Bellas Artes
Institución Universitaria
del Valle del Cauca

Plan de Seguridad y Privacidad de la Información Institución Departamental de Bellas Artes de Cali

Vigencia 2026

Área de recursos tecnologicos

1. Introducción

La protección de la información es un componente esencial para garantizar la confianza, eficiencia y cumplimiento legal dentro de la Institución Departamental de Bellas Artes de Cali. Este plan establece las directrices, políticas y medidas necesarias para salvaguardar la información de la institución frente a amenazas internas y externas, asegurando la confidencialidad, integridad y disponibilidad de los datos.

Objetivo: Garantizar la seguridad y privacidad de la información institucional mediante la implementación de medidas técnicas, administrativas y legales adaptadas a las necesidades y dinámicas de nuestra institución.

Alcance: Este plan aplica a toda la información generada, almacenada, procesada y transmitida por la institución, incluyendo datos de estudiantes, docentes, personal administrativo, proveedores y otras partes interesadas. Esto incluye el manejo de información en nuestras oficinas, aulas, laboratorios y sistemas digitales.

2. Marco Normativo y Legal

El presente plan se alinea con las normativas y leyes nacionales e internacionales aplicables:

- **Ley 1581 de 2012 (Colombia):** Protección de Datos Personales.
- **Decreto 1377 de 2013:** Reglamentación de la Ley de Protección de Datos.
- **ISO/IEC 27001:** Estándares internacionales para la gestión de la seguridad de la información.
- **Ley 1273 de 2009:** Protección de la información y los datos frente a delitos informáticos.

Estos marcos guían la manera en que nuestra institución gestiona, protege y responde frente a incidentes relacionados con la seguridad de la información.

3. Principios Rectores

Este plan se fundamenta en los siguientes principios:

- **Confidencialidad:** Solo las personas autorizadas pueden acceder a la información institucional.

- **Integridad:** La información debe mantenerse completa y sin alteraciones no autorizadas.
- **Disponibilidad:** La información estará accesible para las personas autorizadas cuando sea necesario para las operaciones de nuestra institución.
- **Transparencia:** Los titulares de datos serán informados sobre el uso y tratamiento de su información.
- **Responsabilidad:** La institución asumirá un rol activo en la protección de la información, asegurando que todos los miembros de la comunidad académica cumplan con estas directrices.

4. Identificación de Activos y Evaluación de Riesgos

4.1. Inventario de Activos de Información La institución ha identificado y clasificado los activos de información relevantes para garantizar su adecuada protección:

- **Activos Digitales:**
  - Bases de datos de estudiantes, docentes y administrativos.
  - Sistemas de gestión académica como SIGA.
  - Sistemas de contabilidad orion.
  - Correo electrónico institucional proporcionado a cada miembro de la comunidad.
  - Documentos en la nube y servidores locales gestionados por el área de TI.

- **Activos Físicos:**
  - Expedientes académicos en papel gestionados por el área administrativa.
  - Equipos de cómputo, impresoras, escáneres y cámaras utilizados en las áreas de creación y soporte.

4.2. Evaluación de Riesgos En la institución hemos identificado posibles amenazas que puedan comprometer los activos:

- **Amenazas internas:**
  - Accesos no autorizados debido a errores humanos.
  - Pérdida de dispositivos institucionales.
  - Negligencia en el manejo de información sensible.
- **Amenazas externas:**

- Hackeos dirigidos al sistema de gestión académica.
- Malware y phishing a través de correos electrónicos.
- Robo de equipos en áreas vulnerables de nuestras instalaciones.

Cada amenaza ha sido evaluada en función de su impacto y probabilidad, permitiéndonos establecer un mapa de riesgos específico para priorizar las acciones preventivas y correctivas.

5. Políticas y Procedimientos de Seguridad

5.1. Política de Uso de Contraseñas

Requisitos para la Creación de Contraseñas

Las contraseñas deben cumplir los siguientes requisitos:

- Tener una longitud mínima de 12 caracteres (recomendado 16).
- Incluir al menos:
  - 1 letra mayúscula.
  - 1 letra minúscula.
  - 1 número.
  - 1 carácter especial (e.g., @, #, %, *).
- No deben contener:
  - Palabras comunes o frases populares (e.g., "contraseña", "123456").
  - Información personal como nombres, fechas de nacimiento, documentos de identidad o números telefónicos.

Ejemplo de contraseña segura:

C@l1B3ll@s2025!

Reglas de Rotación y Validez de Contraseñas

- Las contraseñas deben actualizarse cada **90 días**.

- No está permitido reutilizar las últimas **5 contraseñas**.
- Cuando se detecte un incidente de seguridad o compromiso de contraseña, esta deberá ser cambiada de manera inmediata.

Protección y Uso de Contraseñas

- Las contraseñas son personales e intransferibles.
- No deben compartirse por ningún medio, ni con compañeros de trabajo, supervisores o terceros.
- No almacenar contraseñas en lugares accesibles (e.g., post-its, documentos no cifrados).
- Usar un gestor de contraseñas confiable para almacenarlas de manera segura.

Procedimiento para la Gestión de Contraseñas Creación y Actualización de Contraseñas

1. Acceder al sistema o plataforma correspondiente y seleccionar la opción de cambio o creación de contraseña.
2. Generar una contraseña siguiendo los lineamientos establecidos en este procedimiento.
3. Confirmar la contraseña y verificar que cumpla con los requisitos.
4. Registrar la nueva contraseña en un gestor de contraseñas (opcional pero recomendado).

Uso Seguro de Contraseñas

1. Al ingresar contraseñas en un sistema, evitar que personas cercanas puedan visualizarla.
2. Desactivar la opción de "guardar contraseñas" en navegadores de uso compartido.
3. Al detectar conductas sospechosas en el sistema (e.g., acceso no autorizado), reportarlo de inmediato al área de soporte técnico.

Recuperación de Contraseñas Olvidadas

1. Acceder al enlace de recuperación del sistema correspondiente.
2. Seguir el proceso de validación, que puede incluir responder

preguntas de seguridad o autenticación multifactor.
3. Generar una nueva contraseña siguiendo los lineamientos de seguridad.
4. Confirmar la contraseña y asegurarse de su funcionamiento.

Responsabilidades

Responsabilidades

de los Usuarios

- Crear contraseñas seguras y únicas para cada sistema.
- Proteger las contraseñas de accesos no autorizados.
- Informar de inmediato al área de soporte técnico si sospechan que una contraseña ha sido comprometida.

Responsabilidades del Área de Soporte Técnico

- Configurar políticas de contraseñas en los sistemas de la Institución (longitud mínima, complejidad, caducidad).
- Brindar soporte a los usuarios en caso de problemas relacionados con contraseñas.
- Implementar herramientas de monitoreo para detectar accesos no autorizados.
- Realizar auditorías periódicas para verificar el cumplimiento de este procedimiento.

Responsabilidades de la Alta Dirección

- Velar por el cumplimiento de este procedimiento en toda la Institución.
- Promover la capacitación de los empleados en temas de seguridad de contraseñas.

Capacitación y Sensibilización

- Se realizará una capacitación anual sobre las mejores prácticas en la gestión de contraseñas.
- El área de soporte técnico proporcionará guías y tutoriales para el uso de herramientas seguras.

Sanciones por Incumplimiento

El incumplimiento de este procedimiento puede derivar en:

- Suspensión del acceso a los sistemas tecnológicos.

- Sanciones disciplinarias conforme al reglamento interno de la Institución.
- Reportes legales en caso de negligencia grave que comprometa la seguridad de la información.

Revisión y Actualización del Procedimiento

Este procedimiento será revisado y actualizado cada **6 meses** o cuando haya cambios significativos en las tecnologías o en las normativas de seguridad de la información.

Ejemplos de Contraseñas Seguras

- Ejemplo 1: **T3at!ro2025#Cali**
- Ejemplo 2:

Música@B3llas#20

25

Recomendaciones de

Gestores de Contraseñas

- **LastPass** (versión gratuita y de pago).
- **1Password** (versión de pago).
- **Bitwarden** (versión gratuita y de pago).

Guía para Activar la Autenticación Multifactor (MFA)

1. Ingresar a la configuración del sistema.
2. Seleccionar la opción “Seguridad” o “Autenticación”.
3. Activar la autenticación multifactor.
4. Asociar un número de teléfono o aplicación (e.g., Google Authenticator).
5. Confirmar el proceso con un código enviado.

5.2. Política y Procedimiento de Control de Acceso

Ingreso y salida de personal administrativo, estudiantes, docentes, personal de aseo, mantenimiento y seguridad

1. El ingreso y salida se realizará mediante reconocimiento biométrico.

2. Los guardias de seguridad verificarán que no se ingrese con equipos electrónicos sin registro previo.
3. Todo equipo registrado en el ingreso debe coincidir con el registro de salida.

Ingreso y salida de visitantes

1. Se registrará a los visitantes mediante una tarjeta de acceso.
2. Se tomará fotografía de los equipos que ingresen.
3. Al salir, los visitantes deben devolver la tarjeta de acceso.
4. Seguridad verificará que los equipos retirados coincidan con el registro de ingreso.

PERSONAL RESPONSABLE DEL CONTROL DE ACCESO

Requisitos del personal

1. Manejo de tecnologías de escaneo y registro digital.
2. Competencia en herramientas ofimáticas para registro de datos.
3. Habilidades de atención al usuario con profesionalismo.

Horarios de trabajo

1. Turno 1: 8:00 am - 3:00 pm.
2. Turno 2: 3:00 pm - 10:00 pm.
3. Cada turno contará con dos personas para garantizar cobertura.

Funciones del personal de control de acceso

1. Crear, actualizar y eliminar registros en el sistema.
2. Tomar fotografías de equipos al ingreso.
3. Proporcionar información educativa y administrativa a usuarios.

PERSONAL DE SOPORTE

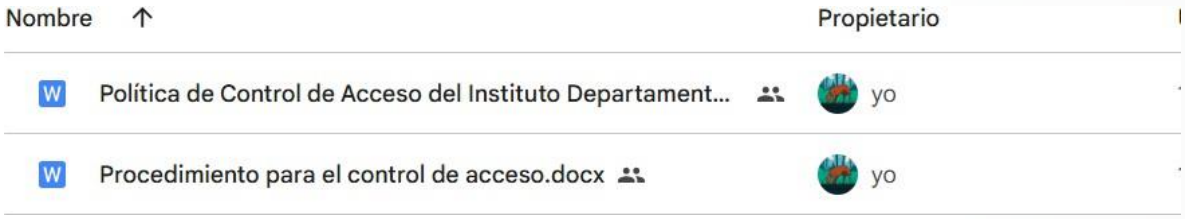
1. El área de TI brindará soporte técnico en caso de fallos en el sistema de control de acceso.
2. Se podrá solicitar soporte enviando un correo a ti@bellasartes.edu.co.

RESPALDO DEL SISTEMA DE CONTROL DE ACCESO

1. El área de TI realizará backups del sistema cada dos meses.
2. Se asegurará la integridad de los datos y el funcionamiento óptimo del sistema.

REVISIÓN Y CUMPLIMIENTO

1. La política será revisada periódicamente para garantizar su efectividad.
2. Se implementarán auditorías regulares para verificar su cumplimiento y detectar oportunidades de mejora.



5.3. Política de Respaldo de Datos

- Los datos críticos de la institución serán respaldados diariamente utilizando sistemas automáticos administrados por TI donde .
- Se mantendrán copias de seguridad en servidores locales y servicios en la nube con acceso restringido.

5.4. El phishing y procedimientos de Manejo de Correos Electrónicos

5.4.1 MANEJO DE CORREO INSTITUCIONAL

Condiciones y lineamientos de uso.

a.) El uso de la cuenta institucional es personal e intransferible

b.) Capacidad de almacenamiento asignada:

Estudiantes: Se les asignan 30 GB de espacio en la plataforma de almacenamiento institucional (Drive). Además, tendrán un periodo de 20 días al finalizar el semestre académico para respaldar o trasladar su información.

Servidores Públicos Docentes: Se les asignan 100 GB de espacio en la misma plataforma, destinados al manejo de contenidos relacionados con actividades académicas y administrativas.

Servidores Públicos administrativos y

trabajadores oficiales: Cuentas de

Dependencias:

Cuentas Temporales:

c.) Exclusividad de uso: El correo electrónico institucional es de uso exclusivo para funciones o actividades académicas propias de la institución y no debe utilizarse para otros fines.

d.) Uso ético y seguro: Los usuarios deben utilizar el correo de manera ética, razonable, eficiente, y sin comprometer la imagen de la institución.

e.) Reporte de SPAM: Los correos no deseados o sospechosos deben reportarse al área de TI Para tomar acciones necesarias.

f.) Cuota de almacenamiento: Los usuarios deben realizar una depuración periódica de los archivos adjuntos para evitar superar el límite de almacenamiento.

g.) Responsabilidad de las cuentas especiales: Las cuentas institucionales especiales deben tener una persona responsable de la depuración periódica del buzón.

h.) Reporte de solicitudes de información personal: Los usuarios deben reportar mensajes que soliciten información personal o financiera.

i.) Tamaño máximo de archivos: El tamaño máximo de cada mensaje enviado o recibido es de 25 MB. Si se supera este tamaño, el archivo se carga en Google Drive y se genera un enlace en el mensaje.

j.) Cuota diaria de envío: Si un usuario supera los 2000 correos electrónicos diarios, la cuenta se suspenderá por 24 horas.

k.) Inactividad: Las cuentas que no presenten actividad por más de un año se eliminarán, incluyendo toda la información asociada.

l.) Responsabilidad de backups: Los usuarios son responsables de los respaldos de información de sus cuentas institucionales.

m.) Exclusividad de uso: Google Drive debe utilizarse exclusivamente para archivos institucionales que permitan el desarrollo de las funciones propias de la institución, respetando la capacidad máxima por usuario.

n.) Responsabilidad de los archivos: Los archivos en Google Drive son responsabilidad de los usuarios, quienes deben realizar depuración periódica para evitar alcanzar el límite de almacenamiento

uso inaceptable:

Del correo electrónico:

a.) Utilizarlo para fines personales, comerciales o cualquier actividad no relacionada con la institución es inaceptable

b.) Enviar mensajes que contengan contenido ofensivo, discriminatorio o inapropiado que comprometa la integridad de la institución.

c.) El envío de correos electrónicos masivos sin la debida autorización o propósito académico válido puede ser considerado spam, lo cual no está permitido y puede llevar a la suspensión de la cuenta.

d.) Compartir información confidencial o sensible sin

autorización pone en riesgo la seguridad de la institución y sus miembros.

e.) Enviar mensajes que excedan el tamaño máximo permitido (25 MB) sin utilizar los métodos adecuados, como la generación de enlaces en Google Drive, es inaceptable y puede afectar el rendimiento del sistema de correo.

Del almacenamiento en la nube

a.) Almacenar archivos personales, comerciales o no relacionados con la institución es inaceptable.
b.) Compartir archivos sin las medidas de seguridad adecuadas, como permisos de acceso restringidos, puede comprometer la privacidad y seguridad de la información almacenada.
c.) No realizar la depuración periódica de archivos puede llevar a exceder el límite de almacenamiento.

RESPONSABILIDAD:

es responsabilidad de cada usuario:

a.) Cada usuario debe proteger la contraseña, así como el evitar que la cuenta sea utilizada por terceros.
b.) Cada usuario es responsable de salvaguardar la información haciendo los Backups correspondientes.
c.) Mantenerse actualizado sobre las modalidades de ataques cibernéticos para evitar el robo de información.

Gestión de contraseñas: Cuando requiera el cambio de contraseña deberá tramitarse directamente por el usuario del correo ante el área de TI; el cual será atendido a más tardar en dos (2) días hábiles.

Cualquier incumplimiento de los lineamientos aquí establecidos dará lugar a la suspensión de la cuenta institucional, sin perjuicio de las sanciones disciplinarias que pueda acarrear y para los contratistas, la terminación del vínculo contractual.

Alcance: El correo electrónico institucional es un servicio tecnológico provisto por el Instituto Departamental de Bellas Artes de uso imperativo para todos los miembros de la comunidad universitaria ya que este constituye un medio de comunicación oficial, por lo tanto, los presentes lineamientos son de obligatorio cumplimiento.

La presente rige a partir de la fecha de su expedición y su publicación, la cual se entenderá surtida el día de la publicación

5.4.2 Procedimiento identificación de correo electrónico malignos(Phishing)

CONDICIONES GENERALES PARA LA IDENTIFICACIÓN DE CORREOS MALICIOSOS

4.1 Características de los correos maliciosos

1. **Remitente sospechoso:** Direcciones de correo que imitan a entidades legítimas, pero con modificaciones.
2. **Asuntos alarmantes:** Mensajes con títulos urgentes o que presionan para actuar rápidamente.
3. **Errores ortográficos:** Contenido mal redactado, indicativo de correos fraudulentos.
4. **Solicitudes de información personal:** Ninguna organización legítima solicita credenciales vía correo electrónico.
5. **Enlaces sospechosos:** URLs que no coinciden con el dominio oficial.
6. **Archivos adjuntos desconocidos:** Pueden contener malware y deben evitarse.

4 Acciones a seguir ante un correo sospechoso

1. No abrir el correo.
2. No hacer clic en enlaces ni descargar archivos adjuntos.
3. No responder al remitente.
4. Reportar el correo al equipo de TI.

DESCRIPCIÓN DETALLADA DEL PROCEDIMIENTO

No	ACTIVIDAD	RESPONSABLE	DOCUMENTO	TIEMPO
1	Identificación del correo sospechoso	Usuario final	N/A	Inmediato
2	No interactuar con el contenido sospechoso	Usuario final	N/A	Inmediato
3	Reporte al equipo de TI	Usuario final	Correo de notificación	Inmediato
4	Análisis del correo	Equipo de TI	Informe técnico	24 horas
5	Aplicación de medidas preventivas	Equipo de TI	Registro de seguridad	Según caso
6	Capacitar a los usuarios	Dirección de Seguridad Informática	Material de formación	Periódico

DOCUMENTACIÓN Y REGISTRO

Los incidentes relacionados con correos maliciosos deben registrarse en el sistema de seguridad informática, incluyendo:

- Registro del correo recibido.
- Análisis técnico del mensaje.
- Acciones correctivas y preventivas adoptadas.
- Reportes consolidados para la alta dirección.

6. Medidas Técnicas y Organizativas

6.1. Medidas Técnicas:

- **Cifrado:** Todos los datos sensibles serán cifrados antes

de ser almacenados o transmitidos.

- **Actualizaciones:** Se aplicarán actualizaciones regulares a los sistemas operativos y software utilizados en nuestras instalaciones.
- **Antivirus y Firewall:** Todos los dispositivos estarán protegidos con soluciones actualizadas de seguridad por medio de la aplicación karpeski.

6.2. Medidas Organizativas:

- **Capacitación:** Programas periódicos de formación en seguridad digital para todos los empleados y estudiantes.
- **Auditorías:** Revisiones trimestrales realizadas por el área de TI para evaluar el cumplimiento de las políticas establecidas.

7. Plan de Respuesta a Incidentes

7.1. Procedimiento de Respuesta:

- **Detección:** Monitoreo constante utilizando herramientas automatizadas para identificar incidentes.
- **Contención:** Acciones inmediatas dirigidas a mitigar el impacto del incidente.
- **Análisis:** Evaluación profunda para determinar la causa raíz y el alcance del problema.
- **Recuperación:** Restauración de sistemas y datos afectados en el menor tiempo posible.
- **Informe:** Elaboración de un informe detallado para aprendizaje y mejora continua.

7.2. Roles y Responsabilidades:

- **Equipo de TI:** Gestión técnica del incidente y coordinación de la recuperación.
- **Directivos:** Comunicación con estudiantes, docentes y partes externas según sea necesario.

8. Monitoreo y Auditorías

8.1. Monitoreo:

- Herramientas avanzadas supervisan los sistemas críticos de la institución en tiempo real.

8.2. Auditorías:

- Evaluaciones anuales del cumplimiento del plan por parte de auditores externos.
- Auditorías internas trimestrales realizadas por el equipo de TI.

9. Concienciación y Capacitación

- Talleres regulares sobre protección de datos y buenas prácticas digitales dirigidos a estudiantes, docentes y administrativos.
- Campañas informativas a través de correos electrónicos y carteles en nuestras instalaciones.
- Manuales prácticos distribuidos digitalmente con guías específicas para el manejo seguro de la información.

10. Revisión y Mejora Continua

El plan será revisado anualmente tras incidentes significativos para garantizar su relevancia y efectividad. Se incorporarán nuevas tecnologías, normativas y mejores prácticas adaptadas a nuestras necesidades institucionales.
Compromiso Institucional: La Institución Departamental de Bellas Artes de Cali reafirma su compromiso con la seguridad y privacidad de la información, promoviendo una cultura organizacional enfocada en la protección de los datos y la prevención de riesgos. Nuestro equipo se dedica activamente a garantizar que este plan sea una herramienta viva, alineada con los objetivos académicos y administrativos.