenciamiento.
- e) El colaborador es responsable por el equipo de cómputo asignado y por los daños ocasionados por su mal uso.
- f) Es responsabilidad del colaborador salvaguardar la información institucional contenida en los diferentes repositorios a los cuales accede, evitando compartir las claves de ingreso con personas ajenas a ÚNICA.
- g) Está prohibido que el colaborador haga uso del equipo de cómputo asignado en sitios públicos o diferentes a los autorizados por ÚNICA.
- h) El Coordinador de Tecnología debe verificar periódicamente el cumplimiento de las condiciones técnicas y de seguridad aquí establecidas en este documento.

5.1.1.9 Aspectos relacionados con la Gestión de Medios Removibles

- 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, se usan bajo la responsabilidad del Director de cada área en el desarrollo de sus funciones.

5.1.1.10 Aspectos relacionados con la Seguridad Física y del Entorno

- Áreas seguras
 - a) El acceso físico a las instalaciones está controlado por el personal de seguridad del Centro Colombo Americano y es complementado con el control de cámaras de seguridad en el ingreso de personal.
 - b) 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 los colaboradores.
 - c) Los visitantes deben estar autorizados por el área responsable de la visita y deben estar acompañados en todo momento por un colaborador de ÚNICA.
 - d) Siempre debe permanecer una persona en las oficinas. De lo contrario, las oficinas


 <p>Vigilada MinEducación</p>	<p>POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 14 de 22

deben quedar con llave.

- e) La Asistente Administrativa como Brigadista debe gestionar con el Centro Colombo Americano los requerimientos relacionados con los extintores y camilla, y con la Dirección Financiera y Administrativa de ÚNICA lo relacionado con el botiquín de emergencia.
 - f) El proceso de Gestión SST debe establecer los planes de emergencia contra amenazas externas y ambientales.
 - g) Cabe resaltar que ÚNICA mantiene sus servicios tecnológicos en la nube por lo que no cuenta con *data center* en sus instalaciones.
- Equipos
 - a) El Coordinador de Tecnología debe velar 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 Coordinador de Tecnología debe definir mecanismos de soporte y mantenimiento para los equipos de cómputo y equipos de red y debe llevar registro de éstos.
 - c) Cuando un equipo sea reasignado o retirado de servicio, el Coordinador de Tecnología garantiza la eliminación de toda información mediante mecanismos de borrado seguro, teniendo en cuenta que previo a esta actividad se debe realizar una copia de seguridad.
 - d) El Coordinador de Tecnología 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.

5.1.1.11 Aspectos relacionados con la organización del escritorio y pantalla asignada.

- a) Todos los colaboradores de ÚNICA deben 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 de los colaboradores debe permanecer organizado y la información clasificada como confidencial o sensible, debe guardarse bajo llave, mientras el responsable de ésta no esté trabajando con ella.
- c) Los equipos de cómputo con información de ÚNICA deben 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 deben ser retirados inmediatamente de las impresoras, fax, fotocopiadoras y escáneres.
- e) Se debe tener control de la información en físico que se presta a otras áreas o que sale de las instalaciones de ÚNICA.
- f) No se deben reutilizar o reciclar documentos impresos clasificados como


 <p>Vigilada MinEducación</p>	<p>POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 15 de 22

confidenciales o sensibles. Estos deben ser destruidos garantizando que no queden disponibles para su uso.

5.1.1.12 Aspectos relacionados con la Seguridad de las operaciones

- Procedimientos operacionales y responsabilidades
 - a) El Coordinador de Tecnología debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.
 - b) El Coordinador de Tecnología 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 *Roll back* (Deshacer cambio).
 - c) El Coordinador de Tecnología debe evaluar, aprobar o negar la implementación de los cambios requeridos, teniendo en cuenta los posibles riesgos que se puedan presentar.
 - d) El Coordinador de Tecnología y el Director de Innovación y Desarrollo Tecnológico son responsables de los sistemas de información y de los servicios tecnológicos y por tanto deben gestionar la capacidad, llevar a cabo las proyecciones de crecimiento y alertar cuando dichas capacidades estén llegando a los límites establecidos.

- Protección contra códigos maliciosos
 - a) ÚNICA cuenta con un antivirus Institucional que debe estar instalado en todos los equipos institucionales.
 - b) El Coordinador de Tecnología debe garantizar que el software antivirus se mantenga actualizado con las últimas firmas y debe monitorear las alertas generadas por dicho software en donde se encuentre instalado.
 - c) El Coordinador de Tecnología debe definir los pasos para la detección, prevención y recuperación contra códigos maliciosos.
 - d) El Coordinador de Tecnología debe promover la cultura de seguridad de la información, entre el personal administrativo, docentes, contratistas y, en general, con las partes interesadas en ÚNICA que permitan 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 Coordinador de Tecnología debe asegurar que no se pueda detener el software antivirus instalado en los equipos institucionales.
 - g) Los colaboradores deben 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

	<p style="text-align: center;">POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 16 de 22

notificar de inmediato al Coordinador de Tecnología con el fin de tomar las medidas correspondientes.

- Copias de respaldo
 - a) El Coordinador de Tecnología y el Director de Innovación y Desarrollo Tecnológico deben definir y documentar el proceso para la generación de las copias de respaldo de la información más crítica almacenada en la nube. Este proceso establece el esquema de qué, cómo, quién y con qué periodicidad es necesario realizar el copiado de la información, así como el tipo de respaldo requerido y nivel de criticidad identificado.
 - b) Se deben llevar a cabo *back-ups* o copias de respaldo de la configuración e información crítica almacenada en sistemas de información y aplicaciones, las cuales se deben almacenar en el OneDrive Institucional.
 - c) En caso de ser necesario, se debe 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.
 - d) El Coordinador de Tecnología 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.
 - e) Los líderes de procesos deben guardar la información en los recursos en la nube autorizados como, por ejemplo. Office 365 (Correo, Teams, OneDrive, SharePoint), DATASAE – SIGA, Clientify, Open Journal System, Zoom, elemplo.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

El responsable del sistema o el Coordinador de Tecnología debe:

- a) Parametrizar los registros de auditoría que contengan excepciones o eventos relacionados con la seguridad en los sistemas administrados.
- b) Salvaguardar los registros de auditoría que se generen en los sistemas administrados
- c) Monitorear excepciones a los eventos de la seguridad de información.
- d) Garantizar que los sistemas de información y servicios tecnológicos tengan configurada la misma zona horaria para facilitar futuras investigaciones.
- e) Monitorear los registros de eventos realizados por los responsables de los sistemas o servicios tecnológicos.

- Control de software operacional

El Coordinador de Tecnología debe:

- a) Controlar la instalación de software no autorizado mediante la configuración de un usuario administrador local en los equipos Institucionales.
- b) Configurar los equipos institucionales para que instalen actualizaciones de seguridad



- en los sistemas operativos automáticamente.
- c) Definir el listado de aplicaciones permitidas para estar instaladas en los equipos institucionales en el formato “Listado de aplicativos por área” F-GT-08.
 - d) Realizar de manera periódica una inspección del software instalado en los equipos institucionales y debe desinstalar el software no autorizado.
 - e) Y demás lineamientos descritos en este documento.
- Gestión de Vulnerabilidades Técnicas

El Coordinador de Tecnología debe:


- a) 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) Documentar, informar, gestionar y corregir las vulnerabilidades encontradas.

5.1.1.13 Aspectos relacionados con la Seguridad en las Comunicaciones

- Gestión de seguridad de las redes

El Coordinador de Tecnología debe:

- a) Realizar monitoreo sobre la utilización del servicio de internet a través del antivirus.
 - b) Implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos.
 - c) Proteger la red mediante el uso de dispositivos perimetrales, como *firewalls*.
 - d) Proteger el acceso a la red inalámbrica mediante el uso de protocolos fuertes de autenticación, como WPA2, así mismo, debe cambiar la contraseña de acceso a la red inalámbrica periódicamente mínimo (1) vez al año.
- Transferencia de información
- a) Se garantiza 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 debe 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 validados por el director de área o el Coordinador de Tecnología.
 - d) El Comité de Desarrollo Institucional es el responsable de autorizar la entrega de información confidencial a la autoridad, ente regulador, de control, de vigilancia o

 <p>Vigilada MinEducación</p>	<p>POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</p>	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 18 de 22


judicial que lo requiera formalmente.

- e) La información confidencial transmitida por correo electrónico debe protegerse mediante archivos Zip con contraseña y la contraseña se debe comunicar por un canal de comunicación diferente.
- Acuerdos de confidencialidad o de no divulgación
- 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 explícitas y aceptadas en un documento de acuerdo de confidencialidad o cláusula del contrato al momento de iniciar alguna relación contractual.

5.1.1.14 Aspectos relacionados con la adquisición, desarrollo y mantenimiento de sistemas

El responsable de los sistemas de información y el Coordinador de Tecnología deben:

- 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.
- b) Establecer en lo posible ambientes de desarrollo, prueba y producción por separado.
- c) Asegurar que no se usen datos personales y sensibles en ambientes de prueba.
- d) Asegurar que se asignen los privilegios mínimos requeridos para el desarrollo de las actividades por parte del colaborador en los ambientes de producción.
- e) Asegurar que la autenticación de los usuarios en Office 365 mediante múltiple factor de autenticación.
- f) 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.
- g) 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.
- h) 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) Realizar mantenimiento periódico y planificado a los sistemas de información, para garantizar su correcto funcionamiento (depuración de usuarios, bases de datos,

	POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Código: PL-GT-02	
		Proceso: Gestión Tecnológica	
		Fecha aprobación: 15-12-2023	
		Versión: 02	Página 19 de 22

configuraciones, parámetros, entre otros y demás que puedan resultar en un incidente).

- j) 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) 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 software que se está implementando, todo lo cual debe quedar descrito en las cláusulas o especificaciones técnicas del contrato a ejecutar.

5.1.1.15 Aspectos relacionados con los proveedores y terceros

- a) ÚNICA debe establecer los criterios para la selección de proveedores y terceros, relativos a la experiencia, reputación y 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 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, debe definir los requisitos de seguridad para procesar, almacenar, comunicar o suministrar información y, por último, debe 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 debe realizar revisiones periódicas para verificar el cumplimiento de los acuerdos establecidos entre las partes.

5.1.1.16 Aspectos relacionados con la gestión de incidentes de seguridad de información

- a) Todo colaborador, contratista y, en general, las partes interesadas en ÚNICA deben

reportar los incidentes según el “Instructivo Gestión de Incidentes de Seguridad de la Información I-GT-02”.

- b) Se debe llevar un registro 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 en el formato “Atención de Incidentes de Seguridad de la Información F-GT-03”.
- c) El Coordinador de Tecnología debe investigar y proponer la solución más efectiva para los incidentes notificados, implementando las acciones necesarias para prevenir su reincidencia.
- d) El Coordinador de Tecnología debe 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, según el “Instructivo Gestión de Incidentes de Seguridad de la Información I-GT-02”.
- e) El personal administrativo, docentes, contratistas y, en general, las partes interesadas en ÚNICA que se encuentren responsables según los resultados de la investigación del incidente asumen 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.
- f) Se deben mantener los contactos apropiados con autoridades pertinentes para atender incidentes de seguridad, tales como el ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) o CCP (CAI Virtual de la Policía Nacional) y demás autoridades que respalden la atención de una emergencia. Ver Formato “Listado de Contactos de Emergencia en ÚNICA F-SST-01”.

5.1.1.17 Aspectos relacionados con el Cumplimiento

- Cumplimiento de Requisitos Legales y Contractuales

ÚNICA, a través del Coordinador de Tecnología y Directores de Área, debe realizar la 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

- a) ÚNICA debe gestionar 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, de las partes interesadas, y debe vigilar que 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 deben conservar estricta confidencialidad de éstos.



- c) La responsabilidad y confidencialidad sobre datos personales debe quedar explícita y aceptada por los colaboradores de ÚNICA en una cláusula del contrato al momento de iniciar la relación contractual.
- d) Los responsables de los recursos tecnológicos deben 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 debe 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

- a) ÚNICA debe garantizar que 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, debe propender por el cumplimiento por parte del personal administrativo, docentes, contratistas y, en general, de las partes interesadas, que hagan uso de los recursos tecnológicos.
- b) El Coordinador de Tecnología debe 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 cuenta con un inventario del software permitido en la Institución y además, debe implementar controles que validen la instalación de software autorizado únicamente.

- Revisión de la Seguridad de la Información

El Comité de Desarrollo Institucional verifica el cumplimiento de políticas, procedimientos, objetivos y de la implementación de controles de seguridad de la información definidos para ÚNICA, a través de los resultados de las auditorías 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.

- Aspectos relacionados con el mejoramiento continuo.

- a) El Coordinador de Tecnología debe actualizar la documentación del sistema de acuerdo con 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.
- b) El Coordinador de Tecnología se mantiene informado sobre las últimas prácticas de seguridad y privacidad en la gestión de la información. La educación continua ayuda a adaptarse a nuevas amenazas y a mantener los datos protegidos.
- c) El Coordinador de Tecnología, el Director de Innovación y Desarrollo Tecnológico, el Director de Planeación y Aseguramiento de la calidad y demás directivos y

colaboradores de la Institución pueden presentar propuestas al Comité de Desarrollo Institucional sobre ajustes, modificaciones, buenas prácticas, nuevas actividades, software, hardware que permitan garantizar la seguridad de la información.

- d) Los directivos de la Institución actualizan la documentación relacionada con el sistema de Gestión de Seguridad de la Información de manera permanente de acuerdo con las modificaciones aprobadas por el Comité de Desarrollo Institucional.

6 Control de cambios

Fecha del Cambio	Versión	Razón del Cambio	Aprobación
25-05-2022	01	Elaboración primera vez	Sala General - Acuerdo 6 del 25 de mayo de 2022
15-12-2023	02	Actualización de cargos y revisión de directrices.	Sala General – Acuerdo 5 15 de diciembre de 2023

* Nota: Las impresiones de este documento son copias no controladas.

7 Revisión y Aprobación

Revisó Documento	
<i>Firma en Original</i> Dirección de Innovación y Desarrollo Tecnológico	<i>Firma en Original</i> Dirección de Planeación y Aseguramiento de la Calidad

Aprobó Documento	
<i>Firma en Original</i> JOSÉ ALEJANDRO CORTÉS O. Presidente Sala General	<i>Firma en Original</i> MARÍA LUCÍA CASAS PARDO Secretaria Sala General