



RECTORÍA

Documento Manual de Seguridad y Privacidad - MSPI

Universidad de Caldas
Abril de 2025



**Tejiendo
Universidad**

Autoevaluación Institucional 2018 - 2026

TABLA DE CONTENIDO

Tabla de contenido

1.	OBJETIVO.....	3
2.	OBJETIVO DEL MANUAL.....	3
3.	ALCANCE DEL MANUAL	3
4.	DEFINICIONES.....	3
4.	POLÍTICAS.....	8
	POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS.....	8
	POLÍTICAS DE GESTIÓN DE ACTIVOS	8
	POLÍTICAS DE CONTROL DE ACCESO LÓGICO	8
	CRIPTOGRAFÍA	9
	POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO	9
	POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES.....	9
	POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES	9
	POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	9
	POLÍTICAS DE RELACIONES CON LOS PROVEEDORES	10
	SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO	10
	POLÍTICAS DE GESTIÓN DE INCIDENTES	10
	POLÍTICAS DE CUMPLIMIENTO	10
	ESCRITORIO LIMPIO.....	10
	USO ADECUADO DE INTERNET	11
	ADOPCIÓN DEL PROTOCOLO IPV6.....	11
	USO ADECUADO DE CORREO ELECTRÓNICO:	11
	USO DE USUARIOS Y CONTRASEÑAS:	13
5.	SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN.....	13
	SENSIBILIZACIÓN Y COMUNICACIÓN	13
	CAPACITACIONES EN SEGURIDAD.....	14
6.	APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS	14
7.	SANCIONES.....	14



1. OBJETIVO

La información es uno de los activos más valiosos de toda entidad, por lo que debe ser protegida en todo momento, independientemente de cómo sea producida, manipulada, divulgada o almacenada.

Para la Universidad de Caldas, la preservación de la confidencialidad, integridad y disponibilidad de la información es una prioridad. Por tanto, es responsabilidad de todos garantizar que no se realicen actividades que contradigan la esencia y el espíritu de estas políticas.

Las políticas de seguridad de la información contenidas en este manual son una parte fundamental del Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL). Estas políticas constituyen la base para la implementación de controles, procedimientos y estándares definidos.

El desarrollo del manual se basa en el Modelo de Seguridad y Privacidad de la Información presentado por el Ministerio de Tecnologías de la Información y las Comunicaciones, que recopila las mejores prácticas para proporcionar requisitos para el diagnóstico, planificación, implementación, gestión y mejora continua; teniendo en cuenta las necesidades y objetivos, los requisitos de seguridad, los procesos misionales, así como el tamaño y estructura de la Universidad de Caldas.

El modelo a seguir se fundamenta en las Normas Técnicas NTC ISO/IEC 27000 e ISO/ICONTEC, la legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otros. Está alineado con el Marco de Referencia de Arquitectura TI y apoya transversalmente los demás componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

2. OBJETIVO DEL MANUAL

El objetivo es establecer lineamientos de seguridad de la información como complemento de la “**Política General de Seguridad de la Información de la Entidad**”, para preservar la confidencialidad, integridad y disponibilidad de los activos de **La Universidad de Caldas**.

3. ALCANCE DEL MANUAL

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes de **UNIVERSIDAD DE CALDAS** por alguna razón tengan cualquier tipo de interacción con los activos de información.

4. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder

a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de Información:** cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Universidad de Caldas y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Amenaza:** es la posibilidad de cualquier evento o acción que pueda causar daño (material o inmaterial) a los elementos de un sistema, en el contexto de la Seguridad Informática, a los elementos de información. Se refiere a una posible causa de un incidente no deseado que pueda dañar un sistema o una organización. (ISO/IEC 27000).
- **Análisis de riesgos de seguridad de la información:** proceso sistemático de identificar fuentes, estimar impactos y probabilidades, y comparar estas variables contra criterios de evaluación para determinar las consecuencias potenciales relacionadas con la confidencialidad, integridad y disponibilidad de la información.
- **Archivo:** Conjunto de documentos, sin importar su fecha, forma o soporte material, acumulados de manera natural por una persona o entidad pública o privada durante su gestión, conservados respetando su orden original para servir como testimonio e información tanto a la persona o institución que los produce como a los ciudadanos, o como fuentes históricas. También se refiere a la institución encargada de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y determinar el grado en que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autenticación:** Procedimiento para verificar la identidad de un usuario o recurso tecnológico al intentar acceder a un recurso de procesamiento o sistema de información.
- **Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales (Ley 1581 de 2012, art 3). MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI
- **Bases de Datos Personales:** es un conjunto organizado de datos personales que se recopilan, almacenan y gestionan para su uso en diversas actividades. Estos datos pueden incluir información vinculada o asociada a una o varias personas naturales determinadas o determinables, como nombres, direcciones, números de identificación, entre otros.
- **Ciberseguridad:** Capacidad para minimizar el riesgo al que están expuestos los ciudadanos ante amenazas o incidentes cibernéticos. (CONPES 3701).



- **Ciberespacio:** Ambiente físico y virtual compuesto por computadores, sistemas computacionales, programas (software), redes de telecomunicaciones, datos e información utilizada para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Confidencialidad:** Garantía de que la información no está disponible ni es divulgada a personas, entidades o procesos no autorizados.
- **Control:** Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también se usa como sinónimo de salvaguarda o contramedida. En términos simples, es una medida que modifica el riesgo.
- **Datos Abiertos:** Datos primarios o sin procesar en formatos estándar e interoperables que facilitan su acceso y reutilización. Estos datos, bajo custodia de entidades públicas o privadas con funciones públicas, se ponen a disposición de cualquier ciudadano de forma libre y sin restricciones, permitiendo la reutilización y creación de servicios derivados (Ley 1712 de 2014, art 6).
- **Datos Personales:** Información vinculada o asociada a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Datos que no son semiprivados, privados o sensibles. Incluyen, entre otros, datos relativos al estado civil, profesión u oficio, y calidad de comerciante o servidor público. Por su naturaleza, pueden estar contenidos en registros públicos, documentos públicos, gacetas y boletines oficiales, y sentencias judiciales ejecutoriadas que no estén sujetas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Datos de naturaleza íntima o reservada solo relevantes para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos:** Información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, como origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos u organizaciones sociales, derechos humanos, intereses políticos, salud, vida sexual, y datos biométricos. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, tras el resultado de los procesos de evaluación y tratamiento de riesgos, y su justificación, así como la justificación de exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** es un derecho fundamental que protege la vida privada y personal de los individuos, garantizando que su información personal no sea divulgada sin su consentimiento. Este derecho asegura que las personas puedan mantener su privacidad y que su información íntima no sea expuesta o utilizada de manera indebida.
- **Disponibilidad:** Garantía de que los usuarios autorizados tienen acceso a la información y activos asociados cuando lo requieran.



- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del responsable del tratamiento. (Ley 1581 de 2012, art 3).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Información en poder o custodia de un sujeto obligado, perteneciente al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, cuyo acceso puede ser negado o exceptuado bajo circunstancias legítimas y necesarias según lo consagrado en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada:** Información en poder o custodia de un sujeto obligado, exceptuada de acceso ciudadano por daño a intereses públicos y bajo cumplimiento de requisitos del artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Integridad:** Protección de la exactitud y estado completo de los activos de información.
- **Ley de Habeas Data:** la Ley de Habeas Data en Colombia se refiere a la Ley Estatutaria 1266 de 2008. Esta ley regula el manejo de la información personal contenida en bases de datos y archivos, tanto en el sector público como en el privado. Su objetivo principal es proteger los derechos de los ciudadanos en relación con el tratamiento de sus datos personales, garantizando la privacidad, la seguridad y la confidencialidad de la información. La ley establece principios y procedimientos para la recolección, almacenamiento, uso y circulación de datos personales, y otorga a los individuos el derecho a conocer, actualizar y rectificar la información que sobre ellos se haya recogido en bases de datos.
- **Ley de Transparencia y Acceso a la Información Pública:** se refiere a la Ley Estatutaria 1712 de 2014. Esta ley establece el derecho fundamental de todas las personas a conocer y acceder a la información pública que esté en posesión o bajo control de sujetos obligados. Su objetivo principal es promover la transparencia y la rendición de cuentas en la gestión pública, garantizando que la información pública sea accesible, clara y oportuna. La ley también define los principios y procedimientos para la clasificación, reserva y divulgación de la información pública, asegurando que solo se exceptúe el acceso a la información bajo circunstancias legítimas y necesarias.
- **Mecanismos de protección de datos personales:** Alternativas disponibles para entidades destinatarias para proteger los datos personales de los titulares, tales como acceso controlado, anonimización o cifrado.
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar, ser afectada o percibirse como afectada por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las funciones misionales o del negocio en caso de evento imprevisto que las ponga en peligro. (ISO/IEC 27000).



- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar riesgos de seguridad de la información inaceptables e implementar los controles necesarios para protegerla. (ISO/IEC 27000).
- **Privacidad:** se refiere al derecho de los individuos a controlar la recopilación, uso y divulgación de su información personal en este contexto. Este concepto abarca la protección de datos personales contra el acceso no autorizado y el uso indebido, garantizando que la información sensible se maneje de manera confidencial y segura.
- **Propietarios de los activos de información:** Responsables de cada activo de información (archivos, bases de datos, contratos, documentación, manuales, aplicaciones, software, equipos, servicios informáticos y de comunicaciones, personas, etc.), encargados de mantener su seguridad.
- **Recursos tecnológicos:** Componentes de hardware y software como servidores, estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y seguridad, servicios de red de datos y bases de datos, entre otros, que apoyan las tareas administrativas necesarias para el buen funcionamiento y optimización del trabajo.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a tratamiento que operan en el país. (Ley 1581 de 2012, art 25).
- **Responsabilidad Demostrada:** Conducta de responsables o encargados del tratamiento de datos personales, quienes deben demostrar a la Superintendencia de Industria y Comercio que han implementado medidas apropiadas y efectivas para cumplir con la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza explote una vulnerabilidad causando pérdida o daño en un activo de información, combinando probabilidad de evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y objetivos de seguridad de la información y alcanzarlos, basado en gestión y mejora continua. (ISO/IEC 27000).
- **Sistema de información:** Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados para su uso posterior, generados para cubrir una necesidad u objetivo. Elementos pueden ser personas, actividades o técnicas de trabajo, datos y recursos materiales en general.
- **Titulares de la información:** Personas naturales cuyos datos personales son objeto de tratamiento. (Ley 1581 de 2012, art 3).



- **Tratamiento de Datos Personales:** según la ley colombiana se refiere a cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión de dichos datos.
- **Trazabilidad:** Calidad que permite asociar todas las acciones realizadas sobre la información o sistema de tratamiento de la información de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. POLÍTICAS

La Universidad de Caldas establece los siguientes lineamientos de seguridad de la información, que deben ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad se clasifican en diferentes temáticas, según el contexto interno y externo de la entidad:

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información generada, almacenada o transformada por funcionarios, contratistas o proveedores usando los recursos de la entidad es propiedad de la Universidad de Caldas.
- Los activos proporcionados por la Universidad de Caldas solo se usarán para tareas laborales de la institución.
- La Universidad de Caldas identificará, clasificará y gestionará su inventario de activos según los manuales y procedimientos formalizados de Gestión de Activos.

POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

CRIPTOGRAFÍA

- La Universidad de Caldas implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el Grupo/Oficina de Tecnológica de Información y las Comunicaciones determinará los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- La Universidad de Caldas adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- La Universidad de Caldas definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de la Universidad de Caldas deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. La Universidad de Caldas planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- El Grupo de Tecnológica de la Información y las Comunicaciones, establecerá los controles para acceso lógico y protección de las redes de la Universidad de Caldas, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
- La Universidad de Caldas definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- La Oficina Asesora de Planeación y Sistemas, velará que los sistemas de información que sean implementados en la Universidad de Caldas cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimientos y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la Universidad de Caldas deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con

el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

- La Universidad de Caldas establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- La Universidad de Caldas establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
- La Oficina Asesora de Planeación y Sistemas generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

POLÍTICAS DE GESTIÓN DE INCIDENTES

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar a La Oficina Asesora de Planeación y Sistemas por cualquiera de los medios dispuestos para tal fin.
- Será responsabilidad de La Oficina Asesora de Planeación y Sistemas seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

POLÍTICAS DE CUMPLIMIENTO

- La Universidad de Caldas velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

ESCRITORIO LIMPIO

- No deberán dejarse documentos críticos en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).
- Cada vez que los funcionarios se retiren del lugar de trabajo deben bloquear los equipos de cómputo.
- Emplear las cajoneras o archivos para el almacenamiento de la información sensible o crítica.

USO ADECUADO DE INTERNET

- El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.
- Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- La Oficina Asesora de Planeación y Sistemas podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

ADOPCIÓN DEL PROTOCOLO IPV6

La Universidad de Caldas deberá adoptar el protocolo IPV6, a través de la Oficina Asesora de Planeación y Sistemas considerando las siguientes políticas para una adopción efectiva:

- **Planificación y Evaluación:** Realizar una evaluación exhaustiva de la infraestructura actual para identificar las necesidades y los cambios necesarios para la adopción de IPv6.
- **Capacitación y Sensibilización:** Capacitar al personal técnico y a los usuarios sobre las diferencias y beneficios de IPv6 en comparación con IPv4.
- **Actualización de Equipos y Software:** Asegurarse de que todos los equipos de red y software sean compatibles con IPv6. Aquellos que permitan mantener en dualidad ambos protocolos, se debe activar esta capacidad para afrontar la etapa de transición.
- **Seguridad:** Implementar medidas de seguridad específicas para IPv4 - IPv6, como la configuración de firewalls y la protección contra amenazas específicas de IPv4 - IPv6.
- **Pruebas y Pilotos:** Realizar pruebas piloto en segmentos controlados de la red antes de una implementación completa.
- **Monitoreo y Gestión:** Establecer sistemas de monitoreo y gestión para supervisar el rendimiento y la seguridad de la red IPv4 - IPv6.
- **Documentación y Políticas:** Documentar todos los procedimientos y políticas relacionadas con la adopción de IPv6 para asegurar una transición ordenada y coherente.

USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a la Universidad de Caldas, por lo tanto, su contenido también es propiedad de la Entidad.
- La Oficina Asesora de Planeación y Sistemas podrá verificar el contenido de los buzones de los correos electrónicos en los casos que se requiera acudir a

información para continuar con la prestación del servicio o para investigaciones específicas (previa solicitud por parte de la Secretaría General o requerimiento de autoridad judicial).

- **Uso apropiado del correo electrónico:**
 - Uso profesional: El correo electrónico corporativo debe utilizarse exclusivamente para comunicaciones relacionadas con el trabajo.
 - Prohibición de uso personal: Evitar el uso del correo electrónico de la empresa para asuntos personales.
 - Contenido prohibido: No distribuir material ofensivo, discriminatorio, obsceno o ilegal.
 - Cadenas y spam: Está prohibido el envío de mensajes en cadena o correos no solicitados.
- **Seguridad y confidencialidad:**
 - Contraseñas: Establecer contraseñas seguras y cambiarlas periódicamente (recomendado cada 90 días).
 - Información confidencial: No compartir información sensible sin autorización previa.
 - Verificación de destinatarios: Revisar cuidadosamente la lista de destinatarios antes de enviar correos.
 - Phishing: No abrir archivos adjuntos ni hacer clic en enlaces de remitentes desconocidos.
 - Dispositivos móviles: Proteger los dispositivos móviles que acceden al correo corporativo con contraseñas y bloqueo automático.
- **Formato y estilo:**
 - Línea de asunto: Usar líneas de asunto claras y específicas que reflejen el contenido del mensaje.
 - Firma profesional: Incluir una firma corporativa estandarizada con información de contacto.
 - Uso de CC y CCO: Utilizar CC solo para personas que necesitan estar informadas y CCO para proteger la privacidad en correos masivos.
 - Ortografía y gramática: Revisar los mensajes antes de enviarlos para mantener un estándar profesional.
 - Responder a todos: Evitar "Responder a todos" cuando no sea necesario.
- **Gestión y retención de correos:**
 - Clasificación: Organizar los correos por categorías o carpetas para facilitar su gestión.
 - Política de retención: Establecer periodos de conservación para diferentes tipos de correos (ej.: 1 año para comunicaciones generales, 7 años para comunicaciones financieras).
 - Archivo: Archivar correos importantes periódicamente para optimizar el espacio.
 - Eliminación: Eliminar correos innecesarios para mantener la capacidad de almacenamiento.
- **Respuesta y accesibilidad:**

- Tiempo de respuesta: Establecer expectativas sobre tiempos de respuesta (ej.: 24-48 horas en días laborables).
- Ausencias: Configurar respuestas automáticas en caso de ausencia.
- Horarios: Definir horarios recomendados para el envío de correos corporativos.
- Urgencia: Establecer protocolos para comunicaciones urgentes.
- **Cumplimiento legal:**
 - Avisos legales: Incluir descargos de responsabilidad en correos externos.
 - Protección de datos: Cumplir con regulaciones de protección de datos aplicables (GDPR, LGPD, etc.).
 - Registro de comunicaciones: Aclarar que la empresa puede monitorear las comunicaciones por correo electrónico.
 - Propiedad intelectual: Proteger la propiedad intelectual de la empresa en las comunicaciones.
- **Sanciones por incumplimiento:**
 - Graduación de sanciones: Se debe ceñir a los lineamientos del código disciplinario para funcionarios de la Universidad o lo establecido en los contratos de prestación de servicios.
 - Procedimiento disciplinario: Se debe ceñir a los lineamientos del código disciplinario para funcionarios de la Universidad o lo establecido en los contratos de prestación de servicios.
 - Capacitación: Establecer programas de formación sobre el uso adecuado del correo electrónico.
- **Revisión y actualización:**
 - Periodicidad: Revisar y actualizar la política de correo electrónico anualmente.
 - Comunicación de cambios: Informar a todos los empleados sobre cualquier actualización de la política.
 - Acuse de recibo: Solicitar a los empleados que confirmen haber leído y entendido la política.

USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

5. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

La Universidad De Caldas, definirá un **“Plan de Comunicación en Seguridad de la Información”** a través de su oficina de comunicación interna y externa y La Oficina Asesora de Planeación y Sistemas, donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones o tips de seguridad de la información por

diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de La Oficina Asesora de Planeación y Sistemas y/o el Oficial de Seguridad de la información.

CAPACITACIONES EN SEGURIDAD

La Universidad de Caldas, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de la información, La Oficina Asesora de Planeación y Sistemas y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de la Universidad de Caldas.

7. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de la Universidad De Caldas de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

- Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
- Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
- La Oficina Asesora de Planeación y Sistemas será la encargada de recopilar y entregar a la Oficina de Control Interno las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, La Oficina Asesora de Planeación y Sistemas será la encargada de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.



ELABORÓ	REVISÓ Y APROBÓ
Nombre: Héctor Fabio Torres Martínez Cargo: Líder del grupo interno de sistemas Fecha: 1-abril-2025	Nombre: Yamile Uribe Cargo: Jefe Oficina Asesora de Planeación y Sistemas Fecha: 1-abril-2025

Control de versiones

VERSIÓN	DESCRIPCIÓN	FECHA
1.0	Versión inicial	1/04/2025