UNIVERSIDAD ABIERTA Y A DISTANCIA DE MÉXICO

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

TABLA DE CONTENIDO

INTRODUCCIÓN

La LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales. Siendo de orden público y de observancia general en toda la República, para todas las dependencias y entidades, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

La Universidad Abierta y a Distancia de México es un órgano desconcentrado de la Secretaría de Educación Pública (SEP), con autonomía técnica, académica y de gestión, que oferta educación superior en la modalidad abierta y a distancia; es un sujeto obligado en materia de protección de datos personales y por ende responsable del tratamiento de los datos personales que trata para el ejercicio de sus atribuciones.

OBJETIVO

Establecer las políticas institucionales para la Protección de los Datos Personales, específicamente las medidas de seguridad concretas implementadas en los sistemas de supervisión y vigilancia para comprobar el cumplimiento de dichas políticas. Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales, así como poner en práctica programas de capacitación y actualización del personal. Fijar parámetros para la actuación de los responsables de protección de datos personales previstos en la LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS y demás disposiciones que resulten aplicables en la materia.

PARTE 1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

A. Coordinación de Tecnología e Innovación Educativa - Universidad Abierta y a Distancia de México

A1. Sistema de Gestión Escolar (SIGE)

Responsable:

- Nombre: Elizabeth González Salazar
- Cargo: Directora de Asuntos Escolares y Apoyo a Estudiantes
- Funciones:
    - Integrar, procesar y evaluar la información académica y escolar de los estudiantes inscritos en la Universidad generando los registros correspondientes en las bases de datos, las estadísticas que de ellas se deriven; así como administrar y vigilar su uso, en los términos de la Ley de Transparencia y Acceso a la Información Pública Gubernamental y otras disposiciones aplicables.
- Obligaciones:
    - Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Encargados:

- Nombre: Gabriela Charlotte Quiroz Schumann
- Cargo: Coordinadora de Tecnología e Innovación Educativa
- Funciones:
    - Administrar, resguardar y mantener actualizadas las bases de datos de los alumnos inscritos en los planes y programas de estudio que imparta la Universidad en todos los niveles, tipos y modalidades, así como la del personal académico.
    - Obligaciones:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- Guardar confidencialidad respecto de los datos personales tratados;
- Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

- Nombre: César Gerardo Waldo González
- Prestador de servicos profesionales por honorarios responsable de Base de Datos
- Actividades:
  - Administrar el Manejador de base de datos
  - Validar la confiabilidad de la base de datos
- Obligaciones:
  - Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
  - Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
  - Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
  - Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
  - Guardar confidencialidad respecto de los datos personales tratados;
  - Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Usuarios:

- Nombre: Elizabeth González Salazar
- Cargo: Directora de Asuntos Escolares y Apoyo a Estudiantes
- Funciones:
  - Integrar, procesar y evaluar la información académica y escolar de los estudiantes inscritos en la Universidad generando los registros correspondientes en las bases de datos, las estadísticas que de ellas se deriven; así como administrar y vigilar su uso, en los términos de la Ley de Transparencia y Acceso a la Información Pública Gubernamental y otras disposiciones aplicables.
- Obligaciones:
  - Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

- Nombre: Edgar Alcantar Corchado
- Cargo: Coordinador Académico y de Investigación
- Funciones:
  - Proporcionar a la Secretaría General, en el ámbito de su competencia, la información para el Sistema Institucional de Información y las estadísticas que de ella se deriven, con base en los lineamientos que emita dicha Secretaría.
- Obligaciones:
  - Guardar confidencialidad respecto de los datos personales tratados

Datos personales contenidos en el sistema:

Señale los medios a través de los cuales se obtienen los datos personales en este tratamiento	Describe el medio por el cual se obtienen los datos personales	Indique los datos personales que fueron recabados	Indique los datos sensibles que fueron recabados
El estudiante ingresa los datos personales por medio del Sistema de Gestión Escolar, el cual es un aplicativo web, que puede ser accedido desde cualquier navegador, y su acceso se encuentra disponible directamente desde el sitio principal de la Universidad.	A1. Sistema de Gestión Escolar (SIGE)	1. Cédula Profesional (número de cédula) 2. CLABE Interbancaria 3. Correo electrónico personal y alterno 4. CURP 5. Datos laborales (Institución o empresa, puesto, fecha de inicio, fecha de término, referencias) 6. Domicilio (País, Municipio, código postal, colonia, calle, número exterior o interior) 7. Edad 8. Estado civil 9. Estudios cursados 10. Fotografía 11. Género 12. Matrícula 13. Nacionalidad 14. Datos de identificación (Nombre(s) completos, apellido paterno, apellido materno) 15. Número de Seguridad Social 16. Número telefónico 17. RFC	1. Estado de salud (padecimiento de algún tipo de discapacidad) 2. Origen Étnico (específicamente si son hablantes de lengua indígena)

Indique el formato de la base de datos	Indique la ubicación de los datos recabados	Indique los servidores con acceso a la información	Indique las transferencias que serealizan y el instrumento jurídico que las faculta
Los datos se encuentran almacenados en una base de datos: [redacted]	Base de datos: [redacted]	Se encuentra en el servidor [redacted] de los servidores de IPICYT	No se realizan transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados o aquellas en el ejercicio de las atribuciones encomendadas a esta Casa de Estudios, de conformidad con lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Específicamente, los datos personales que se recopilan de LOS ESTUDIANTES son destinados a los siguientes propósitos:

- FINALIDADES PRIMARIAS: a) Para fines de identificación, b) Para fines de validación de información, c) Para fines estadísticos y de análisis interno, d) Para fines de información y contacto, e) Para la creación de un perfil de estudiante, y asignación de matrícula, f) Para fines de inscripción/reinscripción, g) Para acceso a las plataformas tecnológicas, h) Para equivalencias, revalidación y acreditación de estudios, así como para realizar todos los trámites necesarios ante las autoridades competentes como son: validación de antecedentes escolares, gestiones necesarias para el otorgamiento de becas, estímulos y otros medios de apoyo por parte de otras dependencias o personas morales, trámites relacionados con el título profesional y grado académico para la

expedición de la cédula profesional electrónica, seguro de salud para estudiantes en modalidad 32 ante el IMSS, entre otros. , i) Para la inscripción a eventos y/o actividades extracurriculares, j) Para la integración del expediente electrónico, y/o k) para eventualmente contactarlo vía telefónica o por correo electrónico para fines académicos/administrativos.

- FINALIDADES SECUNDARIAS: la Universidad Abierta y a Distancia de México "UnADM" utilizará su información personal para las siguientes finalidades que no son necesarias, pero que nos permiten otorgarle una mejor atención: enviarle información sobre actividades extracurriculares, para realizar difusión de reconocimientos por logros destacados, para la aplicación de encuestas y evaluaciones para mejorar la calidad de los productos y servicios que ofrecemos.

Los datos personales que se recopilan de los ADMINISTRATIVOS, DOCENTES EN LINEA, ASESORES ACADEMICOS Y TUTORES son destinados a los siguientes propósitos:

- FINALIDADES PRIMARIAS: a) Para fines de reclutamiento y selección, b) Para fines de validación de información, c) Para fines de identificación y creación de un perfil, d) Para fines estadísticos y de análisis interno, e) Para fines de información, f) para fines de contacto, g) Para la administración de servicios de recursos humanos, h) Para el cumplimiento de las disposiciones del Contrato de trabajo, i) Para acceso a las plataformas tecnológicas j) Para la realización del expediente electrónico y/o físico laboral, y/o k) Para eventualmente contactarlo vía telefónica o por correo electrónico para fines académicos/administrativos.

- FINALIDADES SECUNDARIAS: la Universidad Abierta y a Distancia de México "UnADM" utilizará su información personal para las siguientes finalidades que no son necesarias, pero que nos permiten otorgarle una mejor atención: para realizar difusión de reconocimientos por logros destacados, para la aplicación de encuestas y evaluaciones para mejorar la calidad de los productos y servicios que ofrecemos.

A2. Sistema de Encuestas UnADM

Responsable:

- Nombre: Elizabeth González Salazar
- Cargo: Directora de Asuntos Escolares y Apoyo a Estudiantes
- Funciones:

- Integrar, procesar y evaluar la información académica y escolar de los estudiantes inscritos en la Universidad generando los registros correspondientes en las bases de datos, las estadísticas que de ellas se deriven; así como administrar y vigilar su uso, en los términos de la Ley de Transparencia y Acceso a la Información Pública Gubernamental y otras disposiciones aplicables.

- Obligaciones:
  - Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Encargados:

- Nombre: Gabriela Charlotte Quiroz Schumann
- Cargo: Coordinadora de Tecnología e Innovación Educativa
- Funciones:
  - Administrar, resguardar y mantener actualizadas las bases de datos de los alumnos inscritos en los planes y programas de estudio que imparta la Universidad en todos los niveles, tipos y modalidades, así como la del personal académico.
  - Obligaciones:
  - Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
  - Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
  - Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
  - Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
  - Guardar confidencialidad respecto de los datos personales tratados;
  - Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
  - Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

- Nombre: César Gerardo Waldo González
- Prestador de servicios profesionales por honorarios responsable de Base de Datos
- Actividades:
    - Administrar el Manejador de base de datos
    - Validar la confiabilidad de la base de datos
- Obligaciones:
    - Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
    - Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
    - Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
    - Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
    - Guardar confidencialidad respecto de los datos personales tratados;
    - Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
    - Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Usuarios:

- Nombre: Elizabeth González Salazar
- Cargo: Directora de Asuntos Escolares y Apoyo a Estudiantes
- Funciones:
    - Integrar, procesar y evaluar la información académica y escolar de los estudiantes inscritos en la Universidad generando los registros correspondientes en las bases de datos, las estadísticas que de ellas se deriven; así como administrar y vigilar su uso, en los términos de la Ley de Transparencia y Acceso a la Información Pública Gubernamental y otras disposiciones aplicables.
- Obligaciones:

- Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

- Nombre: Edgar Alcantar Corchado
- Cargo: Coordinador Académico y de Investigación
- Funciones:
  - Proporcionar a la Secretaría General, en el ámbito de su competencia, la información para el Sistema Institucional de Información y las estadísticas que de ella se deriven, con base en los lineamientos que emita dicha Secretaría.
- Obligaciones:
  - Guardar confidencialidad respecto de los datos personales tratados

Datos personales contenidos en el sistema:

Señale los medios a través de los cuales se obtienen los datos personales en este tratamiento	**Describe el medio por el cual se obtienen los datos personales**	**Indique los datos personales que fueron recabados**	**Indique los datos sensibles que fueron recabados**
El estudiante ingresa los datos personales por medio del llenado de encuestas en línea las cuales tienen por objetivo complementar la información de sus perfiles sociodemográficos	A2. Sistema de Encuestas UnADM	1. Estado civil 2. Genero 3. Edad 4. Lugar de nacimiento 5. Nacionalidad 6. País de residencia 7. Domicilio (País, Municipio, código postal, colonia, calle, número exterior o interior) 8. Idioma 9. Número de Seguridad Social 10. RUSP (Registro de servidores públicos del gobierno federal)	1. Estado de salud (padecimiento de algún tipo de discapacidad) 2. Origen Étnico (específicamente si son hablantes de lengua indígena)

		11. Ingresos 12. Aficiones 13. Datos laborales (Institución o empresa, puesto, fecha de inicio, fecha de término, referencias) 14. Datos laborales (Puesto o cargo que desempeña) 15. Estudios cursados 16. Datos académicos (Trayectoria educativa) 17. CURP 18. Matrícula 19. Datos de identificación (Nombre(s) completos, apellido paterno, apellido materno)	

Indique el formato de la base de datos	**Indique la ubicación de los datos recabados**	**Indique los servidores con acceso a la información**	**Indique las transferencias que serealizan y el instrumento jurídico que las faculta**
Los datos se encuentran almacenados en una base de datos: [redacted]	Base de datos: [redacted]	Se encuentra en el servidor [redacted] de los servidores IPICYT.	No se realizan transferencias de datos personales, salvo aquéllas que sean necesarias para atender requerimientos de información de una autoridad competente, que estén debidamente fundados y motivados o aquellas en el ejercicio de las atribuciones encomendadas a esta Casa de Estudios, de conformidad con lo

			establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Específicamente, los datos personales que se recopilan de LOS ESTUDIANTES son destinados a los siguientes propósitos:

- FINALIDADES PRIMARIAS: a) Para fines de identificación, b) Para fines de validación de información, c) Para fines estadísticos y de análisis interno, d) Para fines de información y contacto.

- FINALIDADES SECUNDARIAS: la Universidad Abierta y a Distancia de México "UnADM" utilizará su información personal para las siguientes finalidades que no son necesarias, pero que nos permiten otorgarle una mejor atención: para la aplicación de encuestas y evaluaciones para mejorar la calidad de los productos y servicios que ofrecemos.

PARTE 2. POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES O BUENAS PRÁCTICAS

Coordinación de Tecnología a Innovación Educativa - Universidad Abierta y a Distancia de México

- **Ciclo de vida de los datos personales**

  1. Obtención de datos. - Al momento en el que el usuario requiere utilizar cualquiera de los servicios que ofrece la Universidad y es a través del propio interesado.
  2. Almacenamiento. - Los datos proporcionados son almacenados de manera electrónica en la base de datos
  3. Uso. - Académicos y administrativos
  4. Divulgación. - No hacemos divulgación de datos personales
  5. Cancelación, supresión o destrucción. - Derivado de la actividad de la Universidad, los datos se mantienen en resguardo histórico, por lo que no se cancelan, suprimen o destruyen.

- **Fundamento legal para el tratamiento de los datos personales**

  La UnADM trata los datos personales antes referidos con fundamento en los artículos 6° Base A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación (DOF) el 5 de febrero de 1917 y reformas posteriores; 17 de la Ley Orgánica de la Administración Pública Federal, publicada en el DOF el 29 de diciembre de 1976 y reformas posteriores; 2, apartado B, fracción V y 47, fracción V del Reglamento Interior de la Secretaría de Educación Pública, publicado en el DOF el 19 de septiembre de 2020 y reformas posteriores; 1° y 3°, fracción XV del Decreto que crea la Universidad Abierta y a Distancia de México, publicado en el Diario Oficial de la Federación, el 19 de enero de 2012; 3, fracción XXXIII, 4, 16, 17, y 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el DOF el 26 de enero de 2017; 23, 24 fracción VI y 68 de la Ley General de Transparencia y Acceso a la Información Pública, publicada en el DOF el 4 de mayo de 2015; 9 y último párrafo del artículo 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el DOF el 9 de mayo de 2016 y reformas posteriores; y 4, 7 y 26 del Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, publicado en el DOF el 26 de enero de

2018.

- **Mecanismos, medios y procedimientos disponibles para ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO)**

  El titular de los datos personales podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición de datos personales (derechos ARCO), ante la Unidad de Transparencia de la Secretaría de Educación Pública ubicada en Donceles No. 100, Oficina 304, Colonia Centro Histórico, Delegación Cuauhtémoc, Ciudad de México, C.P. 06000, en el horario de atención de 9:00 a 15:00 hrs., de lunes a viernes, o bien, a través de la Plataforma Nacional de Transparencia:

  http://www.plataformadetransparencia.org.mx/web/guest/inicio

- **Política interna de seguridad de los sistemas:**

La información que genera la Universidad Abierta y a Distancia de México reside en servidores que se encuentran ubicados en el centro de datos del IPICYT, quedando expresamente convenido en la Cláusula Décima Cuarta del Contrato de prestación de servicios entre El IPICYT y la UnADM, que toda información y documentación que les sea proporcionada u obtenida en virtud del objeto materia del presente contrato es de carácter confidencial, prohibiéndose su divulgación o publicación en forma alguna en cualquier tiempo, sin consentimiento previo por escrito de la otra parte, exceptuándose lo previsto en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

- **Características del Servicio de Seguridad de IPICYT:**

- Soporte en configuraciones y administración de los sistemas que conforman la seguridad perimetral que protegen a los servidores de UnADM.
- Compatibilidad con los sistemas virtuales para permitir la partición en múltiples dominios de seguridad, cada uno de los cuales posee un grupo exclusivo de administradores, políticas, y libretas de direcciones.
- Flexibilidad en la distribución de interfaces virtuales y Zonas de seguridad personalizables para los distintos requerimientos de UnADM.
- Gráficas de procesamiento y sesiones que permiten visualizar las tendencias dentro de los dispositivos de seguridad.
- Detección oportuna en ataques de denegación de servicios por medio de umbrales de conexión.
- Detección y limitación de conexiones que no formen parte de las conexiones normales de los sistemas.

- Gestión basada en políticas para permitir una gestión centralizada y completa del ciclo de vida del servicio.
- Clúster virtualizado de Firewall que permite alta disponibilidad de los servicios de seguridad, cumpliendo con los niveles de servicios ofertados al UnADM.
- Detección basada en políticas para el sistema de prevención de intrusos (IPS), el cual monitorea el tráfico de red y/o las actividades de un sistema, en busca de actividad maliciosa

A1. Sistema de Gestión Escolar (SIGE)

- **Norma o mejor práctica implementada:**

- Desarrollo de sistemas en modelo vista controlador (MVC).
- **Inyección de código**: [redacted]
- **Autenticación rota y Administración de sesiones**: [redacted]
- **Cross Site Scripting (XSS):** [redacted]
- **Referencias inseguras a objetos**: [redacted]
- **Configuración incorrecta de seguridad**: [redacted]
- **Exposición de información sensible**: [redacted]

[redacted]

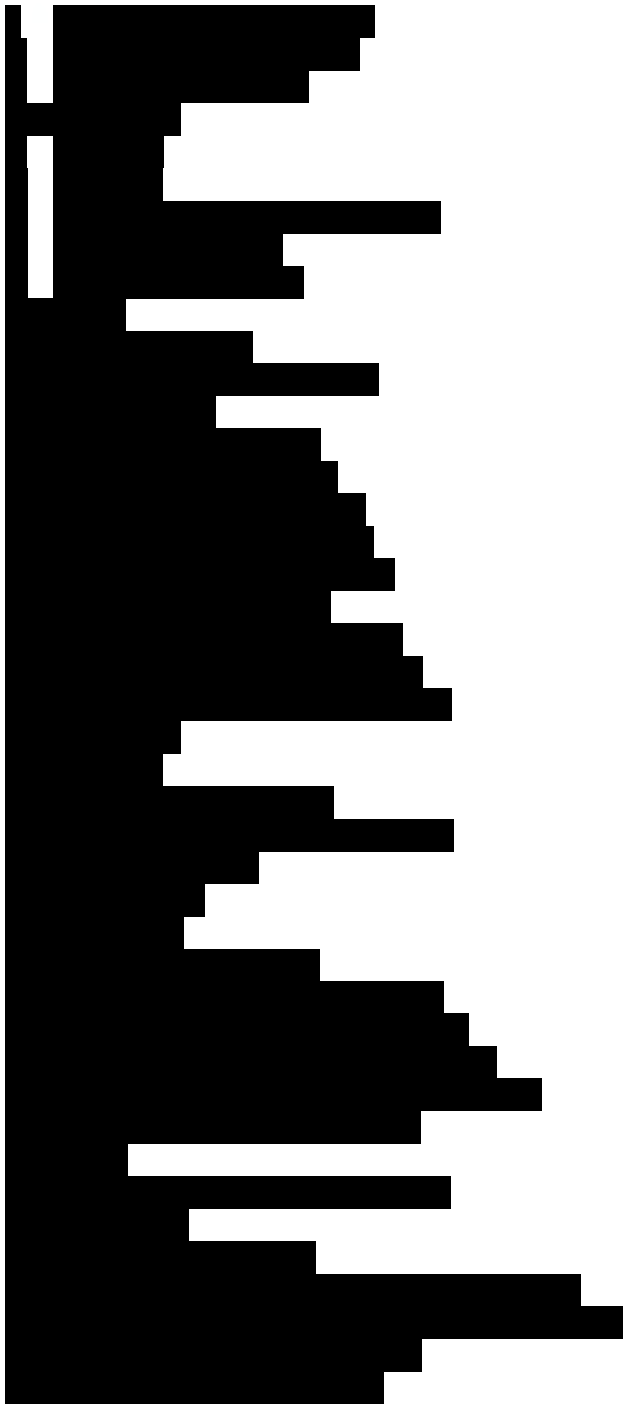
- **Falta de Control de Acceso a nivel función**: [redacted]
- **Cross-Site Request Forgery (CSRF)**: [redacted]
- **Using Known Vulnerable Components**: [redacted]
- **Unvalidated Redirects and Forwards**: [redacted]

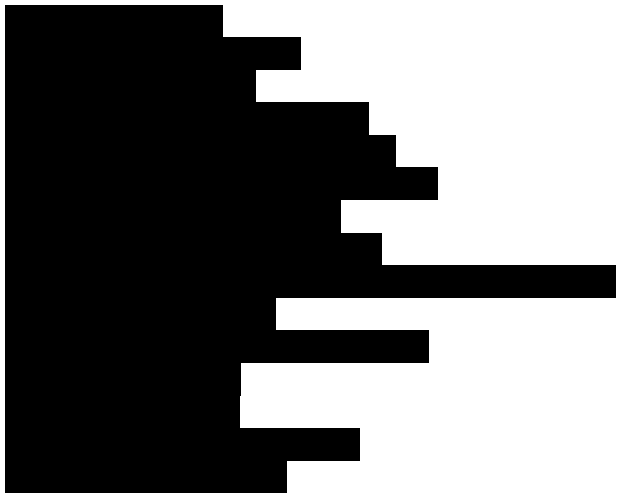
[redacted]

- **Roles y Permisos**: Cada módulo cuenta con usuario y contraseña para acceder a la base de datos. Dichos usuarios cuentan con permisos específicos acorde a la funcionalidad de cada aplicativo y únicamente tienen permisos para acceder desde los servidores donde están desplegadas las aplicaciones.

  Las contraseñas de producción son únicamente de conocimiento del personal del área de Infraestructura, el cual las administra y establece en cada uno de los despliegues en los archivos de configuración correspondientes.

✓ Los roles utilizados son los siguientes.





A2. Sistema de Encuestas UnADM

- Norma o mejor práctica implementada:

- Filtrado HTML para XSS:
- Deshabilitación del script de preguntas para el usuario restringido XSS:
- Incrustación de IFrame permitida:
- Uso de certificado SSL (Secure Sockets Layer):

- [redacted]
- **Autenticación:** [redacted]
- **Prevención de Inyección SQL:** [redacted]
- **Roles y Permisos:** el usuario SuperAdmin tiene el permiso de administrar todos los objetos del sistema (encuestas, preguntas, plantillas, etiquetas, usuarios), sin embargo, sólo el primer Superadmin puede dar este privilegio a otros usuarios.

  Las contraseñas de producción son únicamente de conocimiento del personal del área de Infraestructura, el cual las administra y establece en cada uno de los despliegues en los archivos de configuración correspondientes.

  ✓ Los roles utilizados son los siguientes.
  [redacted]

- **Utilización de la Norma ISO/IEC 27001:2013**

Uso de la metodología ISO 27001 como guía para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, así como para la evaluación y el tratamiento de los riesgos en la seguridad de la información de la Universidad.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información, investigando los potenciales problemas que podrían afectar la información realizando una evaluación y tratamiento de los riesgos

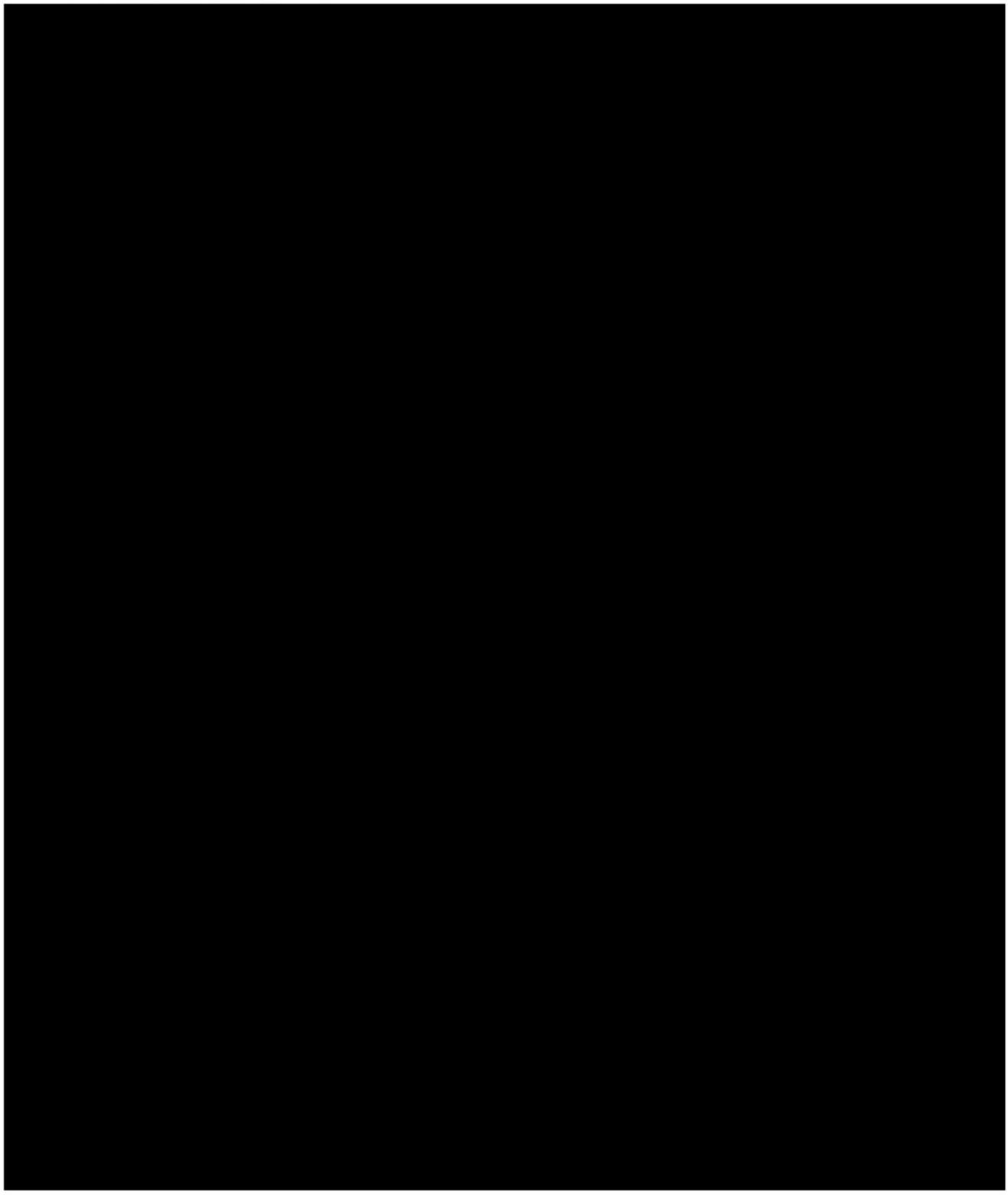
El uso de la norma permite evaluar la capacidad de la Universidad para cumplir con sus propios requisitos de seguridad de la información mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgo, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados.

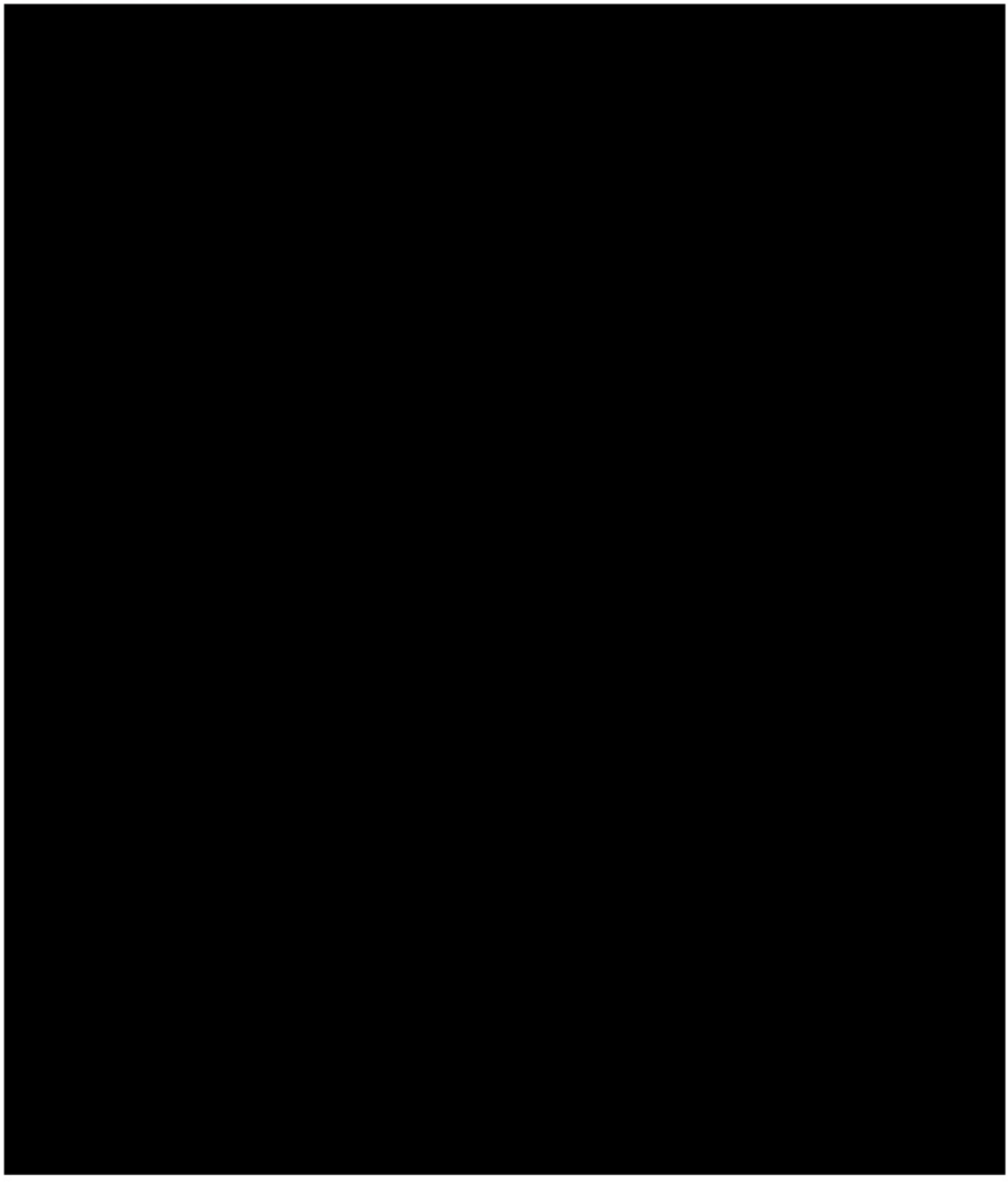
De esta forma se desprende la adopción e implementación de controles directos de la norma como lo son:

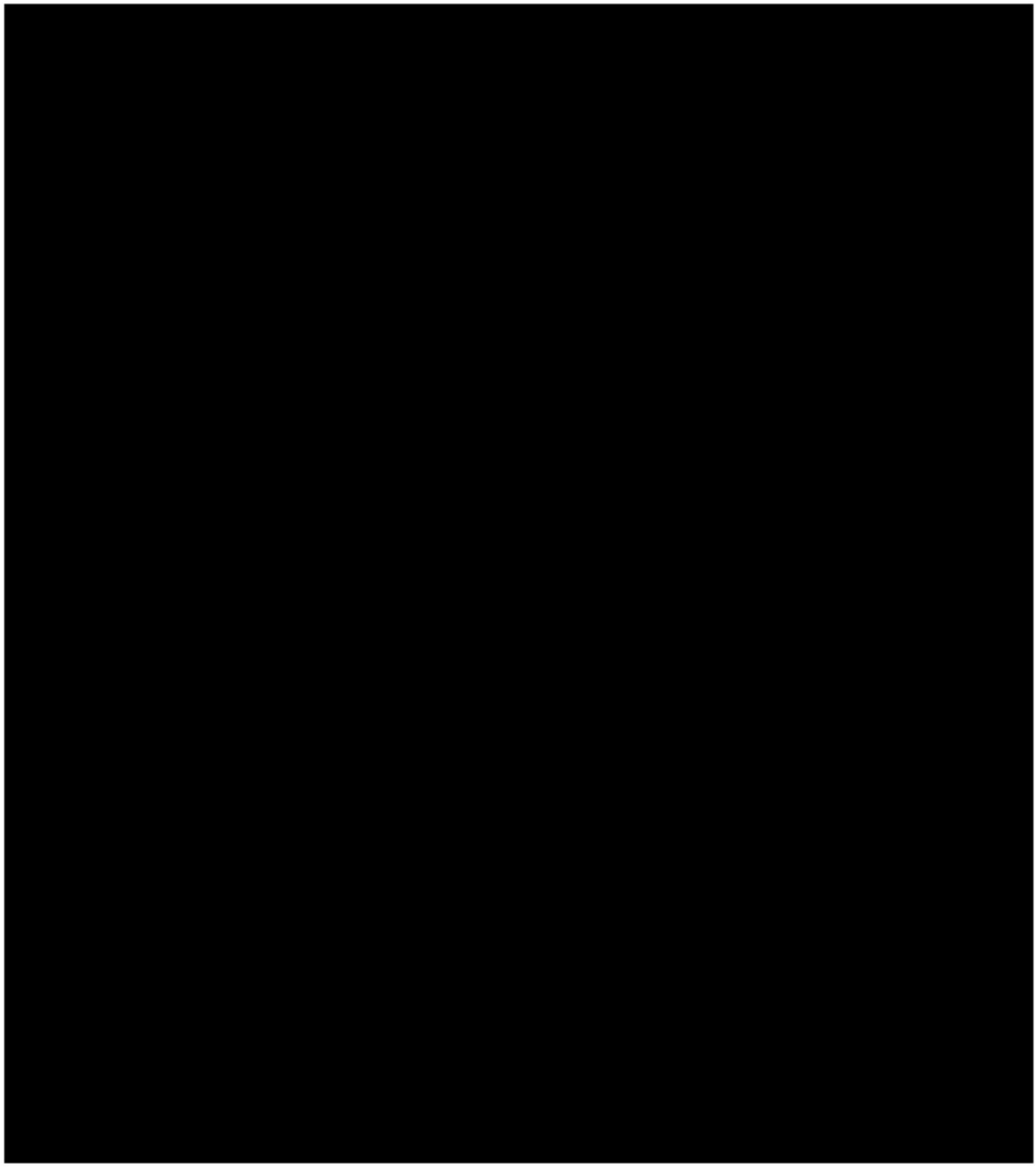
- Políticas de seguridad de la información
    - Directrices de gestión de la seguridad de la información
- Seguridad física y del entorno
    - Áreas seguras
    - Seguridad de los equipos
- Control de acceso
    - Control de acceso a sistemas y aplicaciones
- Seguridad de las operaciones
    - Procedimientos y responsabilidades operacionales
    - Registros y supervisión
    - Gestión de la vulnerabilidad técnica
- Seguridad de las comunicaciones
    - Gestión de la seguridad de las redes
    - Intercambio de información
- Adquisición, desarrollo y mantenimiento de los sistemas de información
    - Seguridad en el desarrollo y en los procesos de soporte
- Aspectos de seguridad de la información para la gestión de la continuidad de negocio

PARTE 3. ANÁLISIS DE RIESGO

Coordinación de Tecnología a Innovación Educativa - Universidad Abierta y a Distancia de México

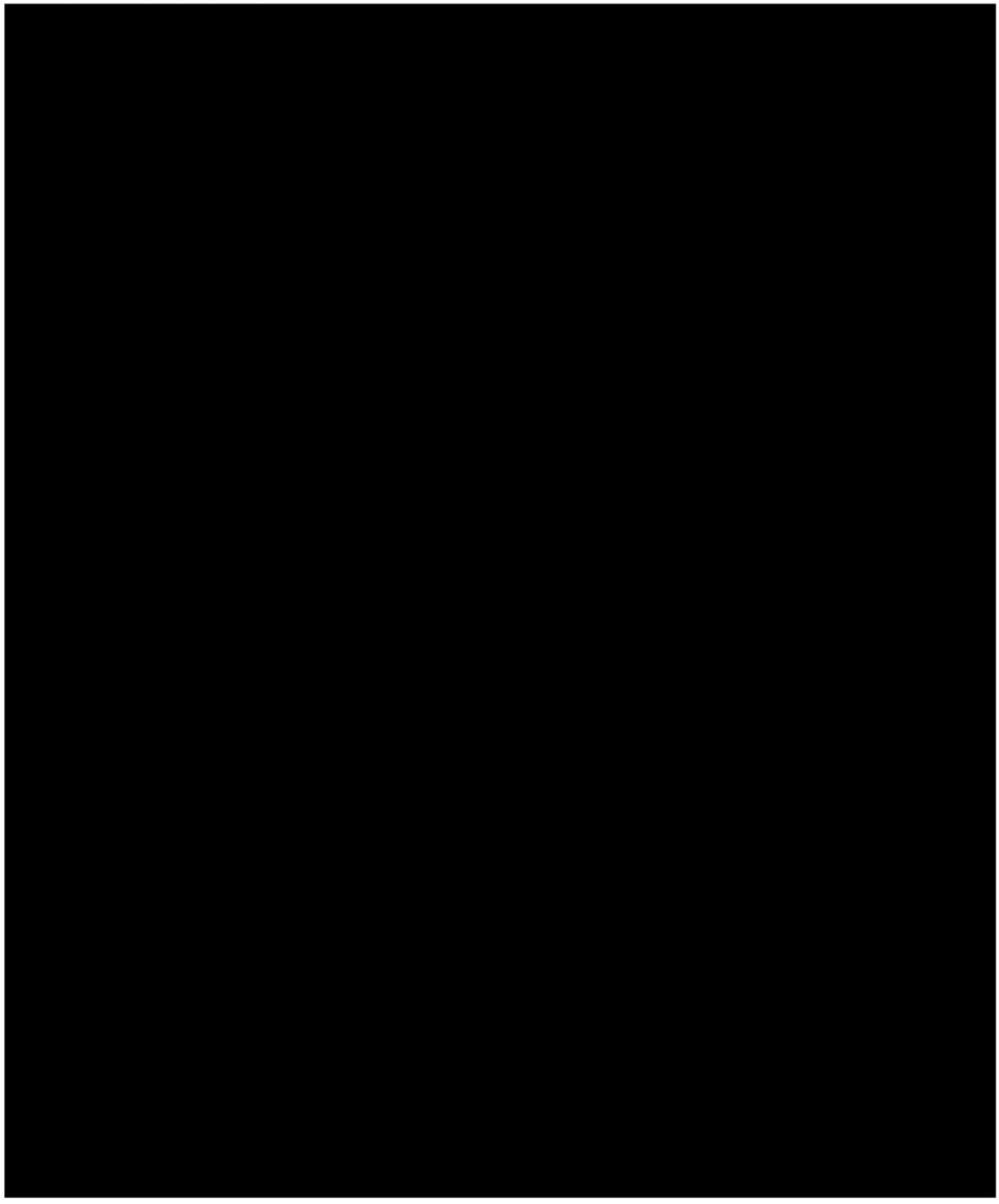


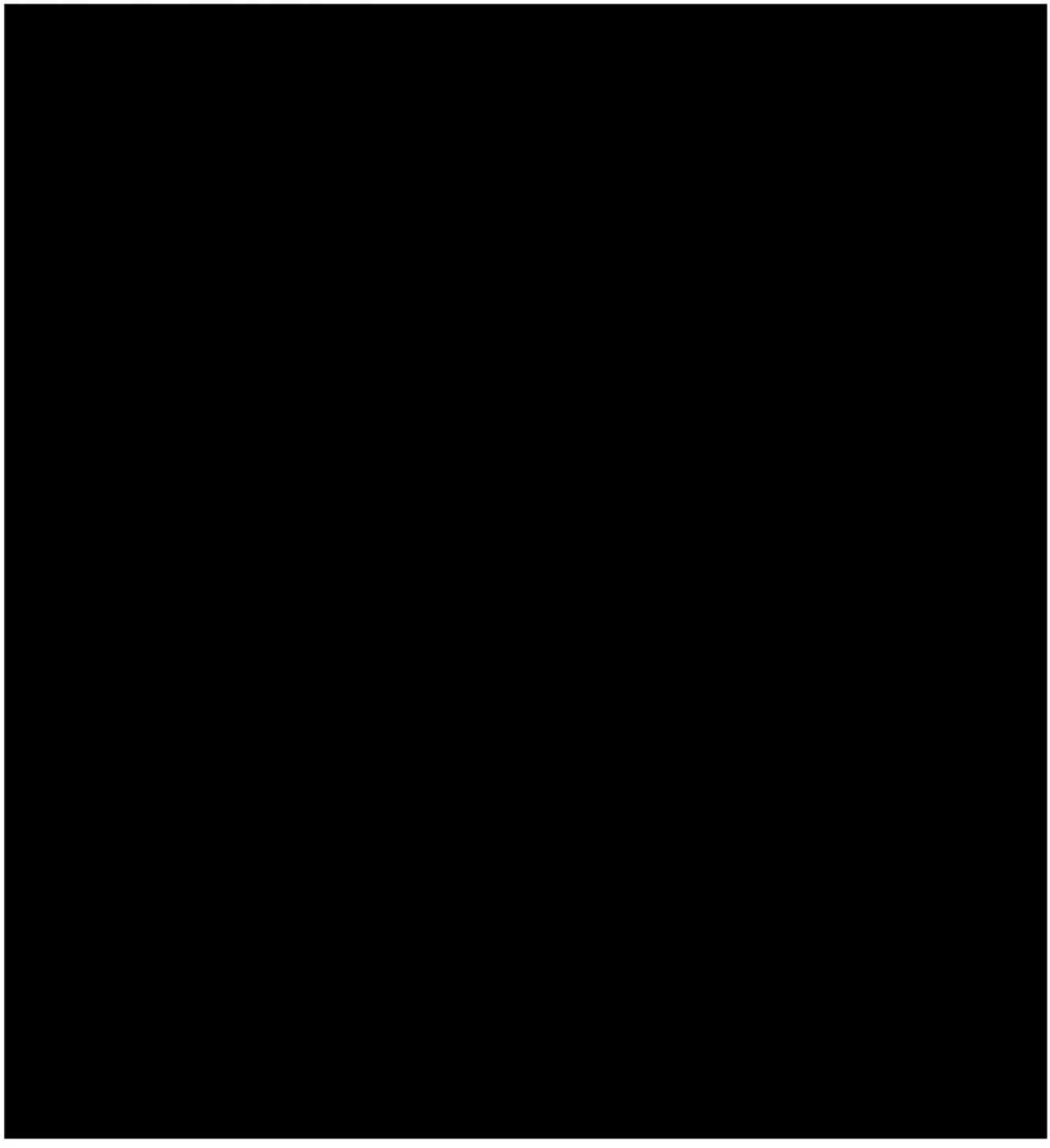


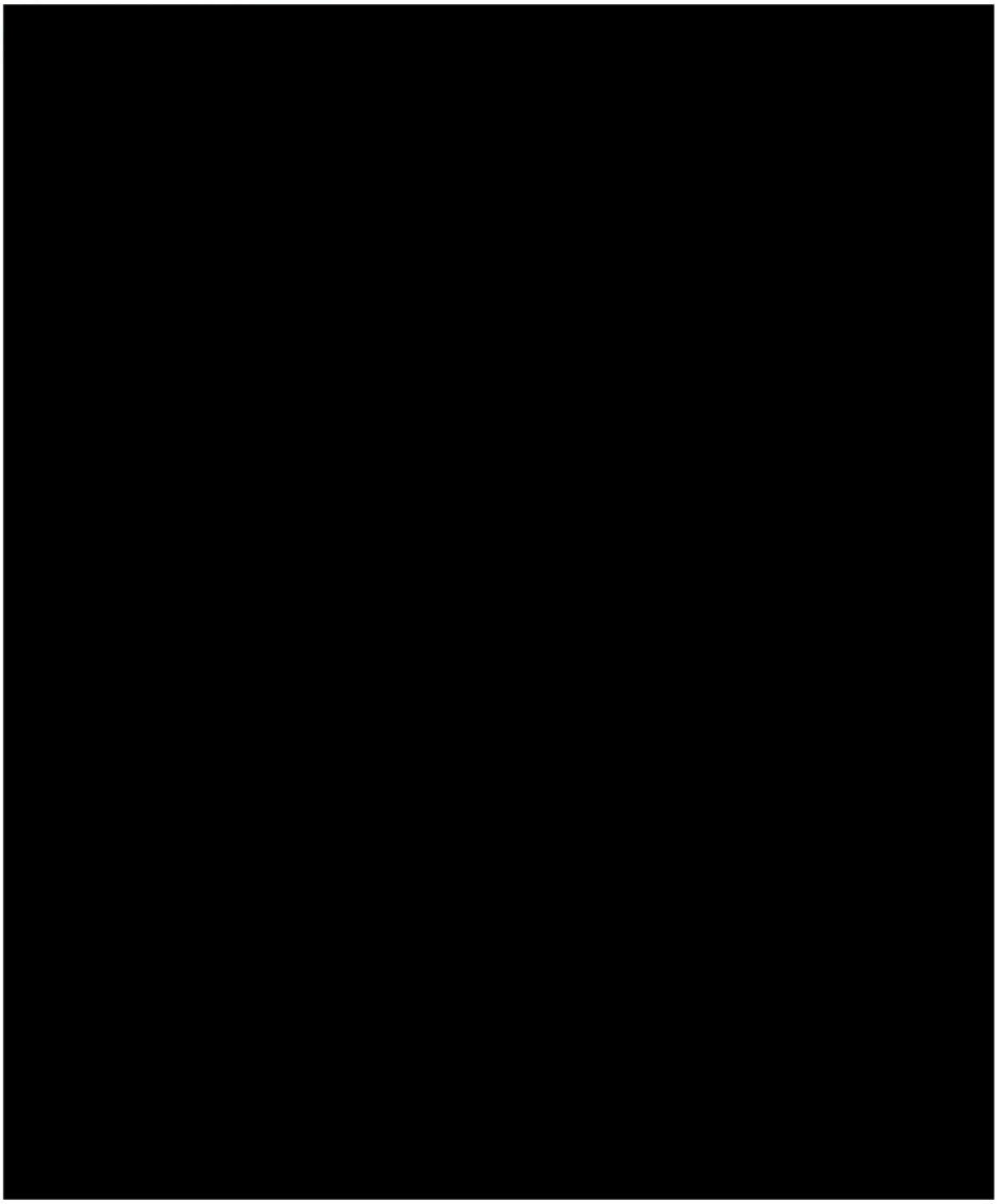


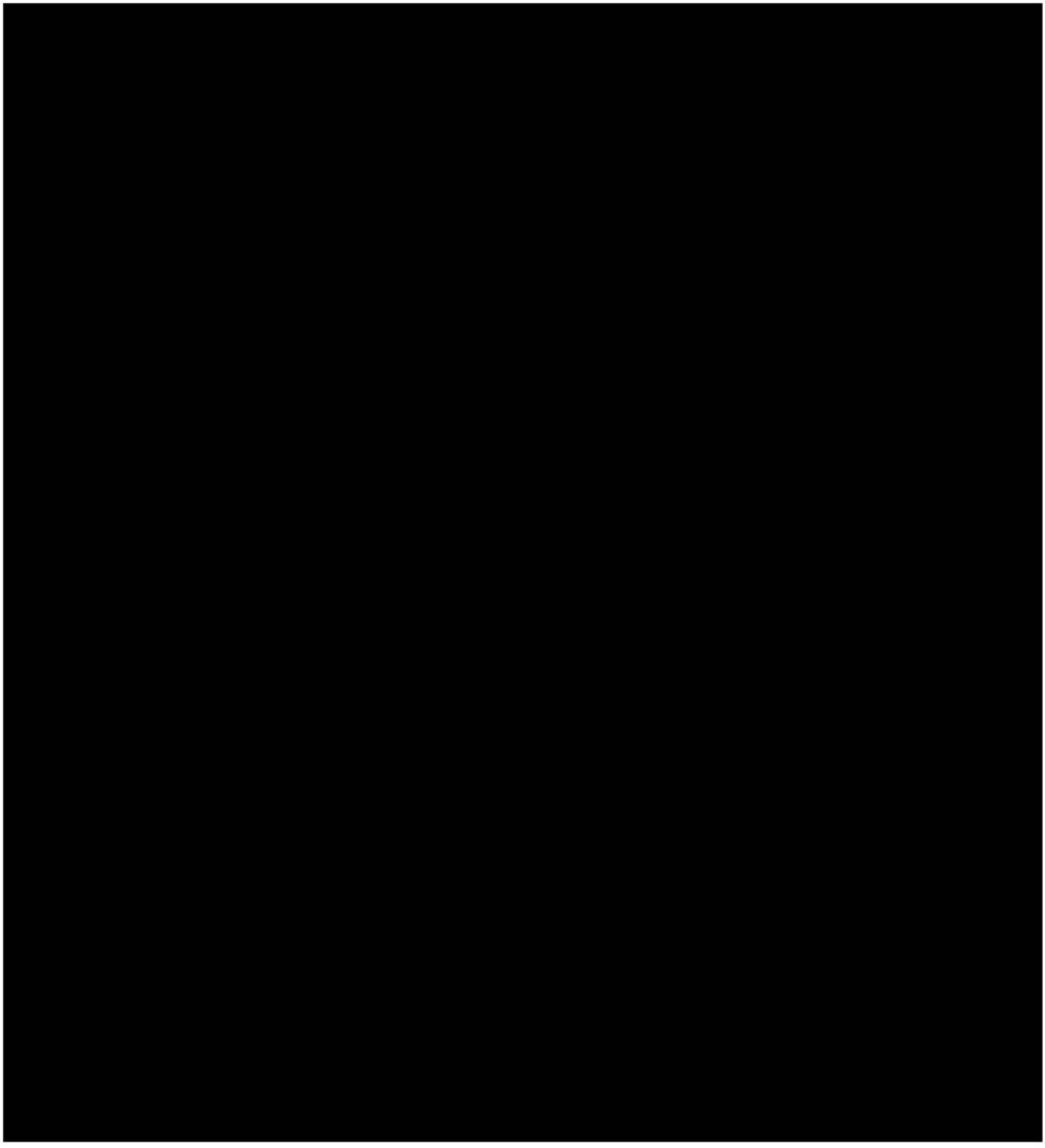
PARTE 4. ANÁLISIS DE BRECHA

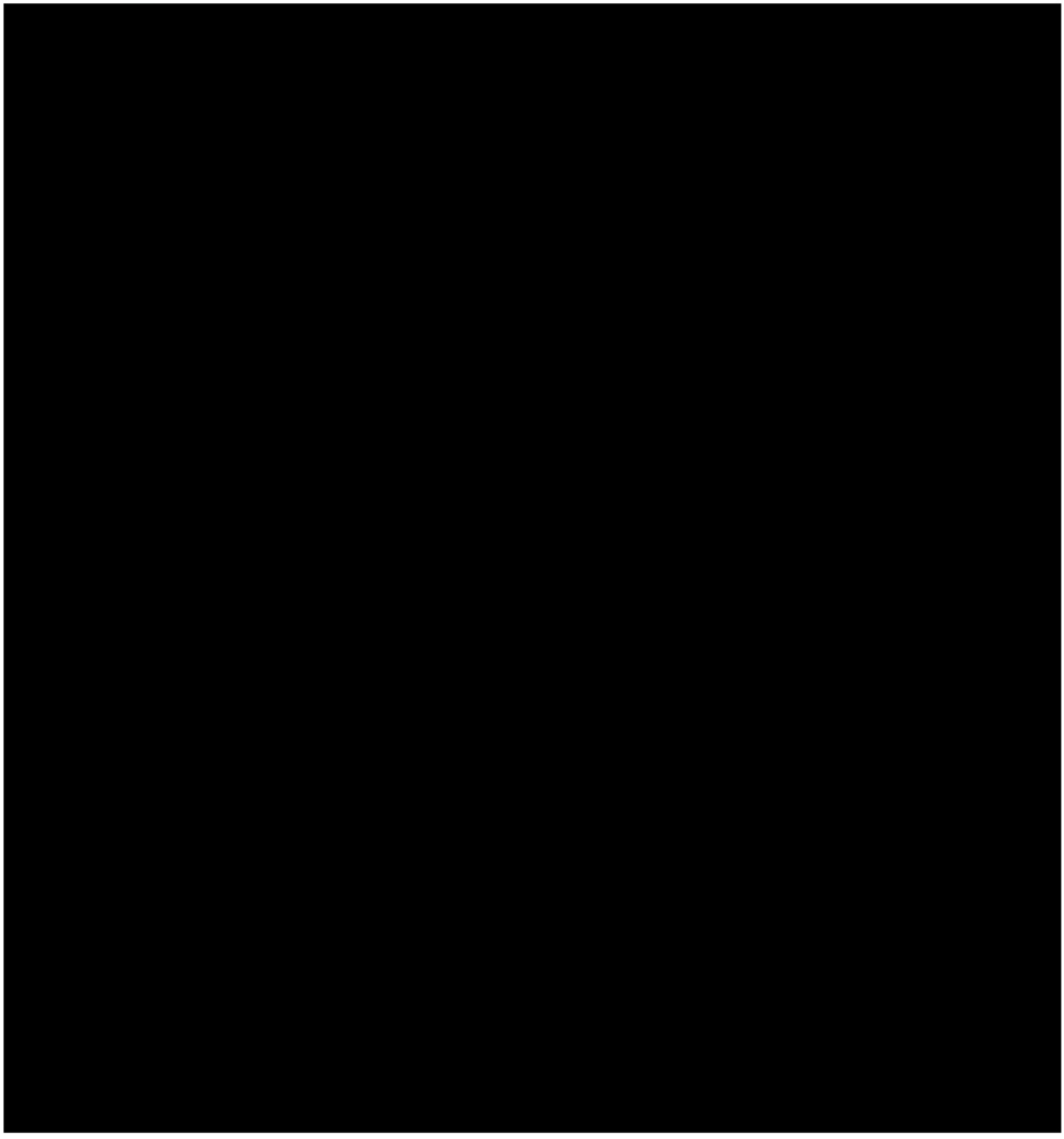
Coordinación de Tecnología a Innovación Educativa - Universidad Abierta y a Distancia de México

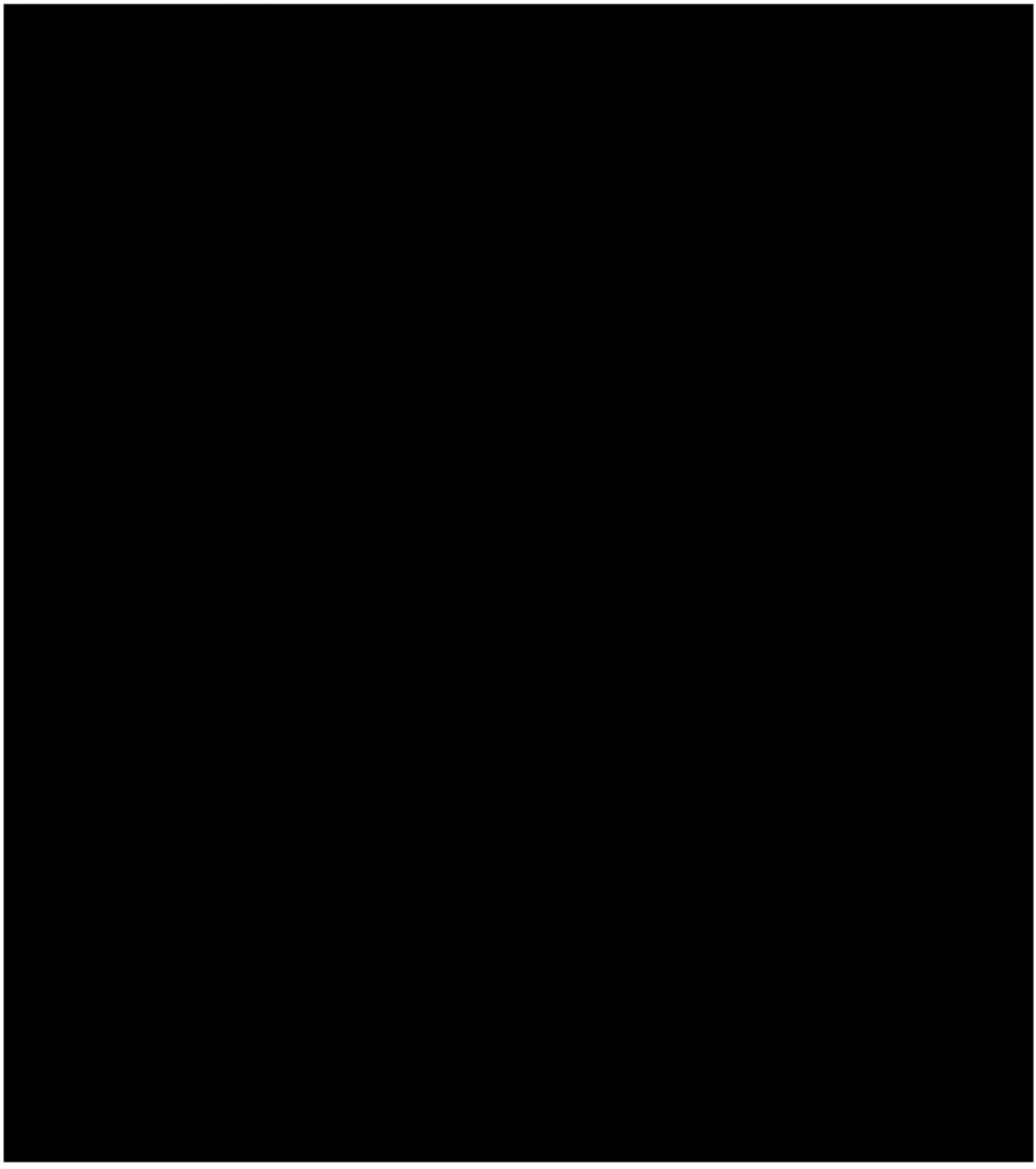


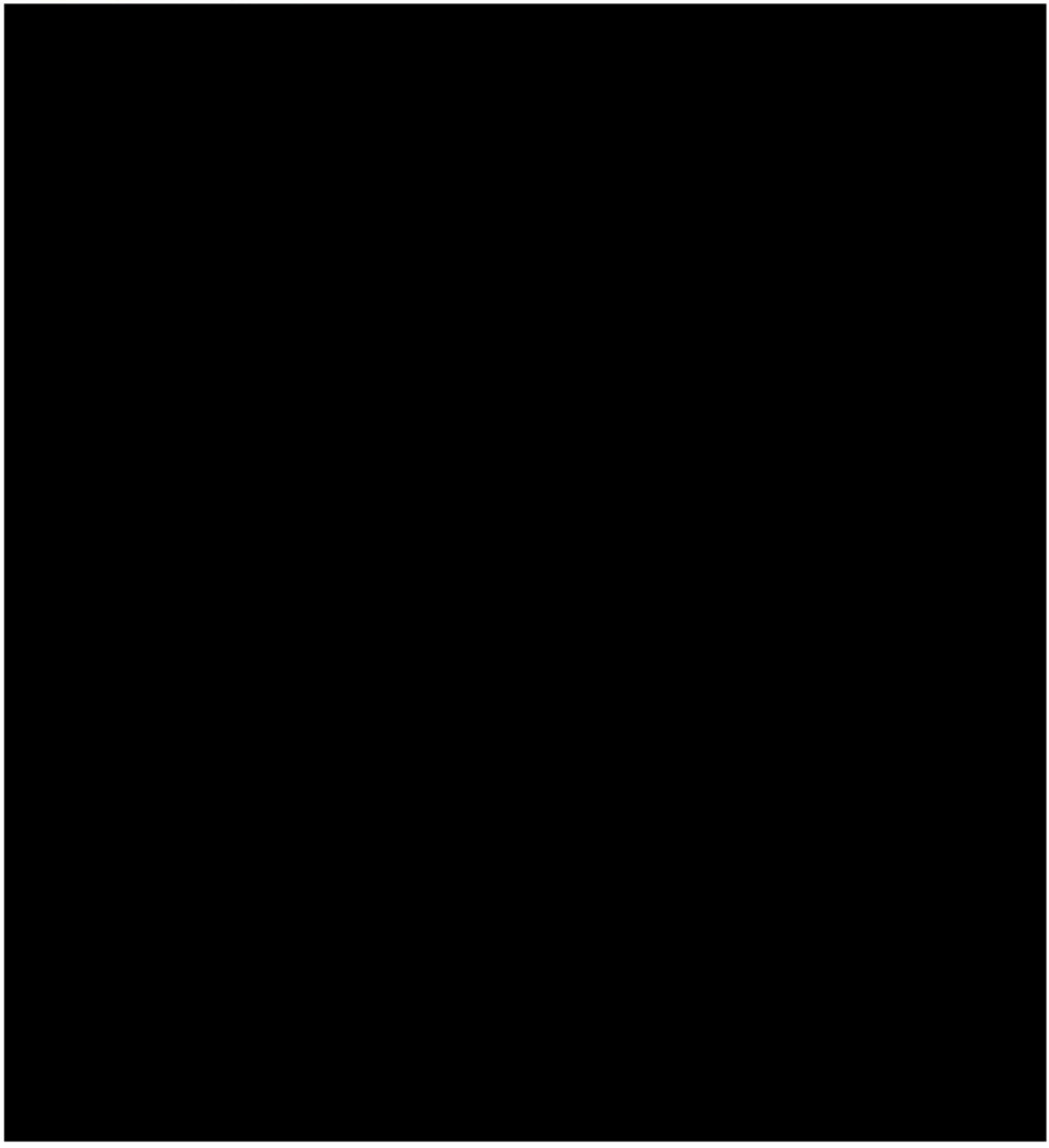


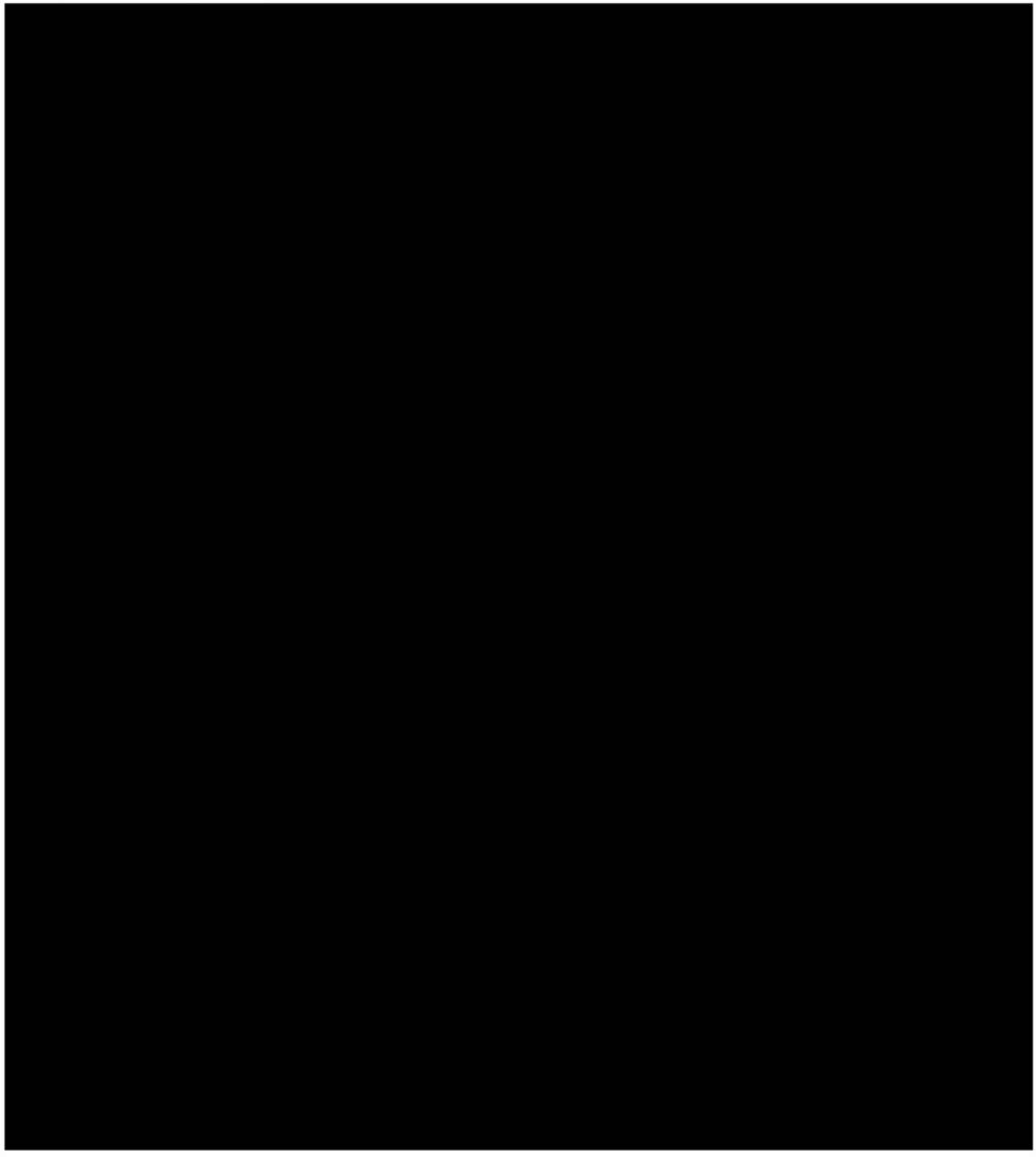


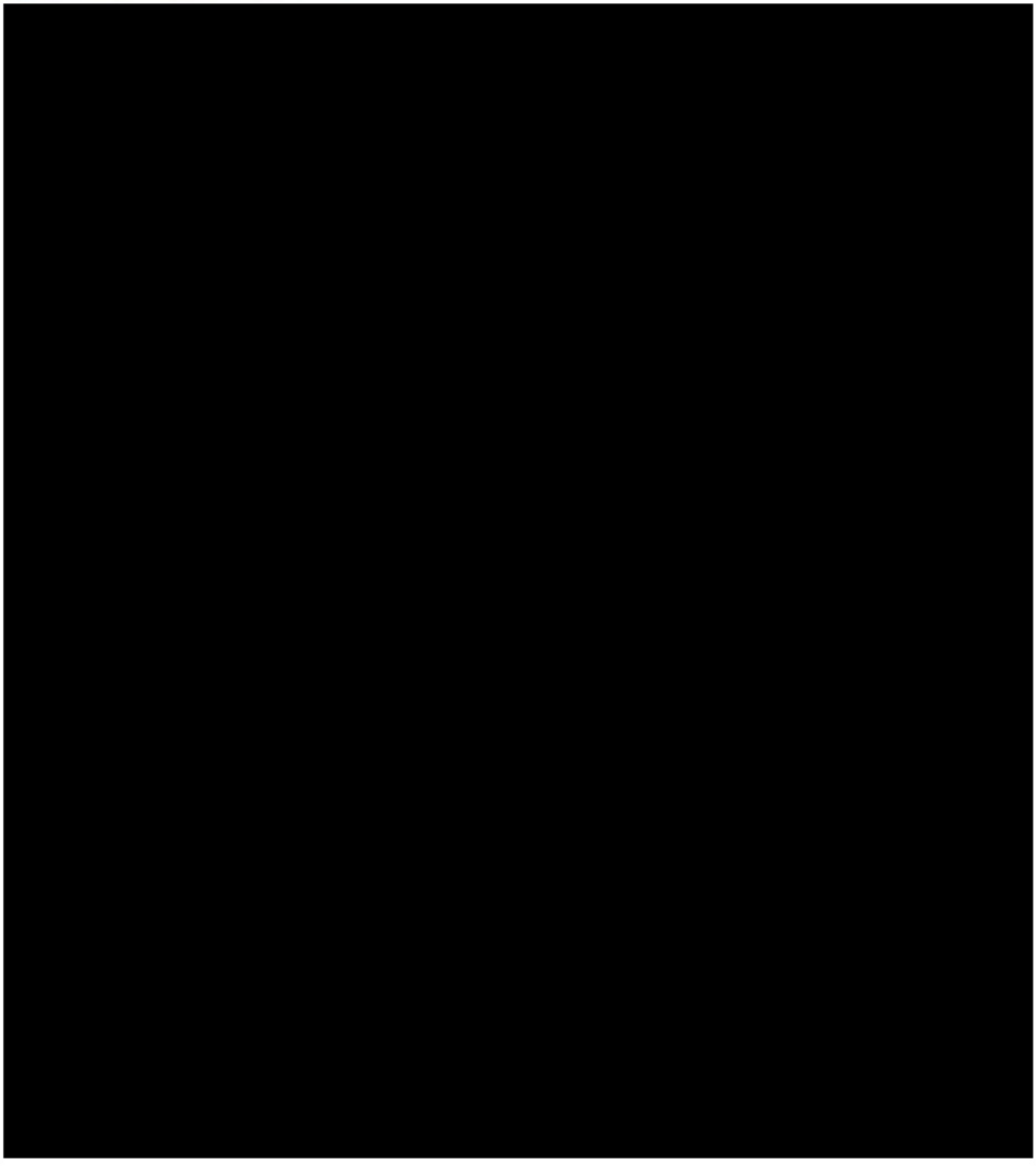


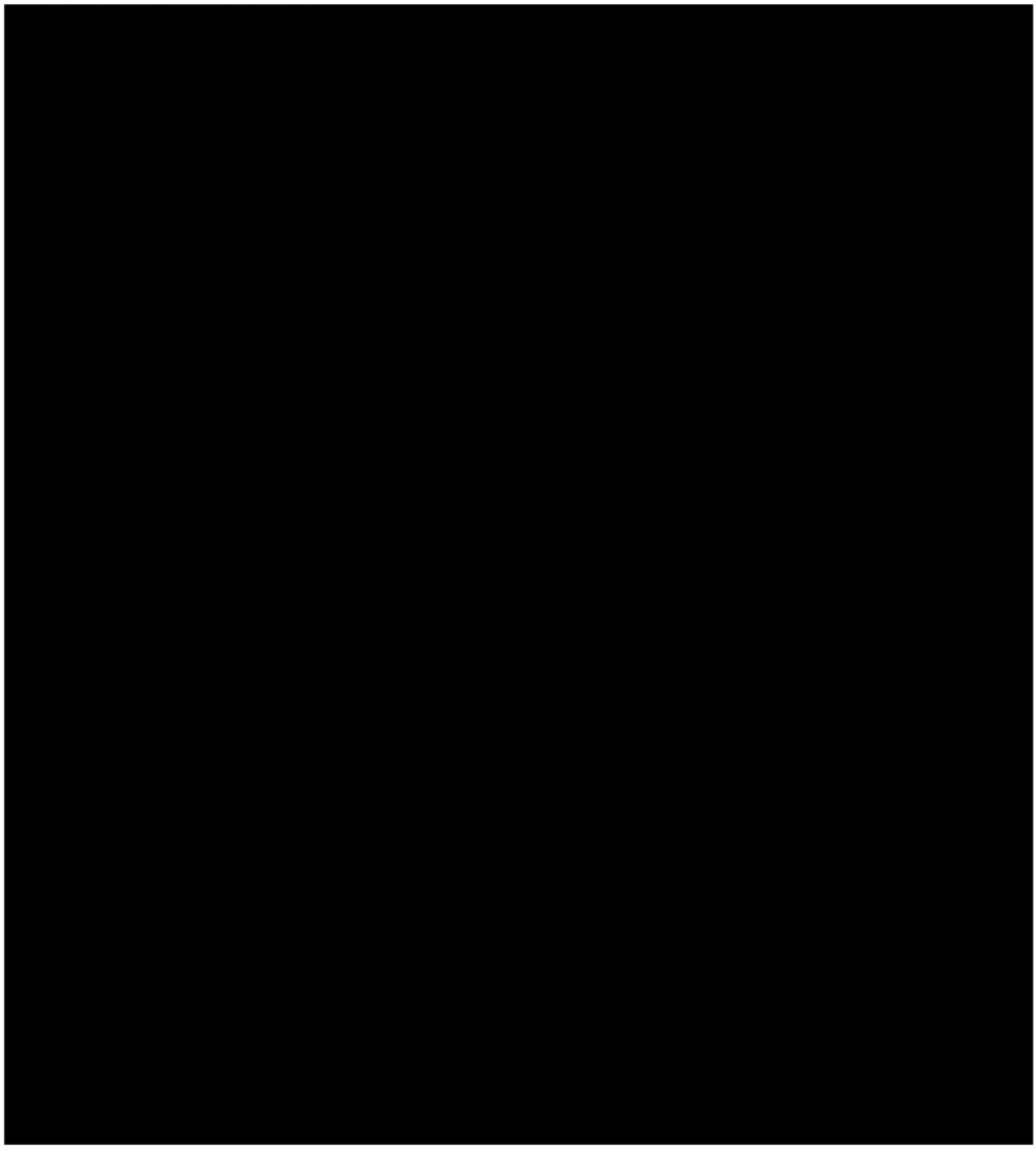


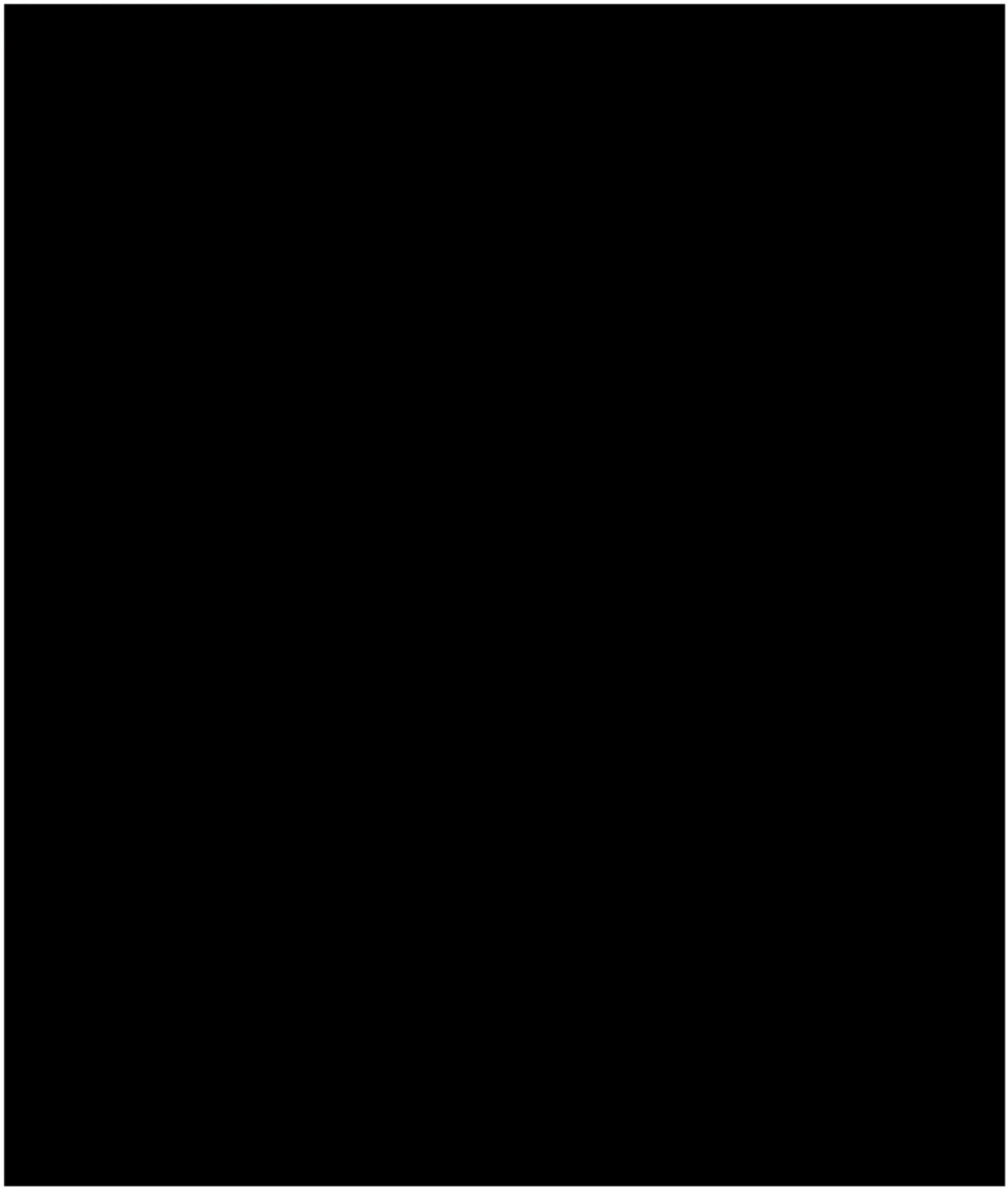


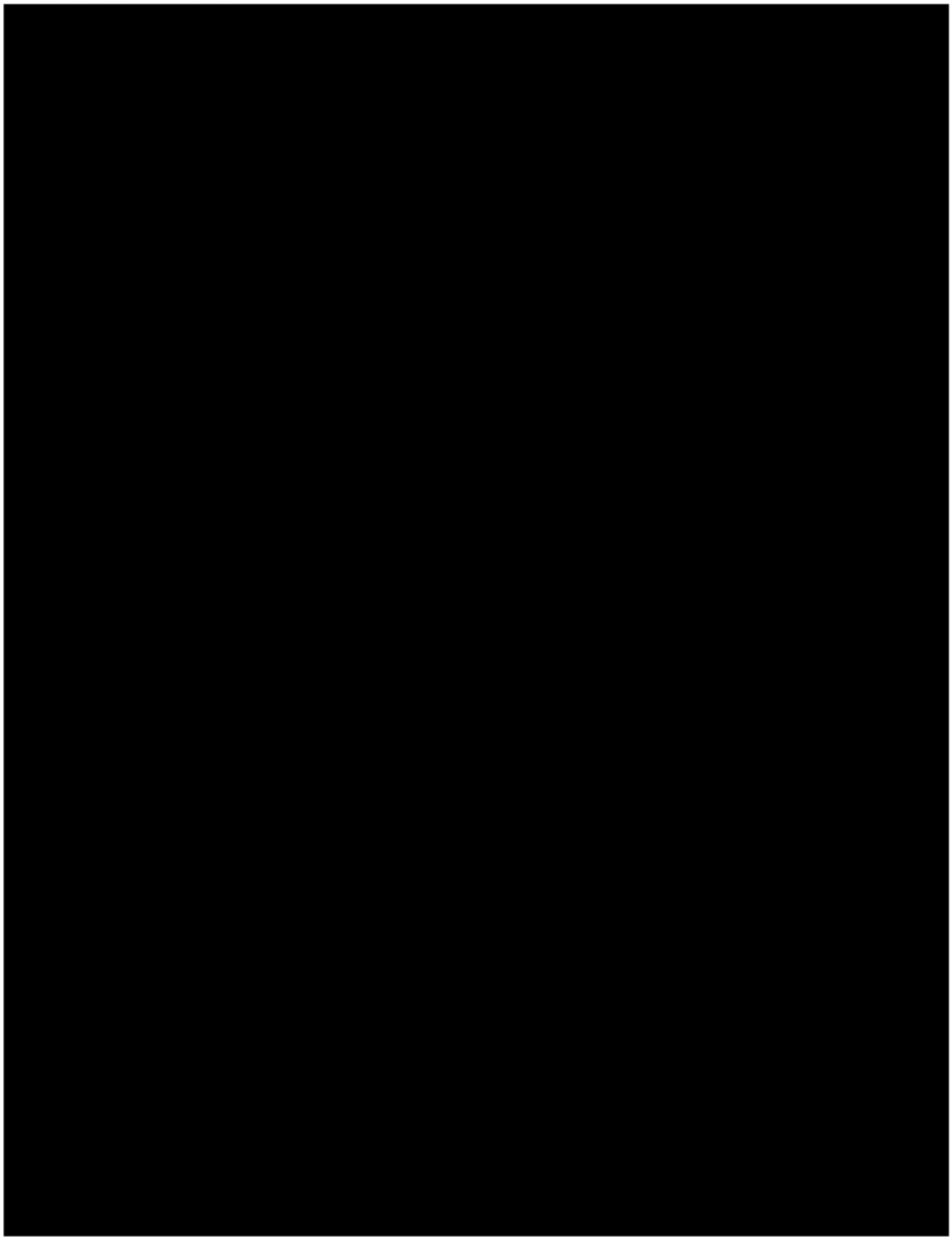


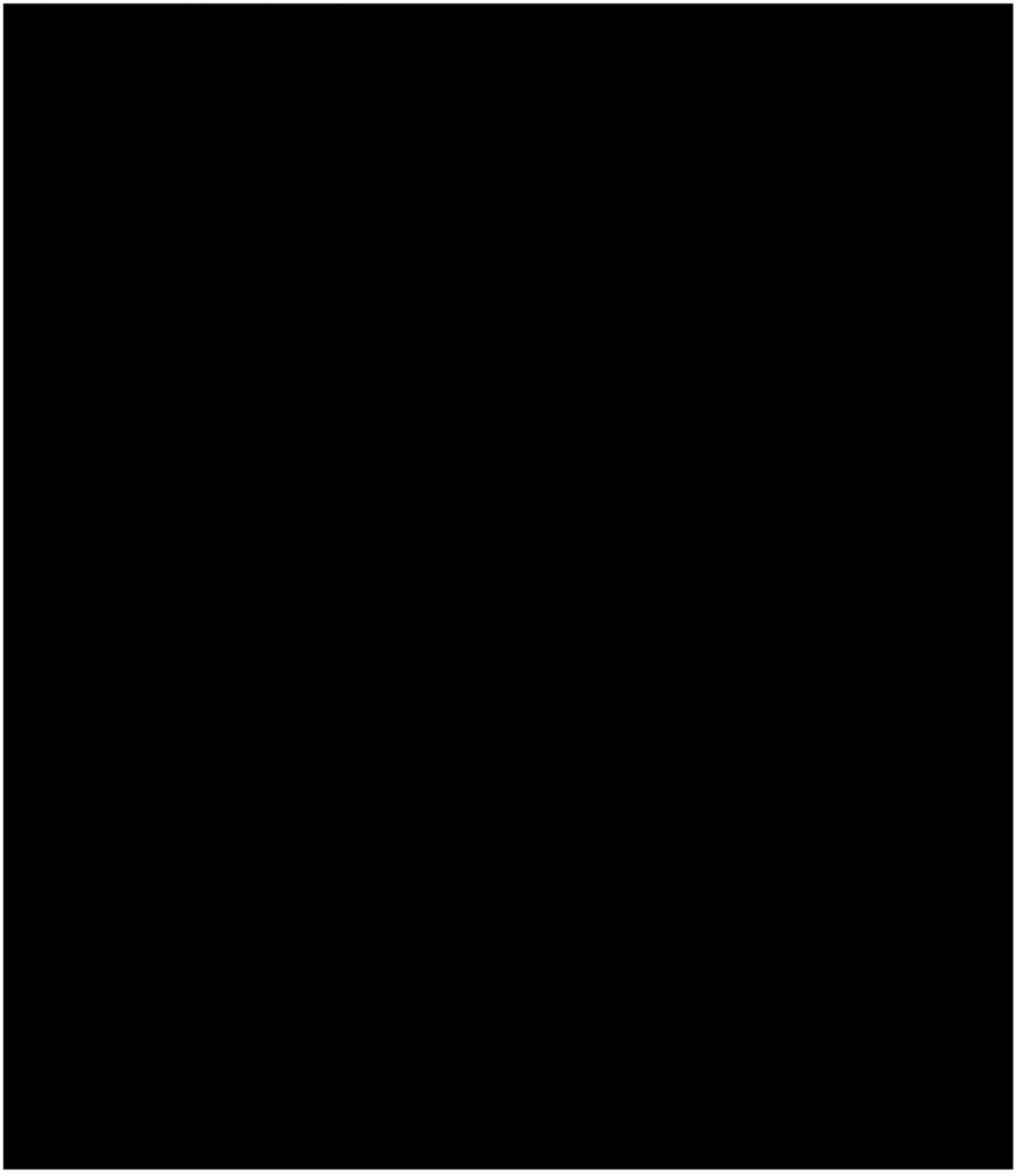


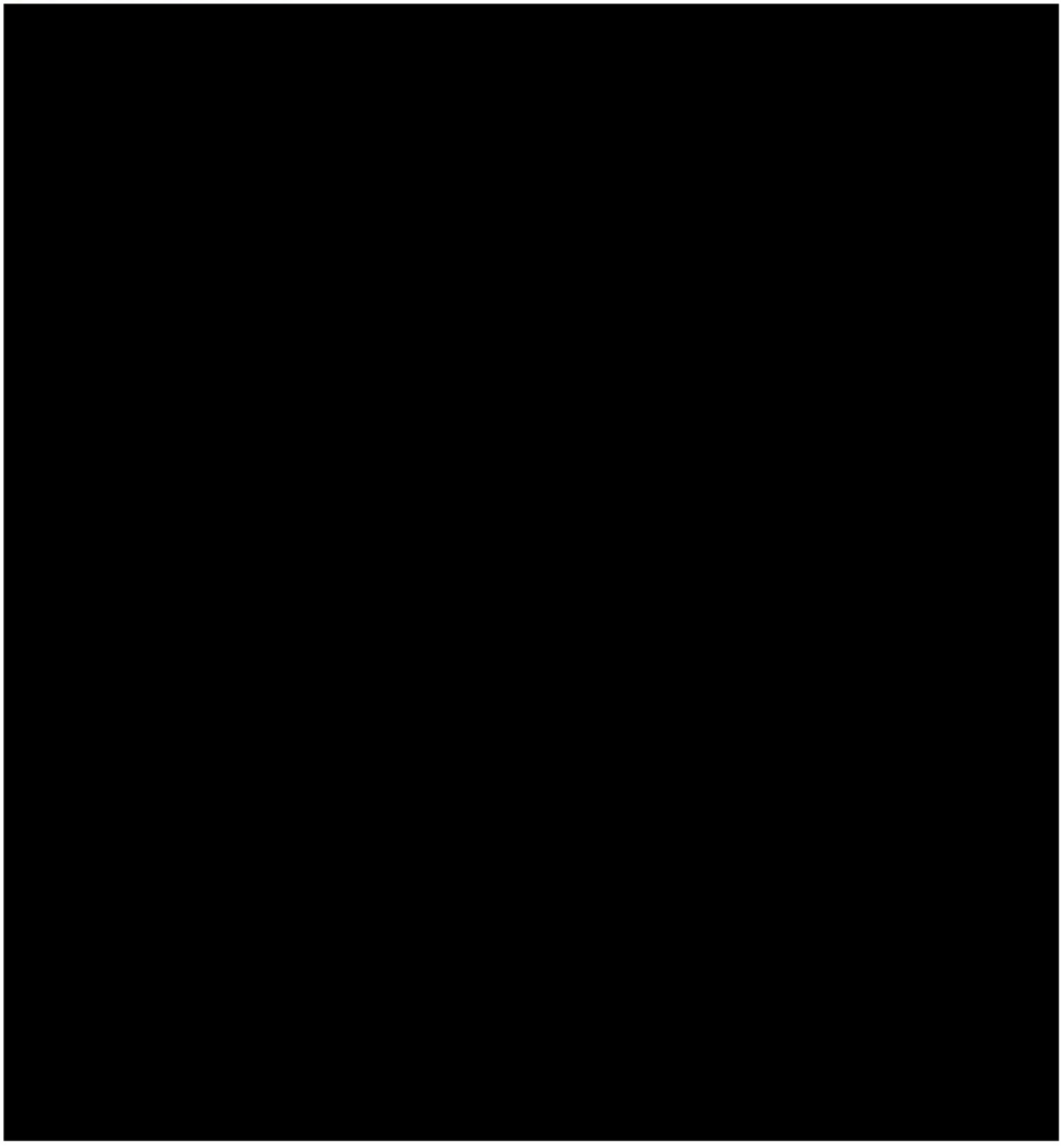


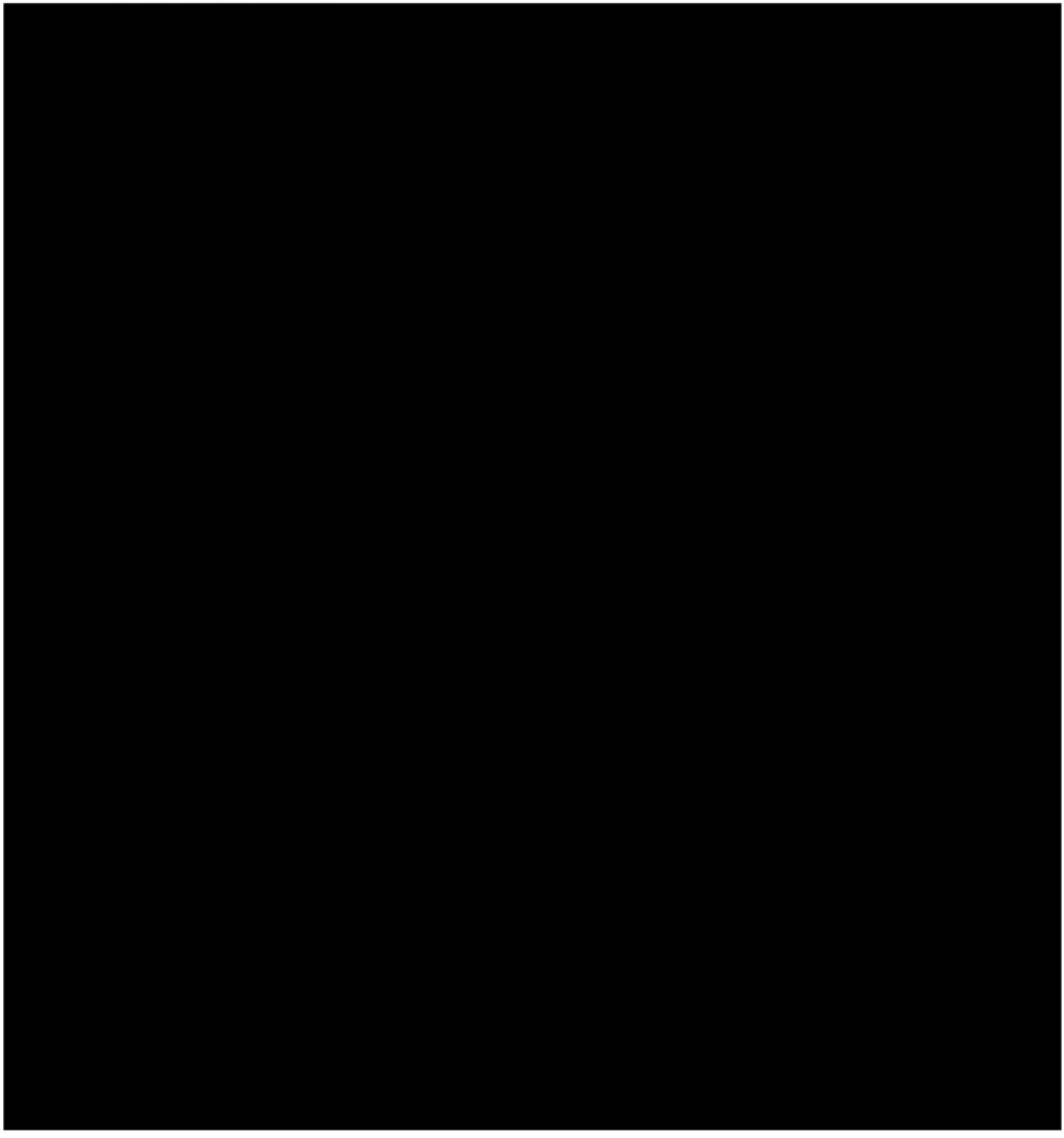


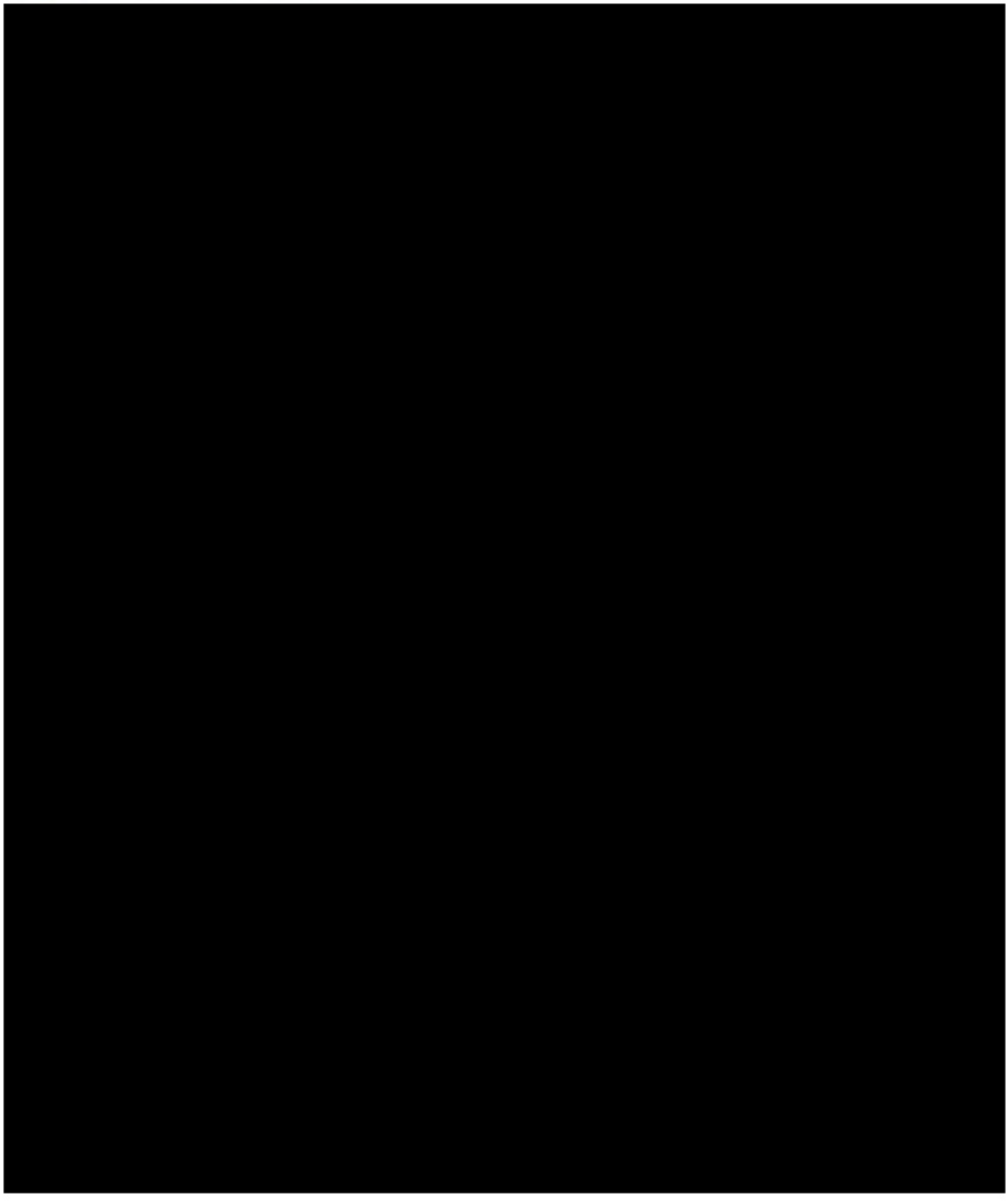


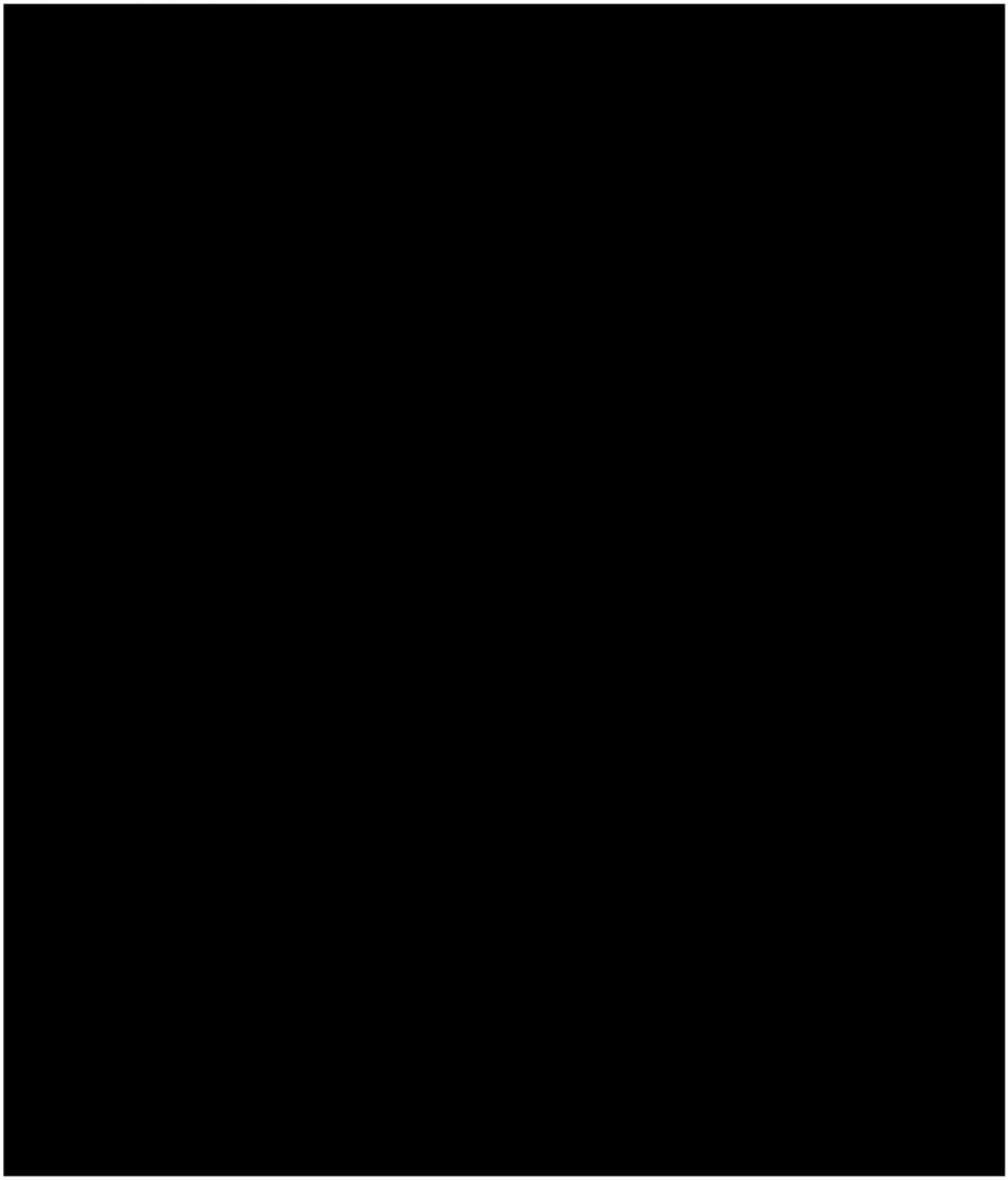


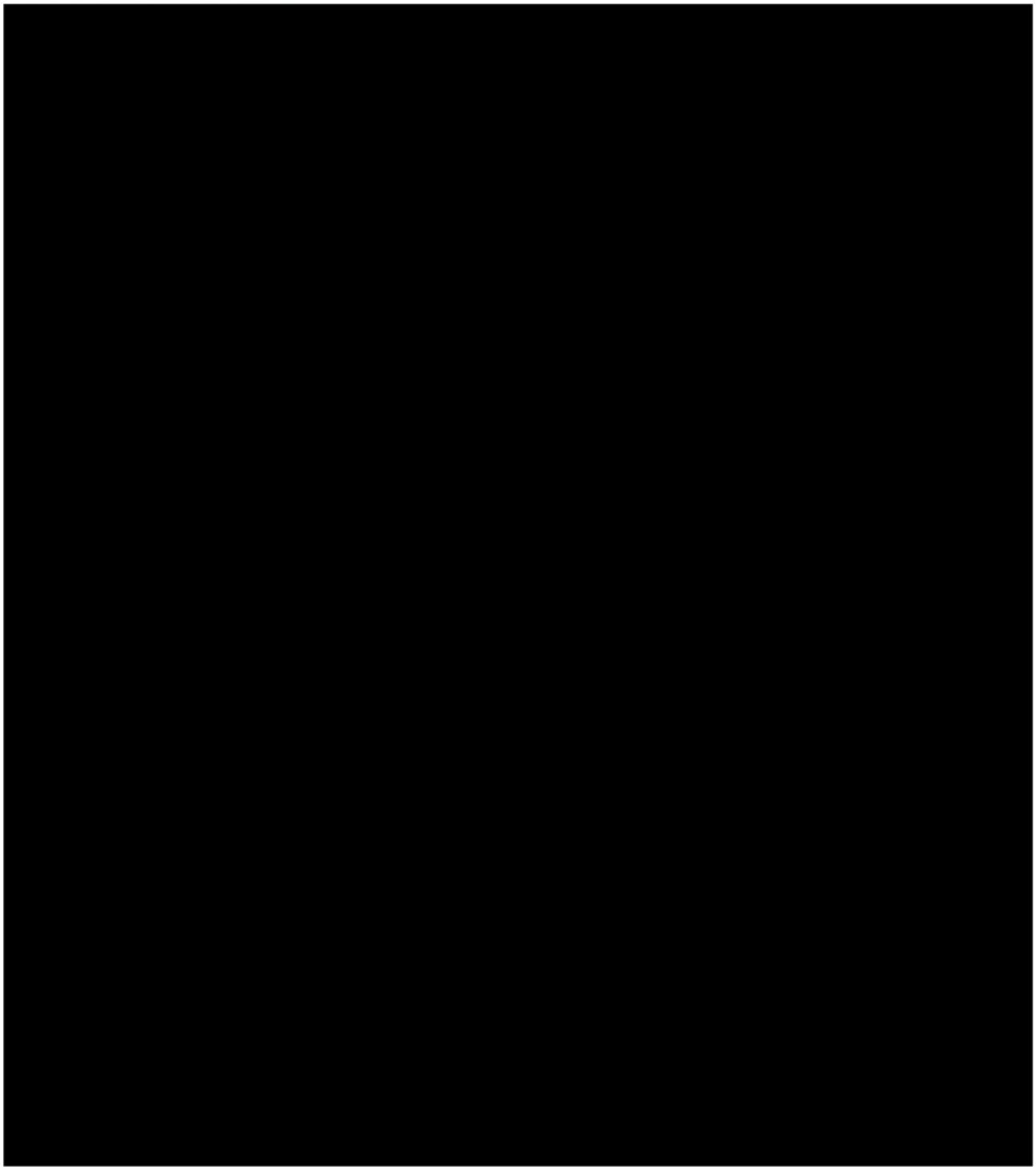


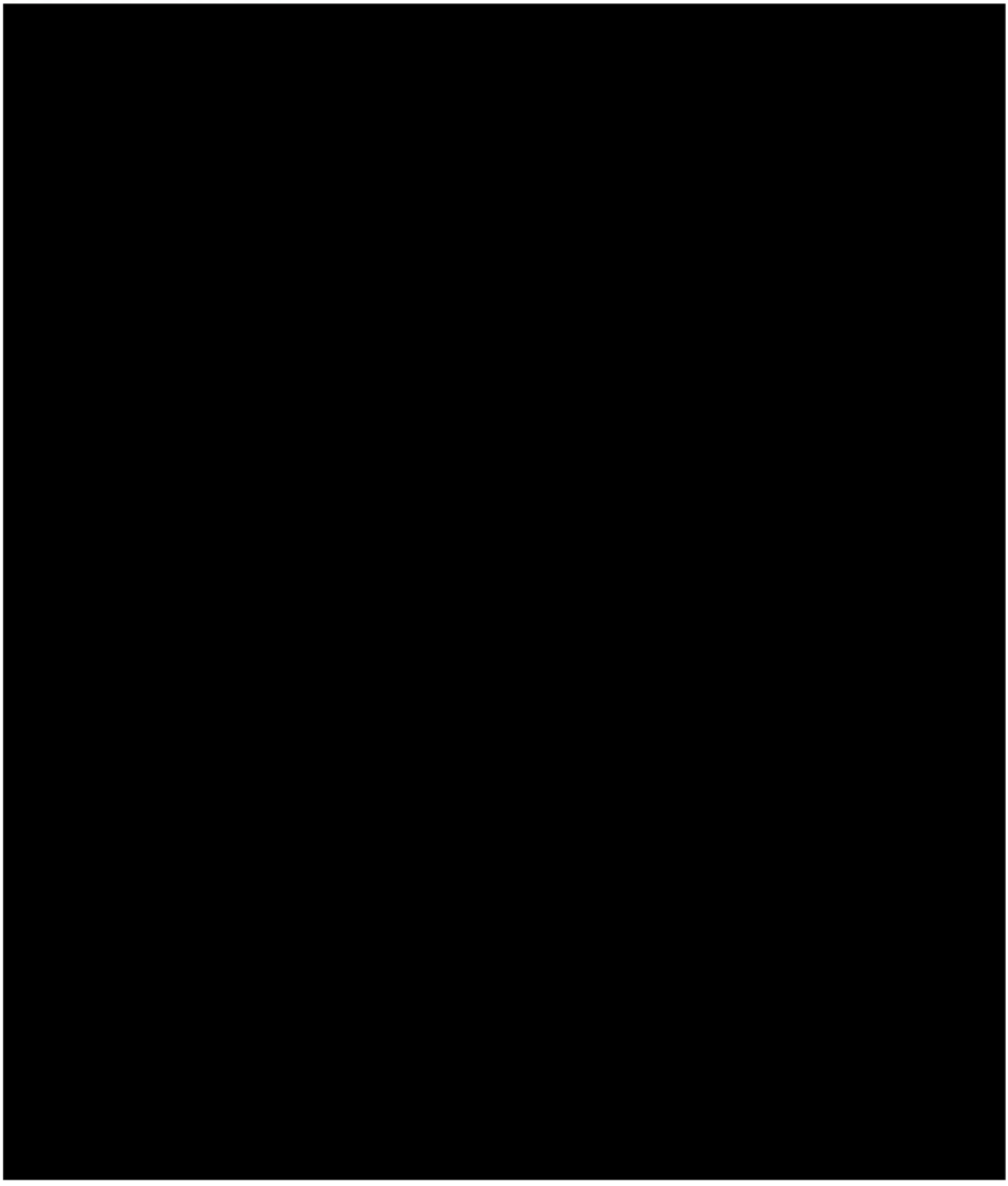


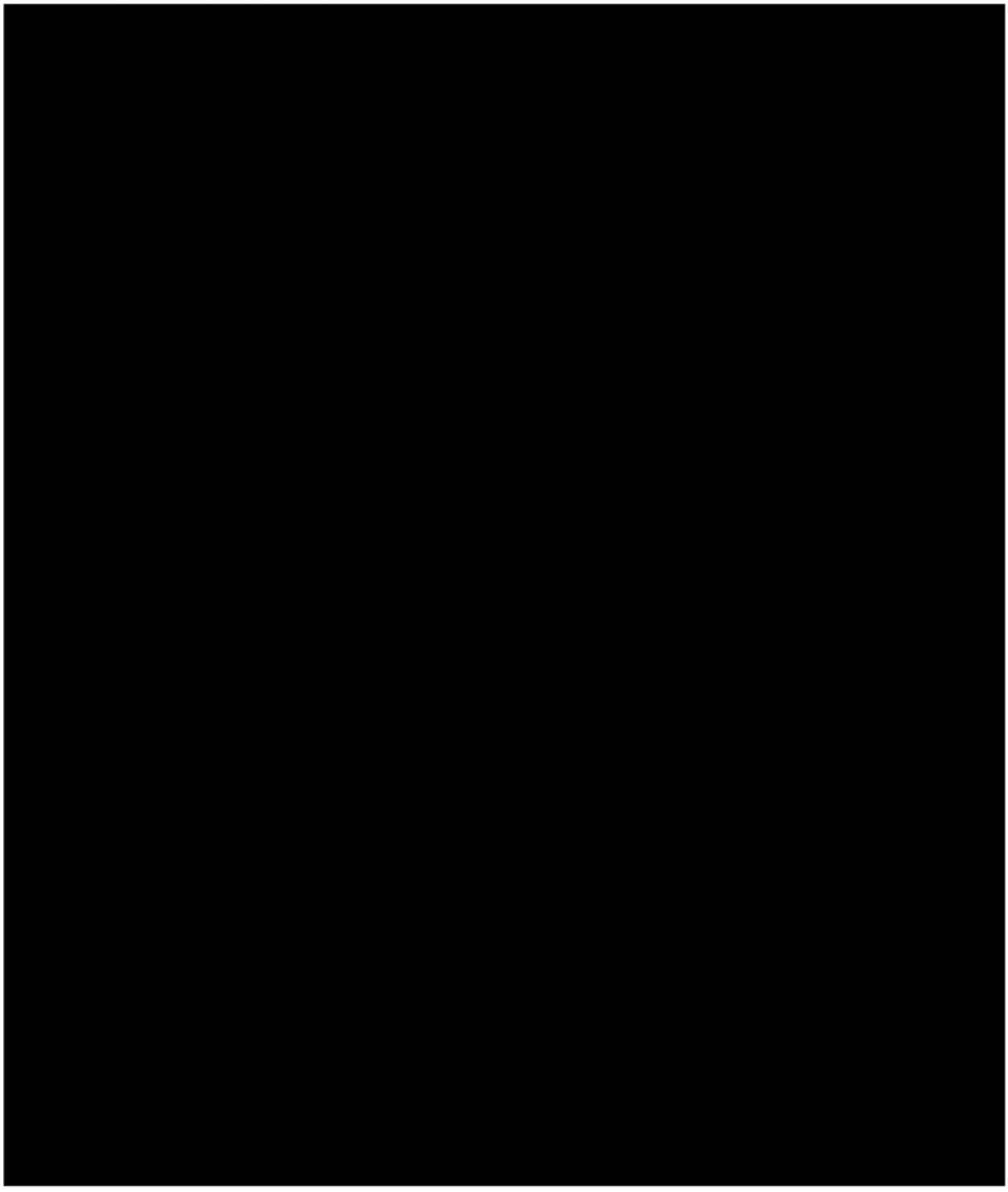


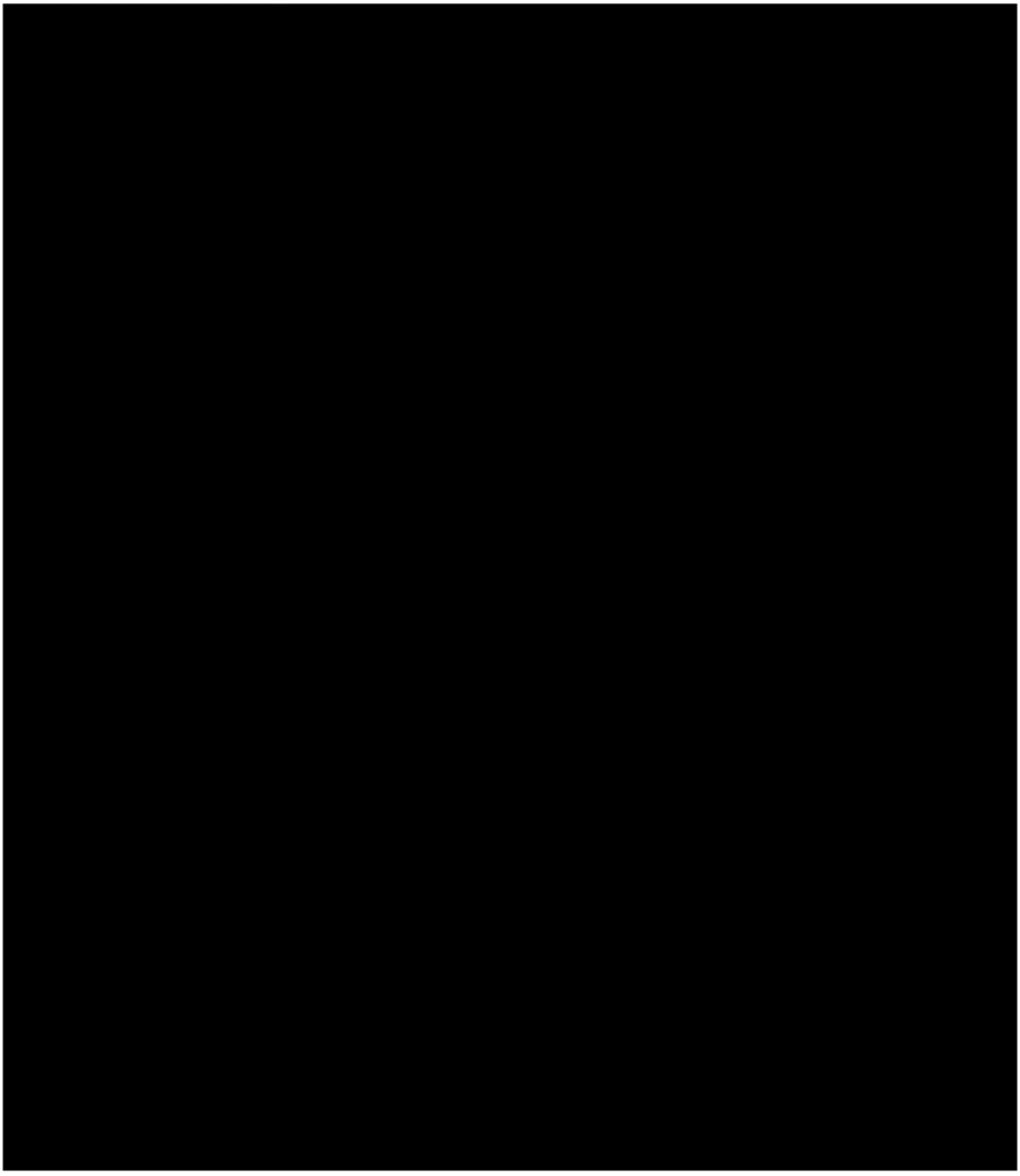












PARTE 5. MEDIDAS DE SEGURIDAD A IMPLEMENTAR

A. Coordinación de Tecnología a Innovación Educativa - Universidad Abierta y a Distancia de México

A1. Sistema de Gestión Escolar (SIGE)

1. **Medida de seguridad deseada:** Interconexión de los aplicativos de UnADM.

1. Objetivo: Mejorar la seguridad de acceso a los procesos y servicios al interior de la UnADM, interconectando los sistemas mejorando la experiencia de los usuarios y agilizando el acceso, por medio de una plataforma de diseño amigable, que reúna y muestre toda la información de acceso disponible para cada usuario.

a) **Acciones a desarrollar y responsables:** Realizar las adecuaciones y modificaciones al código fuente de los sistemas.

b) **Recursos:**

Profesionales de distintas áreas de TIC's, como:
5 - desarrolladores
1 - integrador gráfico
2 - base de datos
1 - documentador

c) **Parámetro de medición:**

Pruebas de conexión
Pruebas de rendimiento
Pruebas de funcionamiento

d) **Tiempo:** 6 meses

A2. Sistema de Encuestas UnADM

1. Medida de seguridad deseada: Generación de reportes históricos de datos para estadística.

1. Objetivo: Almacenamiento de información para extracción.

a) **Acciones a desarrollar y responsables:** Creación de un nuevo esquema para almacenamiento estático de datos. Acceso restringido al repositorio.

b) **Recursos:**

1 desarrollador
1 base de datos

c) **Parámetro de medición:**

Pruebas de funcionamiento

d) **Tiempo:** 6 meses

PARTE 6. PROGRAMA GENERAL DE CAPACITACIÓN

Coordinación de Tecnología a Innovación Educativa – Universidad Abierta y a Distancia de México

Presentar a la unidad administrativa responsable de la capacitación en la Institución, una propuesta para que se integren al programa de capacitación institucional, los cursos necesarios en materia de transparencia, acceso a la información y protección de datos personales, así como de seguridad de la información, con el propósito de difundir los conceptos e importancia, para desarrollar la cultura respecto a las leyes que el INAI tutela, así como en materia de archivos y respecto a la seguridad de la información.

a) Concientización: Llevar a cabo programas a corto plazo para la difusión en general de la protección de datos personales en la organización y su importancia en el entorno laboral. Mediante las siguientes herramientas.
   - Correos electrónicos de parte del Comité de Ética que se envían a los colaboradores de la UnADM.
   - Infografías con diagramas visuales que aportan de manera resumida información respecto a las leyes y su cumplimiento.

b) Entrenamiento: Llevar a cabo programas mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales. Mediante las siguientes herramientas.
   - Webinars institucionales los cuales abordan de manera específica ciertos temas de transparencia y protección de datos personales, así como seguridad de la información. Los webinars cuentan con foros de discusión y son impartidos en diferentes ocasiones durante el año.

c) Educación: programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de la organización. Mediante las siguientes herramientas.
   - Cursos INAI. Esta capacitación se sustenta en las acciones de capacitación que propone el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Los cursos se realizarán en forma continua en los meses julio y agosto de cada año
La modalidad de estudio puede ser presencial / en línea

A continuación, se enlistan lo cursos y sus contenidos:

- Ley General de Transparencia y Acceso a la Información Pública.

Temario
- Conceptos y definiciones básicas
- El Derecho de Acceso a la Información como derecho humano. Una breve perspectiva histórica.
- Desarrollo de la legislación en materia de Transparencia y Acceso a la Información en México
- Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
- Disposiciones generales
- Responsables en materia de transparencia y acceso a la información
- Plataforma Nacional de Transparencia
- Cultura de transparencia y apertura gubernamental
- Obligaciones de transparencia
- Información clasificada
- Procedimientos de acceso a la información pública
- De los procedimientos de impugnación en materia de acceso a la información pública
- Medidas de apremio y sanciones

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
  Temario
  - Función de las Instituciones para la protección de datos personales
  - Manejo de datos personales. Obligaciones de los responsables
  - Derechos para la protección de datos personales y su ejercicio
  - Responsabilidades y Sanciones
- Ley General de Archivos.
  Temario
  - El contexto de la Ley General de Archivos
  - La gestión documental y la administración de archivos
  - La valoración y conservación de archivos
  - El Sistema Nacional de Archivos y su coordinación con los Sistemas Nacionales de Transparencia, Acceso a la Información y Protección de Datos Personales; y el Sistema Nacional Anticorrupción
  - Las obligaciones y sanciones en materia de archivos

PARTE 7. PLAN DE TRABAJO

Coordinación de Tecnología a Innovación Educativa - Universidad Abierta y a Distancia de México

APROBACIÓN DEL DOCUMENTO DE SEGURIDAD

Responsable del desarrollo:

- Nombre: Claudia del Socorro Lara Martínez
- Prestadora de servicios profesionales por honorarios responsable de Ciberseguridad
- Teléfono: 55 3600 2500 ext. 69256
- Correo electrónico institucional: claudia.lara@nube.unadmexico.mx

- Nombre: Eduardo Méndez Santiago
- Prestador de servicios profesionales por honorarios responsable de Ciberseguridad
- Teléfono: 55 3600 2500 ext. 69256
- Correo electrónico institucional: eduardo.mendez@nube.unadmexico.mx

Revisó:

- Nombre: Moisés Alvarado Hermida
- Prestador de servicios profesionales por honorarios responsable de Desarrollo y Base de Datos
- Teléfono: 55 3600 2500 ext. 69256
- Correo electrónico institucional: moises.alvarado@nube.unadmexico.mx

- Nombre: César Gerardo Waldo González
- Prestador de servicios profesionales por honorarios responsable de Infraestructura
- Teléfono: 55 3600 2500 ext. 69147
- Correo electrónico institucional: cesar.waldo@nube.unadmexico.mx

- Nombre: Miguel Castillo García
- Prestador de servicios profesionales por honorarios responsable de Mesa de Servicios
- Teléfono: 55 3600 2500 ext. 69256
- Correo electrónico institucional: miguel.castillogar@nube.unadmexico.mx

Autorizó:

- Nombre: Gabriela Charlotte Quiroz Schumann
- Puesto: Coordinadora de Tecnología e Innovación Educativa
- Teléfono: 55 3600 2500 ext. 69247
- Correo electrónico institucional: gabriela.quirozsch@nube.unadmexico.mx

Fecha: 18/03/2022

GLOSARIO DE TÉRMINOS

Activo
En términos generales, un activo es cualquier elemento que representa un valor para la organización.

Amenaza
Circunstancia o evento con la capacidad de causar daño a una organización.

Análisis de brecha
El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) en el artículo 61 señala nueve acciones para la seguridad de los datos personales. La sexta considera el análisis de brecha, el cual es planteado como la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.

Análisis de riesgo
Tanto el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) consideran que se debe contar con un análisis de riesgos de datos personales para identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento como pueden ser, de manera enunciativa más no limitativa: hardware, software, personal del responsable, entre otros.

Aviso de privacidad
Documento que se debe poner a disposición de los titulares de los datos personales de forma física, electrónica o en cualquier otro formato (por ejemplo, sonoro), a través del cual el responsable informa sobre los propósitos para los cuales serán tratados sus datos personales.

Base de datos
Según la normatividad mexicana, una base de datos es un conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Ciclo de vida de datos personales

Los datos personales —como cualquier tipo de información— están sometidos a un ciclo de vida conformado por diversas fases. Se identifican seis fases que constituyen el ciclo de vida de la información, las cuales son:
1) planear
2) diseñar
3) construir/adquirir
4) usar/operar
5) monitorear
6) eliminar

Confidencialidad de la información
La confidencialidad es un atributo de la información y al mismo tiempo un principio de seguridad que hace referencia a la obligación de que las personas que tienen acceso a ésta apliquen y respeten determinadas reglas y procedimientos a fin de que sea protegida de su divulgación no autorizada a terceros y se garantice que solo el personal autorizado pueda acceder a la misma.

Control
Mecanismo que permite alcanzar los objetivos organizacionales, y posibilita que todos los incidentes no deseados sean prevenidos, detectados y corregidos.
Medio para gestionar riesgos, incluye políticas, procedimientos, guías, prácticas o estructuras organizacionales.

Contenedor
Ubicación en donde los activos son almacenados, transportados o procesados, es decir, es el lugar en donde “vive” el activo.
Los contenedores son puntos vulnerables, susceptibles a amenazas y ataques que ponen en riesgo dichos activos
Técnicos: hardware, software, aplicaciones, servidores, redes.
Físicos: archiveros, papel.
Humanos: personal de la organización.

Dato personal
El concepto “dato personal” es el punto de partida de las normatividades en México en la materia de protección de datos personales. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) define el concepto de dato personal como “cualquier información concerniente a una persona física identificada o identificable”.

Dato personal sensible
Son aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

Deber de confidencialidad
La confidencialidad es la propiedad que posee un objeto, acción, pensamiento, idea, información o cualquier ente de no ser divulgado o expuesto a entidades no autorizadas. En el caso de la información, constituye una de las piedras angulares junto con la integridad y la disponibilidad de lo que es la seguridad de la información, características conocidas como la triada de la seguridad.
Por otro lado, el deber de confidencialidad es la obligación que tiene una entidad de resguardar la confidencialidad de lo que tiene bajo responsabilidad o custodia.

Deber de seguridad
Un pilar básico para una efectiva protección de los datos personales es la implementación de un Sistema de Gestión, que permita planificar, implementar, monitorear y mejorar las medidas de seguridad de carácter administrativo, físico y técnico, a través de una serie de actividades interrelacionadas y documentadas tomando en consideración los estándares nacionales e internacionales, en materia de protección de datos personales y seguridad.

Derechos ARCO
El acrónimo ARCO corresponde a los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales. Los derechos ARCO son una garantía del derecho de autodeterminación de las personas como titulares de datos personales que les permite mantener el control y disponer de sus datos personales frente a los responsables pertenecientes al sector público y al privado.

Disponibilidad de la información
Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

Documento de seguridad
Instrumento que describe en forma detallada las medidas de seguridad implementadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales a cargo del responsable.

Encargado
Persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Firewall
Es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. Un firewall puede ser hardware, software o ambos.

GPL

La licencia GNU GPL (GNU General Public License en español Licencia Pública General de GNU) es una licencia de software libre copyleft publicada por la Free Software Foundation. Los usuarios de un programa con licencia GPL son libres para usarlo, acceder al código fuente, modificarlo y distribuir los cambios; siempre que redistribuyan el programa completo (modificado o no modificado) bajo la misma licencia.

Impacto
Medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

Incidente de seguridad
Evento adverso o una violación a la política de seguridad de la información que compromete o puede comprometer la seguridad de la información implícita o explícitamente.

Información
Es un activo esencial para una organización y necesita estar protegido adecuadamente. La información se presenta en varias formas y estados:

Formas: formato digital (archivos electrónicos), en forma física (escrita o impresa), así como información no presentada, como ideas o el conocimiento.

Estados: puede ser almacenada, procesada o transmitida de diferentes maneras, en formato electrónico, verbal o a través de mensajes escritos o impresos.

Integridad de la información
Propiedad de la información para salvaguardar la exactitud y completitud de la información.

Medidas de seguridad
Las medidas de seguridad son elementos de control que tienen el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. En el caso de los datos personales, las medidas de seguridad se implementan a lo largo de su ciclo de vida para evitar que los datos sean expuestos, alterados o bloqueados por personas o entidades no autorizadas. Las medidas de seguridad se clasifican por su naturaleza en:
a) administrativas;
b) operacionales y
c) tecnológicas

Medidas de seguridad administrativas
Acciones encaminadas a la protección de la información y que están relacionadas con la gente y los procesos. Las medidas de seguridad administrativas se categorizan de la siguiente manera:
a) políticas de seguridad;

b) administración de activos;
c) asignación de roles y privilegios;
d) realización de auditorías;
e) contratos y acuerdos legales y
f) concientización y capacitación

Medidas de seguridad físicas
Las medidas de seguridad físicas refieren a todos los controles que tienen como objetivo asegurar el acceso físico a la información y a todo su entorno.

Medidas de seguridad técnicas
Las medidas de seguridad técnicas refieren a todas las acciones apoyadas de infraestructura tecnológica (hardware y software) que intervienen en la creación, procesamiento, transmisión o almacenamiento de la información.

Protección de datos personales
Es el derecho humano que protege a la persona física identificada o identificable frente al tratamiento ilícito de sus datos personales, otorgándole, en la medida de lo posible dado el actual estado de la técnica, la facultad de decidir y controlar de manera libre e informada las condiciones y características del tratamiento de sus datos personales, permitiéndole, además, el ejercicio de determinados derechos y medios de tutela jurídicos para garantía y eficacia práctica de estos últimos.

Responsable del tratamiento
Personas físicas o morales “que deciden sobre el tratamiento de los datos personales”, aunque difieren en cuanto a la naturaleza, privada o pública, de quien funge como tal.

Riesgo
El riesgo es la combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de seguridad
Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

Riesgo residual
Riesgo residual=Riesgo-Control

Seguridad de la información
La seguridad de la información se define como el conjunto de reglas (políticas), mecanismos (controles) y acciones (procedimientos) que permiten asegurar la información de una organización sin importar la forma en que esta se represente (escrita, oral, gráfica, electrónica, entre otras). Las tres propiedades que la seguridad de la información busca garantizar son: confidencialidad, integridad y disponibilidad.

Titular de los datos personales
El titular de los datos personales es la persona física a quien corresponden o conciernen los datos personales sujetos a tratamiento y por tanto es a quien se considera como sujeto de protección del derecho a la protección de datos personales.

Tratamiento
Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Transferencia
La Ley define a la transferencia como toda comunicación de datos personales dentro o fuera del territorio mexicano realizada a persona distinta del titular, del responsable o del encargado

VLAN
Una red de área local virtual (Virtual Local Area Network), es una tecnología a nivel de capa 2 del modelo de referencia OSI que ayuda a optimizar, proteger y segmentar el tráfico de la red. La capacidad que posee esta tecnología, de ayudar a mejorar el rendimiento de la red, se debe, principalmente, a la creación de dominios de broadcast individuales por cada VLAN creada en el Switch o Router.

VPN (Virtual Private Network)
Es una tecnología de red que sirve para conectar una o más computadoras a una red privada utilizando como medio una red pública como internet, es decir, la Red Privada Virtual permite que estos dispositivos estén conectados entre sí a través de internet de una forma segura, la cual garantiza la integridad y la confidencialidad de la información que se encuentra en dichos dispositivos.

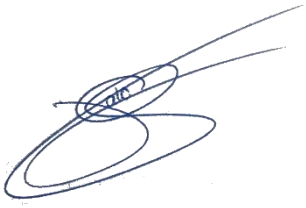
Vulnerabilidad
Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Vulneración de datos personales
La vulneración de datos personales es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales en posesión de las personas físicas o morales que realizan el tratamiento de los datos, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

Firmas de elaboración, revisión y aprobación del Documento de Seguridad para la Protección de Datos Personales

Fecha de Elaboración: 18/03/2022

Universidad Abierta y a Distancia de México

		
Claudia del Socorro Lara Martínez	Eduardo Méndez Santiago	Moisés Alvarado Hermida
Prestadora de servicios profesionales por honorarios responsable de Ciberseguridad	Prestador de servicios profesionales por honorarios responsable de Ciberseguridad	Prestador de servicios profesionales por honorarios responsable de Desarrollo y Base de Datos
claudia.lara@nube.unadmexico.mx	eduardo.mendez@nube.unadmexico.mx	moises.alvarado@nube.unadmexico.mx
3600-2511 Ext. 69256	3600-2511 Ext. 69256	3600-2511 Ext. 69256
Elaboró	**Elaboró**	**Revisó**
		
César Gerardo Waldo González	Miguel Castillo García	Gabriela Charlotte Quiroz Schumann
Prestador de servicios profesionales por honorarios responsable de Infraestructura	Prestador de servicios profesionales por honorarios responsable de Mesa de Servicios	Coordinadora de Tecnología e Innovación Educativa
cesar.waldo@nube.unadmexico.mx	miguel.castillogar@nube.unadmexico.mx	gabriela.quirozsch@nube.unadmexico.mx
3601-2500 Ext. 69147	3601-2500 Ext. 69256	3600-2511 Ext. 69247
Revisó	**Revisó**	**Autorizó**