CONSEJO DIRECTIVO

ACUERDO No. 033

(2 de noviembre de 2023)

POR MEDIO DEL CUAL SE MODIFICA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DE LA CORPORACIÓN UNIFICADA NACIONAL DE EDUCACIÓN SUPEIOR- CUN

El Consejo Directivo de la Corporación Unificada Nacional de Educación Superior – CUN, en uso de sus atribuciones legales y estatutarias, y

CONSIDERANDO:

Que la Corporación Unificada Nacional de Educación Superior es una Institución de Educación Superior privada, sin ánimo de lucro, de utilidad común y con carácter académico Técnica Profesional redefinida para impartir formación profesional por ciclos propedéuticos.

Que la Constitución Política, en su Artículo 69, consagra la autonomía universitaria, permitiendo que las Instituciones de Educación Superior (IES) puedan darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley.

Que la Ley 30 de 1992 en sus artículos 28 y 29 desarrolla los presupuestos de la autonomía universitaria, permitiéndole a las Instituciones de Educación Superior (IES) autorregularse por medio de la expedición de sus propios reglamentos.

Que conforme el artículo 30 literal c del Estatuto Orgánico, es función del Consejo Directivo dirigir el desarrollo de las políticas académicas, administrativas y los objetivos de la corporación.

Que de conformidad con los artículos 15 y 20 de la Constitución Política, los cuales fueron desarrollados mediante la Ley 1581 de 2012, "*Por medio del cual se dictan disposiciones generales para la Protección de Datos Personales*" y el Decreto 1377 de 2013, compilado en el Decreto 1074

de 2015, se estableció la obligación y el deber de los administradores de la información de personas naturales de atender los preceptos asociados a la protección, manejo y suministro de la misma.

Que la Corte Constitucional mediante sentencia C-1011 de 2008 estableció dos modos de clasificación, así: *"la primera, relacionada con el nivel de protección del derecho a la intimidad, que divide los datos entre información personal e impersonal; la segunda divide los datos personales con base en un carácter cualitativo y según el mayor o menor grado en que pueden ser divulgados. Así, se establece la existencia de información pública, semiprivada, privada y reservada."*

Que de acuerdo con lo anterior, cuando el titular de la información personal presta su consentimiento para que estos formen parte de una base de datos de una organización u empresa, pública o privada, ésta se hace responsable del tratamiento de estos datos y adquiere una serie de obligaciones, como son la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Que lo anterior guarda estrecha relación al contenido mínimo que se desprende del derecho al habeas data, acorde a lo descrito por la Corte Constitucional mediante sentencia C-748 de 2011 donde estableció: *"(i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificada o corregida, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien por que se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa."*

Que si bien la responsabilidad del tratamiento de los datos recae en la Corporación, sus competencias se materializan en las funciones que corresponden al personal de la organización responsable del tratamiento de los mismos y que tengan acceso, ya sea directo o indirecto, a las bases que contengan datos personales. Por ello, los colaboradores deben conocer la normativa institucional dispuesta para tal fin, así como los lineamientos institucionales establecidos para tal fin.

Que el Consejo Directivo mediante Acuerdo No. 31 del 21 de diciembre de 2018 aprobó y expidió la política de seguridad de la información personal de la Corporación Unificada Nacional de Educación Superior – CUN.

Que la Vicerrectoría de Servicios Digitales considera que la política de seguridad de la información y de protección de datos personales deben actualizarse acorde a las dinámicas propias de la institución y su deseo de ser un referente tecnológico para el sector educativo. Sustenta su propuesta incorporando normas de calidad internacional ISO 27001:2022 y IEC 13335-12004, para fortalecer la seguridad y protección de la información en nuestra organización en los siguientes aspectos:

- Dispositivos Móviles
- Seguridad de Información Personal
- Uso Aceptable de Activos de Información
- Calificación de la Información
- Manejo y Disposición de Información, Medios y Equipos
- Control de Acceso
- Seguridad Física y de Entorno
- Escritorio y Pantalla Limpia
- Copias de Respaldo
- Gestión de Vulnerabilidades
- Transferencia de Información
- Gestión de Incidentes
- Desarrollo Seguro
- Equipo Desatendido
- Controles Criptográficos
- Teletrabajo

Cada uno de estos ítems contribuye a mantener un entorno seguro y confiable para nuestros activos de información.

Que por lo anteriormente expuesto, el Consejo Directivo de la Corporación encuentra pertinente modificar la política de seguridad de la información personal contenida en el Acuerdo 31 del 21 de

diciembre de 2018 incorporando para ello dos libros, uno dedicado a la seguridad informática y el otro hacia la protección de datos personales.

En mérito de lo expuesto,

ACUERDA

Artículo Primero: Aprobar la modificación de la política de seguridad de la información personal de la Corporación Unificada Nacional de Educación Superior – CUN, la cual, quedará así:

LIBRO I
DE LA SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I
GENERALIDADES

SECCIÓN I
PRESENTACIÓN

Artículo 1. Introducción: La Corporación Unificada Nacional de Educación Superior, en adelante la CUN, determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de esta, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En la presente política se establecen los lineamientos que integran el Sistema de Gestión de Seguridad de la Información SGSI, los cuales deben ser adoptadas por los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la CUN; estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001:2022.

El Sistema de Gestión de Seguridad de la información - SGSI, en el cual, se trata la Seguridad Digital; es para la CUN, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas en la presente política.

Artículo 2. Objetivo: Establecer las políticas que regulan la seguridad de la información en la CUN y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la CUN, bajo el liderazgo de la vicerrectoría de servicios digitales de la CUN.

Artículo 3. Alcance: Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la CUN para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho política. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el comité de seguridad de la información.

Estas políticas como parte de Sistema de Gestión de Seguridad de la Información (SGSI), tienen un alcance en todos los procesos que hacen parte de la CUN, verificándolo y aplicándolo a las sedes.

Artículo 4. Aplicabilidad de las Políticas de Seguridad de la Información: Las políticas del SGSI aplican y son de obligatorio cumplimiento para funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la CUN y en general a todos los usuarios de la información que permitan el cumplimiento de los propósitos generales de la CUN.

SECCIÓN II
TERMINOS Y DEFINICIONES

Artículo 5. Terminología aplicable a las Políticas de Seguridad de la Información: Los términos y definiciones aplicables a la presente política serán las siguientes:

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Activo: En los términos de la norma ISO IEC 13335-12004, se puede concebir como cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la CUN. Se pueden clasificar de la siguiente manera:

-Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la CUN.

-Aplicaciones: Es todo el software que se utiliza para la gestión de la información.

-Personal: Es todo el personal de la CUN, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la CUN.

- Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.

-Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones.

-Instalaciones: Son todos los lugares en los que se alojan los sistemas de información.

-**Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Almacenamiento en la Nube: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

Amenaza: Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Cifrar: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.
Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - **Sistema de Gestión de la Seguridad de la Información**.

Cómputo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Declaración de aplicabilidad (SOA - Statement of Applicability): Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evento: Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la

confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

FTP: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.
Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior.

En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

Keyloggers: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la

ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Punto Único de Contacto (PUC): Entiéndase como mesa de ayuda de acuerdo a las mejores prácticas basadas en ITIL.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha
comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Tratamiento de riesgos: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la CUN, debidamente autorizados para usar equipos, sistemas, aplicativos informáticos disponibles en la red de la CUN y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

CAPÍTULO II
SECCIÓN I
NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Artículo 6. Lineamientos de la Política: La Política de Seguridad de la Información de la Corporación Unificada Nacional – CUN se encuentra encaminada a definir, implementar, revisar y actualizar las políticas de seguridad de la información que se vienen adoptando a nivel nacional e internacional.

Lo anterior se genera al establecer un proceso que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la CUN.

Todos los usuarios de los sistemas de información y telecomunicaciones de la CUN tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en la presente política de Políticas de Seguridad de la Información.

Con la gestión de riesgos de seguridad de la información, se busca mediante la aplicación de las diferentes etapas preservar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, con los controles y la evaluación de su aplicación en el monitoreo trimestral se avalúa la eficacia de su aplicación.

Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información - SGSI, los cuales estarán a cargo de la Oficina de Control Interno.

La CUN debe buscar contar con dispositivos y sistemas de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

Los Jefes de Área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la CUN.

Artículo 7. Norma de estructura organizacional de seguridad de la información: En la CUN en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información - SGSI, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la existencia del Comité de Seguridad de la información.

La vicerrectoría de servicios digitales establecerá y documentará los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la CUN a los funcionarios disponibles en la CUN.

Los roles y responsabilidades de seguridad de la información se encontrarán descritos en la Matriz correspondiente.

Artículo 8. Norma para uso de dispositivos móviles: La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smart phones”, tabletas), entre otros, suministrados por la CUN y personales que hagan uso de los servicios de información de la Entidad.

Cuando se autorice el uso de WhatsApp en los dispositivos suministrados por la CUN, no se permite por esta aplicación, el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Artículo 9. Norma de Seguridad información personal: La CUN implementa acciones para asegurar que los funcionarios, contratistas y demás colaboradores de la Entidad, entiendan sus responsabilidades, como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación a la CUN para el tratamiento de sus datos personales de acuerdo a la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales, lo que se deberá reflejado en las cláusulas de los contratos y en el aplicativo "aspirantes".

Se debe realizar un estudio de seguridad detallado el cual será desarrollado por la persona o empresa que el área de capital social determine para ello.

Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

Se debe asegurar que los funcionarios, contratistas y demás colaboradores de la CUN, adopten sus responsabilidades en relación con las políticas de seguridad de la información de la CUN y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información...

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el proceso disciplinario correspondiente.

Actualmente los usuarios que tienen cuenta de usuario de la entidad, pueden realizar el cambio de su fotografía en el correo electrónico institucional, de tal forma que al realizar la inclusión y/o cambio de fotografía, al ser considerada un dato sensible, "una foto contiene la imagen de una persona, la cual es un dato biométrico", el titular está dando su aprobación, en cuanto al tratamiento de sus datos personales de acuerdo a la Ley Estatutaria 1581 de 2012. El funcionario o contratista debe entregar los activos de información de acuerdo procedimiento de terminación correspondiente.

Artículo 10. Norma uso aceptable activos de información: La CUN es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios de la CUN y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

La CUN es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la CUN (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

La CUN mantiene un inventario actualizado de sus activos de información, quedando bajo la responsabilidad de cada propietario de información y centralizado por el Área de Tecnologías y Sistemas de Información, el cual se publicará en la página web de la Presidencia de la República de Colombia.

Artículo 11. Uso de los activos: La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

A. Uso de estaciones cliente

La CUN establece reglas que permitan orientar que la seguridad es parte integral de los activos de información y mediante la correcta utilización de estaciones por los usuarios finales.

B. Uso de internet

La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando

errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

La vicerrectoría de servicios digitales administrará autorización los cambios solicitados de permisos de navegación a los usuarios de la CUN, previa solicitud del Jefe de cada una de las dependencias**.**

La vicerrectoría de servicios digitales implementara herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.

Los usuarios de los activos de información de la CUN tienen restringido el acceso a redes sociales, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a La vicerrectoría de servicios digitales, para que sea autorizado.

C. Uso de correo electrónico

Definir las pautas generales para asegurar una adecuada protección de la información de la CUN, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Todos los mensajes de correo electrónico son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Entidad.

Dentro de las actividades se debe resaltar el buen uso de la herramienta (correo electrónico), con el fin de evitar malos procedimientos, están los siguientes:
Uso para fines profesionales o académicos: Las cuentas de correo electrónico de la CUN no deben ser, en principio, utilizadas con fines privados, ya que constituyen una herramienta de trabajo.

Uso exclusivo para comunicaciones interpersonales: El correo electrónico es una herramienta para el intercambio de información entre personas, no un medio de difusión masiva e indiscriminada de información.

Está prohibido facilitar el acceso de la cuenta de correo electrónico (e-mail) a otras personas, su cuenta es personal e intransferible.

La información contenida en el correo electrónico hace parte de la confidencialidad de la institución y todos los correos podrán ser monitoreados por parte de la institución, según sea requerido.

Debe estar prohibido utilizar el correo electrónico para cualquier propósito comercial o financiero.

Se debe definir el mantenimiento de las cuentas de correo electrónico activas:
Suspendiendo las cuentas de correo si no son accedidas en un periodo de un año.
Eliminadas si no se lee el correo durante 2 años.

Artículo 12. Norma de calificación de la información: La CUN, consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de calificación establecido por la ley, define reglas de como calificar la información.

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.
- Los usuarios responsables de la información de la CUN, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Valiosa” para la CUN; Independiente del tipo de activo, se deben considerar las siguientes características.

- El activo de información es reconocido como valioso para la CUN.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Forma parte de la identidad de la organización y sin el cual la CUN puede estar en algún nivel de riesgo.
- Las categorías de calificación de la información son: INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA RESERVADA e INFORMACIÓN PÚBLICA CLASIFICADA.

Artículo 13. Norma de manejo disposición de información, medios y equipos: La CUN establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por la CUN, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

Se debe aplicar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez se realiza su devolución.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la vicerrectoría de servicios digitales y será objeto de auditorías de seguridad mediante el módulo de prevención de pérdidas de datos de la entidad.

Se debe implementar el procedimiento para la transferencia de medios físicos.

Artículo 14. Norma de control de acceso: La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de la CUN, considerándolas como importantes para el SGSI.

Todo aplicativo informático o software debe ser comprado o aprobado por la vicerrectoría de servicios digitales.

El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.

El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.

A. Establecimiento, uso y protección de claves de acceso

Ningún usuario deberá acceder a la red o a los servicios de la CUN, utilizando una cuenta de usuario o clave de otro usuario.

Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó la clave.

La CUN suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato.

Las claves o contraseñas deben:

Tener mínimo ocho (8) caracteres alfanuméricos.

Cada vez que se cambien estas deben ser distintas por lo menos de las últimas doce anteriores. La contraseña debe cumplir con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: ¡,$, %, &)

B. Manejo de contraseñas para administradores de tecnología

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal del Área de Tecnologías y Sistemas de la Información no debe dar a conocer su clave de usuario a terceros de los sistemas de información.

Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnologías y Sistemas de la Información son de uso personal e intransferible.

Los Administradores de los sistemas de Información y el personal del Área de Tecnologías y Sistemas de la Información deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado, en lo posible con doble factor de autenticación.

Artículo 15. Norma de Seguridad Física y de Entorno: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

A. Seguridad de los equipos

Asegurar la protección de la información en los equipos.

En el caso que se requiera realizar el retiro de activos de información de las sedes de la Entidad, ya sean documentos, equipos tecnológicos que contengan información, se debe realizar el registro correspondiente**.**

Artículo 16. Norma de escritorio y pantalla limpia: Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la CUN debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de la CUN deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de la CUN deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Artículo 17. Norma Copias de respaldo: Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos.

Los administradores de la plataforma de backup de la CUN, verificarán la correcta ejecución de los procesos de backup.

Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Los administradores de la plataforma de copias de respaldo (backup) de la entidad, deben generar tareas de restauración aleatorias de la información, quedando registradas en el formato correspondiente, con el fin de garantizar la continuidad de las actividades realizadas en la Entidad, usando las herramientas tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos.

A. Realización de copias en estaciones de trabajo de usuario final

Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Talento Humano, el Área de Tecnologías y Sistemas de Información generará una copia de la información contenida en el equipo asignado al perfil del usuario (C:\usuarios\nombre-usuario), a una unidad de almacenamiento.

Artículo 18. Norma de gestión de vulnerabilidades: Evitar la utilización de vulnerabilidades técnicas de los sistemas de información y comunicaciones de la CUN, e implementar los lineamientos para gestión de vulnerabilidades.

Artículo 19. Norma para la transferencia de información: Proteger la información transferida al interior y exterior de la CUN.

El área de Tecnología y Sistemas de la Información realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

Artículo 20. Norma de gestión de los incidentes de la seguridad de la información: Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

Artículo 21. Norma de desarrollo seguro: Establecer lineamientos y mejores prácticas para asegurar que el proceso de desarrollo de software se realice de manera segura y confiable. Su fin es proteger la integridad, confidencialidad y disponibilidad de la información, mitigando riesgos y vulnerabilidades desde las etapas iniciales del desarrollo hasta la implementación final. Se busca garantizar la creación de aplicaciones y sistemas robustos, resistentes a ataques cibernéticos, cumpliendo con estándares de seguridad, asegurando la confidencialidad de los datos y manteniendo la confianza de los usuarios y clientes en la protección de su información personal y sensible.

Artículo 22. Norma de equipo desatendido: Garantizar la seguridad y protección de los equipos que permanecen sin supervisión durante periodos prolongados. Su fin es establecer directrices y medidas de seguridad para mitigar los riesgos asociados a estos equipos, como accesos no autorizados, robo de información o daños físicos. Se busca asegurar que los equipos desatendidos

cuenten con medidas de seguridad adecuadas, como bloqueo automático de sesiones, actualizaciones de software, respaldos regulares y monitoreo remoto, con el objetivo de prevenir incidentes y salvaguardar la integridad y confidencialidad de los datos almacenados en dichos equipos.

Artículo 23. Norma de controles criptográficos: Proteger la confidencialidad, integridad y autenticidad de la información sensible a través del uso de técnicas criptográficas. Establecer lineamientos y procedimientos para la correcta implementación y gestión de mecanismos criptográficos, como el cifrado y la firma digital. Su propósito es asegurar que la información se encuentre protegida contra accesos no autorizados, modificaciones no autorizadas y falsificaciones, garantizando así la seguridad de la información tanto en tránsito como en reposo. Además, la norma busca promover buenas prácticas criptográficas y el cumplimiento de estándares y normativas de seguridad aplicables.

Artículo 24. Norma de seguridad en el teletrabajo: Garantizar la protección de la información y los recursos de la organización mientras los empleados trabajan de forma remota. Establecer las medidas de seguridad necesarias para prevenir y mitigar los riesgos asociados al teletrabajo, como la pérdida, el acceso no autorizado o la divulgación de información confidencial. Además, se pretende promover buenas prácticas de seguridad, concienciar a los empleados sobre los riesgos y responsabilidades en el manejo de la información y asegurar la continuidad de las operaciones de la organización, manteniendo un ambiente de trabajo seguro y protegido incluso fuera de las instalaciones físicas.

SECCIÓN IV
PROCEDIMIENTOS

Artículo 25. Procedimiento de acción correctiva: El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de la CUN, así como: definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTC-IS0: 9001 y NTC-IS0: 27001 se utiliza el procedimiento de elaboración y seguimiento de planes de mejoramiento.

Artículo 26. Procedimiento de acción preventiva: El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real en el sistema de gestión de seguridad de la información y eliminar sus causas.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTC-ISO: 9001 y NTC-ISO: 27001 se utiliza el procedimiento de elaboración y seguimiento de planes de mejoramiento. Proceso de evaluación, control y mejoramiento**.**

CAPÍTULO III
SECCIÓN I
PROCEDIMIENTO DISCIPLINARIO

Artículo 27. Proceso Disciplinario: Dentro de la estrategia de seguridad de la información de la CUN, debe estar establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores de la CUN violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por el la CUN:

- No mantener la confidencialidad de las contraseñas, o permitir que otras personas accedan con el usuario y clave del titular.
- Permitir el acceso u otorgar privilegios a personas no autorizadas.
- Realizar actividades tales como borrar, alterar o eliminar información de manera malintencionada.
- Sustraer de las instalaciones de la CUN, documentos de archivo sin la debida autorización.

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Calificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral.
- No guardar la información digital, producto del procesamiento de la información perteneciente a la CUN.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada y/o información pública clasificada, por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de Tecnologías y Sistemas de Información de la CUN.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización de Área de Tecnologías y Sistemas de Información de la CUN.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la CUN.
- No cumplir con las actividades designadas para la protección de los activos de información de la CUN.

- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de la CUN.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de la CUN, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la CUN.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la CUN.
- El que viole datos personales de las bases de datos de la CUN.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por el la CUN.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la CUN o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la CUN a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de la CUN o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por la CUN.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la CUN, para traslado, reasignación o para disposición final.
- Realizar cambios no autorizados en la plataforma tecnológica de la CUN.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de Tecnologías y Sistemas de Información de la CUN.

Cualquiera de las actividades descritas anteriormente será investigada y, tanto su procedimiento como sanción correspondiente se generará acorde a lo descrito en el Reglamento Interno de Trabajo vigente al momento de la comisión de los hechos que generaron el procedimiento.

LIBRO II
POLÍTICA DE MANEJO, TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

DISPOSICIONES GENERALES

Artículo 1. Objeto: Esta política tiene como objeto establecer el marco normativo de aplicación que establezca la protección de los datos personales suministrados a la Corporación Unificada Nacional de Educación Superior-CUN, conforme lo establecido en la ley o las normas que lo modifiquen, adicionen o deroguen.

Parágrafo 1. Serán objeto de protección con base en la presente política, aquellas personas que, en ejercicio de cualquier actividad, incluyendo las académicas, laborales y comerciales, sean estas permanentes u ocasionales, puedan suministrar cualquier tipo de información o dato personal a la Corporación quien actúa en calidad de responsable del tratamiento de datos personales, y quien deberá permitir al titular de la información, conocerla, actualizarla.

Parágrafo 2. Su finalidad será la de establecer lineamientos y medidas necesarias para garantizar la adecuada recolección, almacenamiento, uso, divulgación y eliminación de los datos personales asegurando el cumplimiento de las leyes y regulaciones de protección de datos, así como el fomentar buenas prácticas en el tratamiento de la información personal. De igual manera, busca proteger los derechos y libertades de los individuos, promoviendo la transparencia y la confianza en el manejo de sus datos personales por parte de la organización.

Artículo 2. Marco legal: La Corporación Unificada Nacional de Educación Superior - CUN, cumple con la regulación y la normativa que establece el Estado Colombiano en materia de Protección de datos personales:

a) Ley 1266 de 2008, en la que se dictan las disposiciones generales de habeas data y se regula el manejo de la información contenida en las bases de datos personales, en especial la financiera,

crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

b) Ley Estatutaria 1581 de 2012, hoy Decreto 1074 de 2015 y demás decretos reglamentarios que definan el ámbito de aplicación en los derechos a la intimidad, el buen nombre y la autodeterminación informativa.

c) Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

d) Decreto 103 de 2015 por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

e) Sentencia C- 1011 de 2008 - Definición de la naturaleza del dato asentado en los Registros Públicos de las Cámaras de Comercio, como dato público.

f) Sentencia C - 748 de 2011 - Constitucionalidad del proyecto de Ley Estatutaria de Protección de Datos Personales.

g) Las instrucciones impartidas por la Superintendencia de Industria y Comercio en ejercicio de la función establecida en el artículo 21 de la Ley 1581 de 2012.

Artículo 3. **Conceptos y definiciones:** Para efectos de la presente política se entiende por:

a) **Acceso Restringido:** Nivel de acceso a la información limitado a parámetros previamente definidos. La Corporación Unificada Nacional de Educación Superior CUN no hará disponibles Datos Personales para su acceso a través de Internet u otros medios de comunicación masiva, a menos que se establezcan medidas técnicas que permitan controlar el acceso y restringirlo solo a las personas Autorizadas.

b) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

c) **Aviso de privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al titular pare el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretender dar los datos personales.

d) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.

e) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

f) **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

g) **Datos Semiprivado:** Es aquella información que no es de naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como es el caso de los datos financieros, crediticios o actividades comerciales.

h) **Datos sensibles:** Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelan el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

i) **Derecho de los niños, niñas y adolescentes:** En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Sólo podrán tratarse aquellos datos que sean de naturaleza pública.

j) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del

Tratamiento. La Corporación Unificada Nacional de Educación Superior CUN, actúa como encargado del tratamiento de datos personales en los casos, en los que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta de un responsable del tratamiento.

k) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

l) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

m) **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.

Artículo 4. Principios rectores: Los principios rectores de la presente política son:

a) **Principio de legalidad en materia de tratamiento de datos:** El tratamiento a que se refiere la presente es una actividad reglada, que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

b) **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legitima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular.

c) **Principio de libertad:** El tratamiento solo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

d) **Principio de veracidad o calidad:** la información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

e) **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernen.

f) Principio e acceso y circulación restringida: El tratamiento se sujeta a los límites que se deriven de la naturaleza de los datos personales. En este sentido. el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente política.

g) Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que la presente política, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

h) Principio de confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente y en los términos de la misma.

Artículo 5. Derecho de los titulares: El titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento este expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento.

c) Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que les han dado a sus datos personales.

d) Revocar la autorización y/o solicitar la supresión de la data cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.

e) Acceder en forma gratuita a sus datos personales que hayan sido objetos de tratamiento.

Artículo 6. Derechos de los Niños, Niñas y Adolescentes: El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y/o requisitos:

- Que respondan y respeten el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Artículo 7. Deberes del responsable del tratamiento: Cuando la Corporación actúe como responsable del tratamiento de la información, cumplirá con los siguientes deberes:

a) Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data.

b) Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

c) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, perdida, consulta, uso o acceso no autorizado o fraudulento.

d) Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.

e) Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.

f) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

g) Suministrar al encargado del tratamiento, según el caso únicamente datos cuyo tratamiento este previamente autorizado de conformidad con lo previsto en la presente política.

h) Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

i) Tramitar las consultas y reclamos formulados en los términos señalados en la presente política.

j) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

k) La Corporación se reserva, en los eventos contemplados en la ley y en sus estatutos y reglamentos internos, la facultad de mantener y catalogar determinada información que repose en sus bases o bancos de datos, como confidencial de acuerdo con las normas vigentes, sus estatutos y reglamentos, todo lo anterior y en consonancia con el derecho fundamental y constitucional a la educación, a la libre catedra y principalmente, de la autonomía universitaria.

Artículo 8. Autorización del titular: El responsable del tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización previa, expresa e informada del titular pare el tratamiento de los mismos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del tratamiento para las cuales se obtiene el consentimiento. La recolección de datos deberá limitarse a aquellos datos personales que sean pertinentes y adecuados para la finalidad para la cual son recolectados y deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior por parte del titular.

Artículo 9. Legitimación para el ejercicio de los derechos del titular: Se ejercerán por las siguientes personas.

a) Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.

b) Por los causahabientes del Titular (en los casos que este falte por muerte o incapacidad), quienes deberán acreditar tal calidad.

c) Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.

d) Por estipulación a favor de otro o para otro.

e) Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Artículo 10. Personas a quienes se les puede suministrar la información: La información que reúna las condiciones establecidas en la presente política podrá suministrarse a las siguientes personas:

a) A los titulares, sus causahabientes o sus representantes legales.

b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.

c) A los terceros autorizados por el titular o por la ley.

Artículo 11. Modo de otorgar la autorización: La autorización del Titular puede darse por escrito, de forma oral o mediante conductas inequívocas de este, que permitan concluir de forma razonable que otorgue la autorización. La autorización puede constar en un documento físico, electrónico (mensaje de datos, Internet, sitios web), o en cualquier otro formato que permita garantizar su posterior consulta. Asimismo, podrá otorgarse mediante un mecanismo técnico e tecnológico idóneo, que permita manifestar su consentimiento de manera electrónica, para concluir de manera inequívoca, que, de no haberse surtido una conducta del titular, los datos nunca hubieren sido capturados y almacenados en la base de datos.

Artículo 12. Prueba de la autorización: La Corporación dispondrá de los medios tecnológicos o físicos, e implementara y adoptara las acciones tendientes y necesarias para mantener registros o mecanismos técnicos o tecnológicos idóneos, que permitan demostrar cuando y como se obtuvo la autorización por parte de los titulares. Para dar cumplimiento a lo anterior, se podrán establecer archivos físicos o repositorios electrónicos realizados de manera directa o a través de terceros contratados para tal fin.

Parágrafo 1: Aviso de privacidad: El Aviso de Privacidad es la comunicación verbal o escrita generada por el Responsable del Tratamiento, dirigida al Titular a través de un medio físico, electrónico en cualquier otro formato conocido o por conocer, que es puesto a disposición de este para el tratamiento de sus datos personales. A través de este documento se informa al Titular, la información relativa a la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las características del Tratamiento que se pretende dar a los datos personales, como mínimo al momento de efectuar la recolección de los datos personales.

CAPITULO SEGUNDO
MANEJO Y TRATAMIENTO DE LA INFOMACIÓN

Artículo 13. Revocatoria de autorización: Los titulares de los datos personales pueden revocar el consentimiento al tratamiento de sus datos personales en cualquier momento, siempre y cuando no lo impida una disposición legal o fuera improcedente en virtud de relación contractual sea cual fuere su naturaleza (académica, laboral, civil o comercial). Para ello, deberá radicar solicitud escrita ante la Instancia del CIGE (Centro integral de atención al estudiante), por medio de la cual solicite de manera expresa revocar dicha autorización.

Artículo 14. Transferencia de la información: En aquellos casos sujetos a los requerimientos legales aplicables, se haga necesario la transferencia de la información a terceros, la Corporación velara porque está siempre sea conforme lo establecido en la presente política. En razón a ello, la Corporación tomará las medidas necesarias para que los terceros receptores de la información conozcan y se comprometan a cumplir esta política, bajo el entendido que la información personal

que reciban, únicamente podrá ser utilizada para asuntos directamente relacionados con la Corporación y no podrá ser destinada para propósito o fin diferente.

Artículo 15. Tratamiento de la información: Los datos recogidos, administrados y procesados por la Corporación en sus bases de datos, será utilizada únicamente en desarrollo de su objeto social y en ejercicio de sus relaciones académicas, contractuales y convencionales.

Artículo 16. Responsable del procedimiento de reclamos y consulta: La Corporación designa al CIGE (Centro integral de gestión al Estudiante), como el área encargada que recibirá, procesará y canalizará las distintas solicitudes y tramites asociados con tratamiento de información personal.

Artículo 17. Consultas: Los titulares y/o sus autorizados podrán consultar la información personal del titular que repose en cualquier base de datos de la Corporación. El responsable del tratamiento o encargado del tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

Las consultas dirigidas a la Corporación Unificada Nacional de Educación Superior - CUN deberán contener como mínimo la siguiente información:

a) Nombres y apellidos del Titular y/o su representante y/o causahabientes;
b) Lo que se pretende consultar.
c) Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
d) Firma, número de identificación o procedimiento de validación correspondiente.
e) Haber sido presentada por los medios de consulta habilitados por la Corporación Unificada Nacional de Educación Superior CUN.

Artículo 18. Procedimiento de las consultas: Una vez radicada la solicitud ante la instancia del CIGE (Centro integral de gestión al estudiante), la misma será atendida en un término máximo de quince (15) días hábiles contados a partir de la fecha de recibo de esta. Cuando no fuere posible atender la consulta dentro de dicho termino, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (05) días hábiles siguientes al vencimiento del primer término.

Artículo 19. Reclamos: El titular y/o sus autorizados que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta política, podrán presentar un reclamo ante el CIGE (Centro integral de gestión al estudiante), bajo el siguiente procedimiento:

Las reclamaciones dirigidas a la Corporación Unificada Nacional de Educación Superior CUN deberán contener como mínimo la siguiente información:

a) Nombres y apellidos del Titular y/o su representante y/o causahabientes;
b) Lo que se pretende consultar.
c) Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
d) Firma, número de identificación o procedimiento de validación correspondiente.
e) Haber sido presentada por los medios de consulta habilitados por la Corporación Unificada Nacional de Educación Superior CUN.

Parágrafo 1. El reclamo se formulará mediante solicitud dirigida en la instancia del CIGE (Centro integral de gestión al estudiante), por medio de un escrito formal. donde se exprese de manera puntual el objeto de la solitud, con identificación del titular, la descripci6n de los hechos que dan lugar al reclamo, la dirección y acompañando los documentos que se quiera hacer valer. Si presentado el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (05) días siguientes a la recepci6n del reclamo para que subsane las fallas. Si transcurrido un (01) mes desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

parágrafo 2. El termino máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo siempre y cuando se cumpla a cabalidad con la totalidad de los requisitos previstos en esta política. Cuando no fuere posible atender el reclamo dentro de dicho termino, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los (08) ocho días hábiles siguientes al vencimiento del primer término.

Artículo 20. Registro Bases de Datos: Dando cumplimiento al Artículo 25 de la Ley 1581 de 2012. La Corporación Unificada Nacional de Educación Superior CUN, registrara sus bases de datos junto con la presente política de tratamiento y protección de datos personales, en el Registro Nacional de bases de datos, administrado por la Superintendencia de industria y comercio, de conformidad con el procedimiento establecido para tal efecto.

parágrafo 1. Todas las bases de datos de propiedad de la Corporación Unificada Nacional de Educación Superior CUN tendrán el periodo y vigencia correspondiente con la finalidad para el cual se autorizó su tratamiento y de las normas especiales que regulen la materia, así aquellas que establezcan el ejercicio de las funciones legales asignadas a la Entidad.

Artículo 21. Sensibilización a funcionarios y colaboradores: La Corporación Unificada Nacional de Educación Superior CUN, apoyada desde el equipo de Seguridad de la Información, desarrollara programas tendientes a la capacitación, sensibilización y apropiación en protección de datos personales, lo anterior con el fin de dar a conocer esta política, con una periodicidad anual.

Desde la Vicerrectoría de Capital Social, se deberá asegurar que los funcionarios, contratistas y terceros conozcan su responsabilidad con respecto a la protección de datos personales; Se debe establecer los planes de capacitación y evaluación de los empleados, teniendo en cuenta los cambios normativos que se vayan actualizando, con el fin de que los planes sean actualizados de manera periódica.

Teniendo en cuenta los cambios de personal al interior de la institución, se debe impartir una capacitación inicial de apropiación sobre esta política, dejando evidencia de su participación y apropiación del conocimiento.

Artículo Segundo: Apruébese la autorización para el tratamiento de datos personales en página web y/o plataformas tecnológicas de la Corporación Unificada Nacional de Educación Superior – CUN, dispuesta en el Anexo 001 del presente Acuerdo.

Artículo Tercero: Expídase copia del presente acuerdo a la Rectoría, las Vicerrectorías, Direcciones y la Secretaría General para efectos de socialización institucional a todo el personal de la Corporación.

Artículo Cuarto: El presente acuerdo rige desde su expedición y deroga todas las disposiciones en contra, especialmente el Acuerdo 31 del 21 de diciembre de 2018, acorde a los artículos que anteceden.

COMUNÍQUESE Y CÚMPLASE.

Dado en Bogotá D.C. a los dos (2) días del mes de noviembre de dos mil veintitrés (2023).

JAIME ALBERTO RINCON PRADO
Rector
En su calidad de Presidente del
Consejo Directivo

SANDRA BIBIANA CASTILLO CASTILLO
Secretaria General

Aprobaciones		
Nombre	**Área**	**Firma**
Diego Sierra	Vicerrectoría de Servicios Digitales	Diego Sierra
Aura Margarita Salcedo	Secretaría General	As
Jorge Enrique Murcia	Vicerrectoría Ejecutiva	