SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS

SIGA

Documento de seguridad

Junio 2022

Área de sistemas

ai.sistemas@patronato.unam.mx

Presentación

La Auditoría Interna se encarga de vigilar, mediante la práctica de auditorías, revisiones y evaluaciones, el uso eficiente y honesto de los recursos, el cumplimiento de las disposiciones legales y normativas aplicables y el logro de los objetivos en las entidades y dependencias universitarias, en un marco de transparencia y rendición de cuentas.

El presente documento de seguridad contiene las medidas de seguridad administrativa, física y técnica aplicables a los sistemas de tratamiento de datos personales de esta área universitaria con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen.

Sistemas de tratamientos de datos personales.

SIGA

El sistema se encarga de mejorar, modernizar, optimizar y agilizar la ejecución del trabajo de Auditoría Interna, con el fin de que se cuente con elementos que permitan la estandarización de procesos, el seguimiento y supervisión de avances y resultados en tiempo real, la disposición permanente de información actualizada y la simplificación de las actividades, para con ello apoyar de manera más efectiva el logro de los objetivos y mejoras institucionales.

A este sistema tiene acceso todo el personal de la Auditoría Interna que recaba información de sus trabajos.

En el sistema se tiene información de datos personales del personal de la dependencia, de la información que se carga de las auditorías que se realizan a las entidades y dependencias de la Universidad puede o no contener información de datos personales.

El detalle de los datos personales que se manejan en cada componente del sistema se describe en los *Anexos 1 Inventario de sistemas de tratamiento de datos personales*.

Roles y responsabilidades de los involucrados en el tratamiento de datos personales.

SIGA

Los perfiles, detalle con las funciones y responsabilidades de cada perfil de las personas que participan en el tratamiento de datos personales se encuentra en el *Anexo 2 Funciones y obligaciones de quienes traten datos personales*.

Análisis de riesgos en el tratamiento de datos personales.

El detalle del análisis de riesgos está descrito en el *Anexo 3 Análisis de riesgos en el tratamiento de datos personales*.

Análisis de brecha.

Ya identificados los controles necesarios para mitigar los riesgos encontrados en nuestros activos de información, se hace un Análisis de Brecha identificando lo siguiente:

- Medida seguridad actual.
- Medida de seguridad necesaria.
- Acciones para remediación.

El detalle del análisis de riesgos está descrito en el *Anexo 4 Análisis de brecha*.

Plan de trabajo.

Realizado el análisis de riesgos y teniendo identificados los controles faltantes para mitigar los riesgos, se hace un plan para implementar los controles de seguridad faltantes.

El detalle del plan de trabajo está descrito en el *Anexo 5 Plan de trabajo*.

Ruta crítica para cumplimiento de las medidas de seguridad técnicas (MST).

El detalle de las medidas de seguridad técnicas se especifican en el *Anexo 6 Formatos para el cumplimiento de las MST.*

Aprobación del documento de seguridad.

		Nombre y firma de quienes revisaron el presente documento.
Responsable del desarrollo:	Ing. Jonathan Neftali Calderón Díaz Coordinador de informática. Auditoría Interna Tel. 5556226410, Ext 48302 jonathan.calderon@patronato.unam.mx	Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022
Revisó:	L.I. Roberto Carlos Pérez Medina Coordinador de Informática. Auditoría Interna Tel. 5556226410, Ext 48302 carlos.perez@patronato.unam.mx	Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022
Autorizó:	Ing. José Alfredo Montero Rojas Titular de la Auditoría Interna Tel. 5556226410 jose.montero@patronato.unam.mx	Firmado digitalmente por José Alfredo Montero Rojas. Fecha: 30/06/2022

ANEXO 1
INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

AUDITORÍA INTERNA Junio 2022

Auditoría Interna	
Identificador único*	AI – SIGA
(Nombre del sistema A1) *	**Sistema Integral de Gestión de Auditorías (SIGA)**
Datos personales (sensibles o no) contenidos en el sistema*:	1. Datos personales en general **a)** Datos de identificación a. Nombre b. RFC **b)** Datos laborales a. correo electrónico institucional UNAM
Responsable*:	Auditoría Interna
Nombre*:	Ing. José Alfredo Montero Rojas
Cargo*:	Auditor Interno
Funciones*:	Las funciones vienen especificadas en el *Anexo2_Funciones_permisos*.
Obligaciones*:	Proveer los recursos necesarios para establecer, implementar, operar y mantener la protección de datos personales dentro de Auditoría Interna.
	Encargados:
(Nombre del Encargado 1*)	L.I. Roberto Carlos Pérez Medina
Cargo*:	Coordinador de Informática
Funciones*:	Las funciones vienen especificadas en el *Anexo2_Funciones_permisos*.
Obligaciones*:	Determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener la protección de datos personales dentro de Auditoría Interna.
(Nombre del Encargado 2*)	Ing. Jonathan Neftalí Calderón Díaz
Cargo*:	Coordinador de Informática
Funciones*:	Las funciones vienen especificadas en el Anexo2_Funciones_permisos.
Obligaciones*:	Determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener una cultura de protección de datos personales dentro de la organización.
	Usuarios:
(Nombre del Usuario 1*)	
Cargo*:	
Funciones*:	
Todos los usuarios que actualmente utilizan el siga se encuentran en el documento anexo "*SIGA_USUARIOS_ANEXO*".	

Auditoría Interna	
Identificador único*	AI – SIGA
(Nombre del sistema A1) *	**Sistema Integral de Gestión de Auditorías (SIGA)**
Datos personales (sensibles o no) contenidos en el sistema*:	1. Datos personales en general **c)** Datos de identificación a. Nombre b. RFC **d)** Datos laborales a. correo electrónico institucional UNAM
Responsable*:	Auditoría Interna
Nombre*:	Ing. José Alfredo Montero Rojas
Cargo*:	Auditor Interno
Funciones*:	Las funciones vienen especificadas en el *Anexo2_Funciones_permisos*.
Obligaciones*:	Proveer los recursos necesarios para establecer, implementar, operar y mantener la protección de datos personales dentro de Auditoría Interna.
	Encargados:
(Nombre del Encargado 1*)	L.I. Roberto Carlos Pérez Medina
Cargo*:	Coordinador de Informática
Funciones*:	Las funciones vienen especificadas en el *Anexo2_Funciones_permisos*.
Obligaciones*:	Determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener la protección de datos personales dentro de Auditoría Interna.
(Nombre del Encargado 2*)	Ing. Jonathan Neftalí Calderón Díaz
Cargo*:	Coordinador de Informática
Funciones*:	Las funciones vienen especificadas en el *Anexo2_Funciones_permisos*.
Obligaciones*:	Determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener una cultura de protección de datos personales dentro de la organización.
	Usuarios:
(Nombre del Usuario 1*)	
Cargo*:	
Funciones*:	
Todos los usuarios que actualmente utilizan el siga se encuentran en el documento anexo "*Anexo6_Usuarios_SIGA*".	

2. ESTRUCTURA Y DESCRIPCIÓN DE LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

Auditoría Interna	
Identificador único¨*	AI – SIGA
(Nombre del sistema A1*)	**Sistema Integral de Gestión de Auditorías (SIGA)**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos relacional
Características del lugar donde se resguardan los soportes:*	Oficina con ventilación natural y aire acondicionado, luz natural y artificial, Site con puerta de acceso de aluminio con cristal y chapa, con muebles que permiten la conservación adecuada del servidor que aloja el sistema.
Auditoría Interna	
Identificador único¨*	AI – SIGA
(Nombre del sistema A1*)	**Sistema Integral de Gestión de Auditorías (SIGA)**
Tipo de soporte:*	Electrónico
Descripción:*	Base de datos relacional
Características del lugar donde se resguardan los soportes:*	Oficina con ventilación natural y aire acondicionado, luz natural y artificial, puerta de acceso de madera y chapa, con escritorios y muebles que permiten la conservación adecuada del servidor que aloja el sistema.

ANEXO 2
FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

AUDITORÍA INTERNA Junio 2022

Permisos registrados en el SIGA:

Permiso	Abreviación
Crear usuario	CU
Editar usuario	EU
Habilitar usuario	HU
Inhabilitar usuario	IHU
Registrar trabajo programado	RTP
Editar trabajo programado	ETP
Cancelar trabajo programado	CTP
Suspender trabajo programado	STP
Activar trabajo programado	ATP
Solicitar validación del responsable en trabajo programado	SVRTP
Otorgar la validación del responsable en trabajo programado	OVRTP
Negar la validación del responsable en trabajo programado	NVRTP
Registrar trabajo no programado	RTNP
Editar trabajo no programado	ETNP
Cancelar trabajo no programado	CTNP
Suspender trabajo no programado	STNP
Activar trabajo no programado	ATNP
Solicitar validación del responsable en trabajo no programado	SVRTNP
Otorgar la validación del responsable en trabajo no programado	OVRTNP
Negar la validación del responsable en trabajo no programado	NVRTNP
Registrar observación	RO
Editar observación	EO
Eliminar observación	ELO
Registrar seguimiento	RS
Editar seguimiento	ES
Generar número de oficio	GNO
Generar reporte de transparencia	GRT
Generar reporte de avance de trabajo	GRAT
Administrar grupo de trabajo	AGT
Cargar archivos testados	CAT
Registrar elemento de catálogo	REC
Editar elemento de catálogo	EEC
Habilitar elemento de catálogo	HEC
Inhabilitar elemento de catálogo	IHEC
Registrar archivos complementarios	RAC
Eliminar archivos complementarios	EAC
Validar desde archivos complementarios	VAC
Invalidar desde archivos complementarios	IVAC
Solicitar validación de transparencia en trabajo programado	SVTTP

Otorgar la validación de transparencia en trabajo programado	OVTTP
Negar la validación de transparencia en trabajo programado	NVTTP
Solicitar validación de transparencia en trabajo no programado	SVTTNP
Otorgar la validación de transparencia en trabajo no programado	OVTTNP
Negar la validación de transparencia en trabajo no programado	NVTTNP
Registrar primer grupo de trabajo	RPGT
Consultar archivos testados	COAT
Cancelar número del oficio	CON
Solicitar número de oficio	SON
Cambiar responsable del trabajo	CRT
Consultar correspondencia de entrada	CCE
Descargar reporte de correspondencia de entrada	DRCE
Registrar correspondencia de entrada	RCE
Reasignar responsable	RR
Turnar correspondencia	TC
Cambiar fecha de recepción de correspondencia.	CFRC
Recibir correspondencia	RC

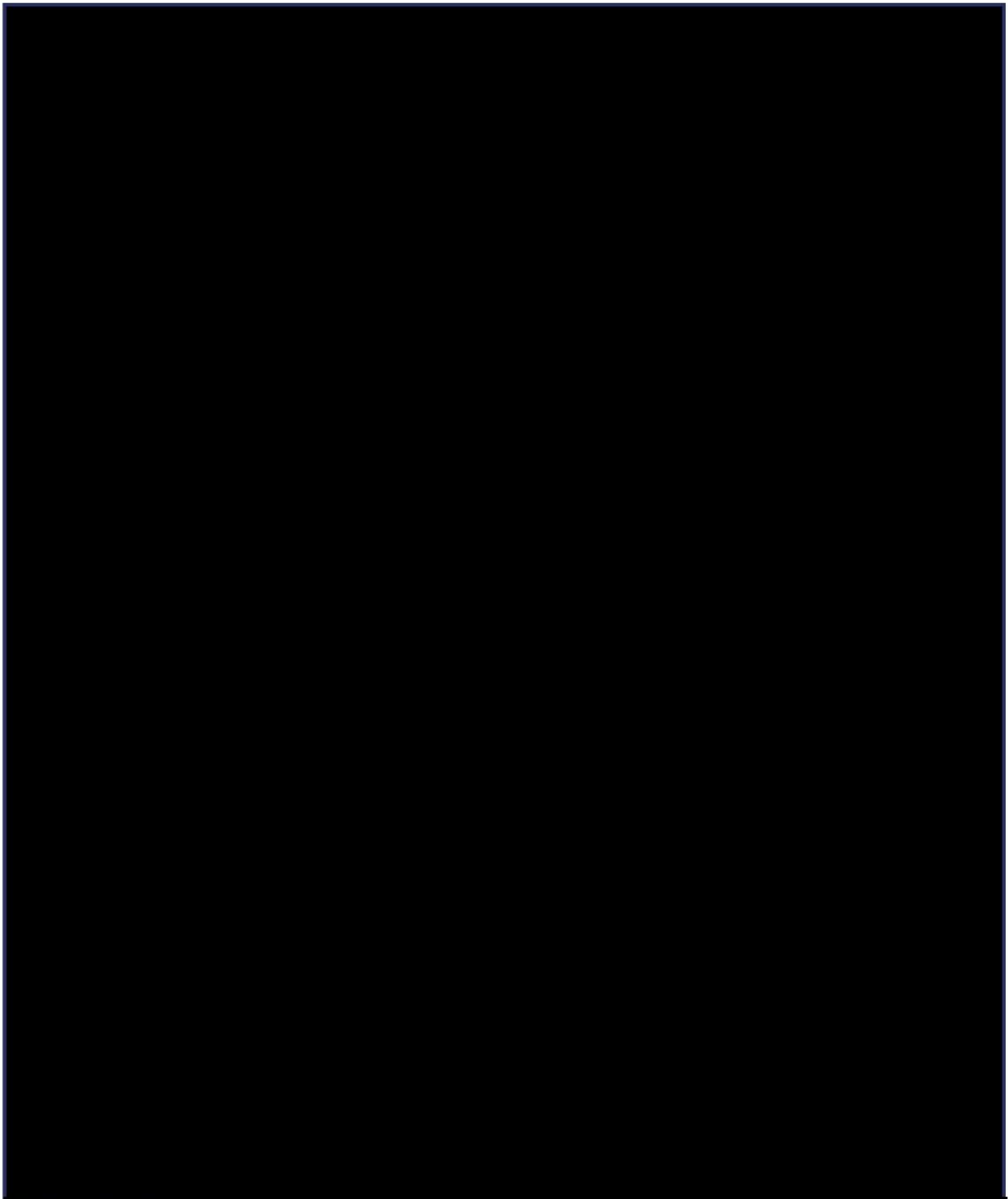
Perfiles registrados en el SIGA.

Perfil	Abreviación
Coordinador administrador	CA
Auditor interno	AI
Director de área	DA
Jefe de departamento	JD
Jefe de proyectista	JP
Coordinador	CO
Jefe de grupo	JG
Auditor	AU
Jefe de departamento de transparencia	JDT
Jefe de grupo de transparencia	JGT
Coordinador de recursos humanos	CRH
Auditor administrador	AA
Jefe de grupo coordinador	JGC
Pool secretarial	PS

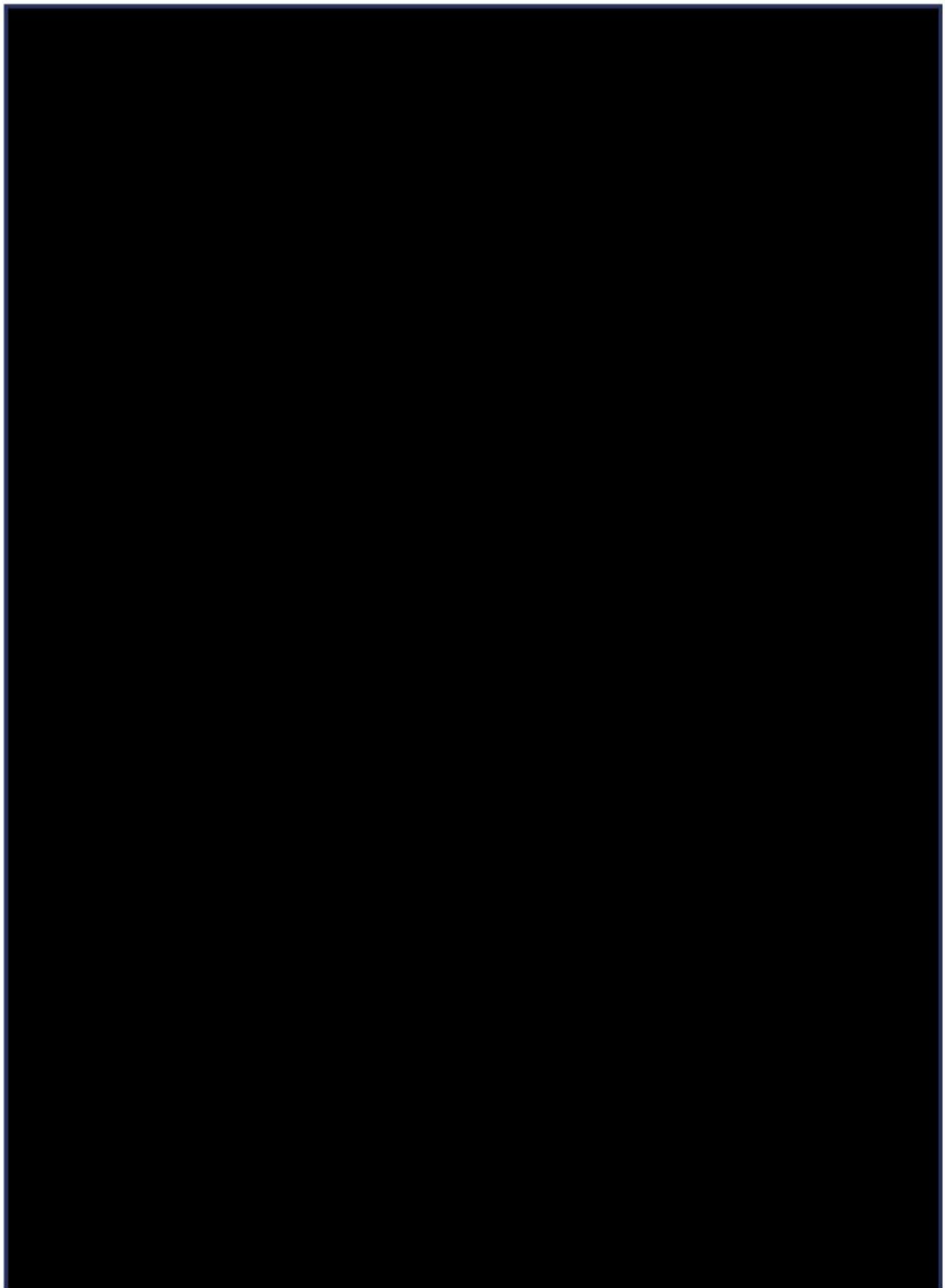
Matriz de perfil y permiso.

	CA	AI	DA	JD	JP	CO	JG	AU	JDT	JGT	CRH	AA	JGC	PS
CU	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
EU	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
HU	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
IHU	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
RTP	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
ETP	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
CTP	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
STP	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
ATP	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
SVRTP	✓	×	×	✓	✓	✓	×	×	✓	×	×	✓	✓	×
OVRTP	✓	×	✓	✓	✓	×	×	×	✓	×	×	✓	×	×
NVRTP	✓	×	✓	✓	✓	×	×	×	✓	×	×	✓	×	×
RTNP	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
ETNP	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
CTNP	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
STNP	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
ATNP	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
SVRTNP	✓	×	×	✓	✓	✓	×	×	✓	×	×	✓	✓	×
OVRTNP	✓	×	✓	✓	✓	×	×	×	✓	×	×	✓	×	×
NVRTNP	✓	×	✓	✓	✓	×	×	×	✓	×	×	✓	×	×
RO	✓	×	×	✓	✓	✓	✓	×	✓	✓	×	✓	✓	×
EO	✓	×	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
ELO	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
RS	✓	×	×	✓	✓	✓	✓	×	✓	✓	×	✓	✓	×
ES	✓	×	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
GNO	✓	✓	✓	✓	✓	×	×	×	✓	×	✓	✓	×	×
GRT	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
GRAT	✓	✓	✓	✓	✓	×	×	×	✓	×	×	✓	×	×
AGT	✓	×	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
CAT	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
REC	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
EEC	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
HEC	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
IHEC	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
RAC	✓	×	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
EAC	✓	×	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
VAC	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
IVAC	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
SVTTP	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×

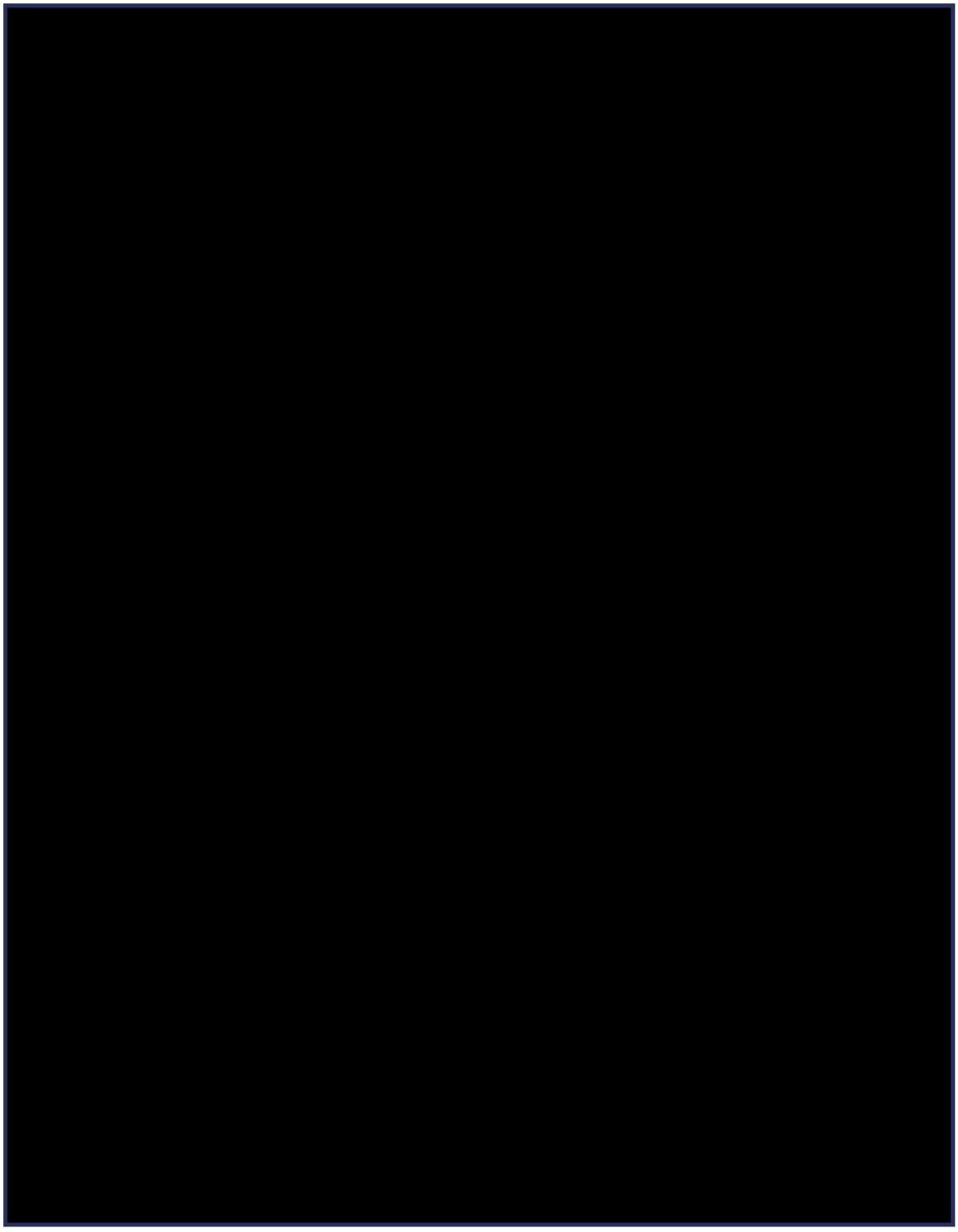
OVTTP	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
NVTTP	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
SVTTNP	✓	✓	✓	✓	✓	✓	×	×	✓	×	×	✓	✓	×
OVTTNP	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
NVTTNP	✓	×	×	×	×	×	×	×	✓	✓	×	✓	×	×
RPGT	✓	×	✓	×	×	×	×	×	×	×	×	✓	×	×
COAT	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
CON	✓	✓	✓	✓	✓	×	×	×	✓	×	×	✓	×	×
SON	✓	×	×	×	×	✓	✓	✓	×	✓	×	✓	✓	×
CRT	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	×
CCE	✓	✓	✓	✓	✓	×	×	×	✓	×	✓	✓	×	✓
DRCE	✓	✓	✓	×	×	×	×	×	×	×	✓	✓	×	×
RCE	✓	×	×	×	×	×	×	×	×	×	×	✓	×	✓
RR	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	✓
TC	✓	✓	✓	×	×	×	×	×	×	×	×	✓	×	✓
CFRC	✓	×	×	×	×	×	×	×	×	×	×	✓	×	×
RC	✓	✓	✓	✓	✓	×	×	×	✓	×	✓	✓	×	×



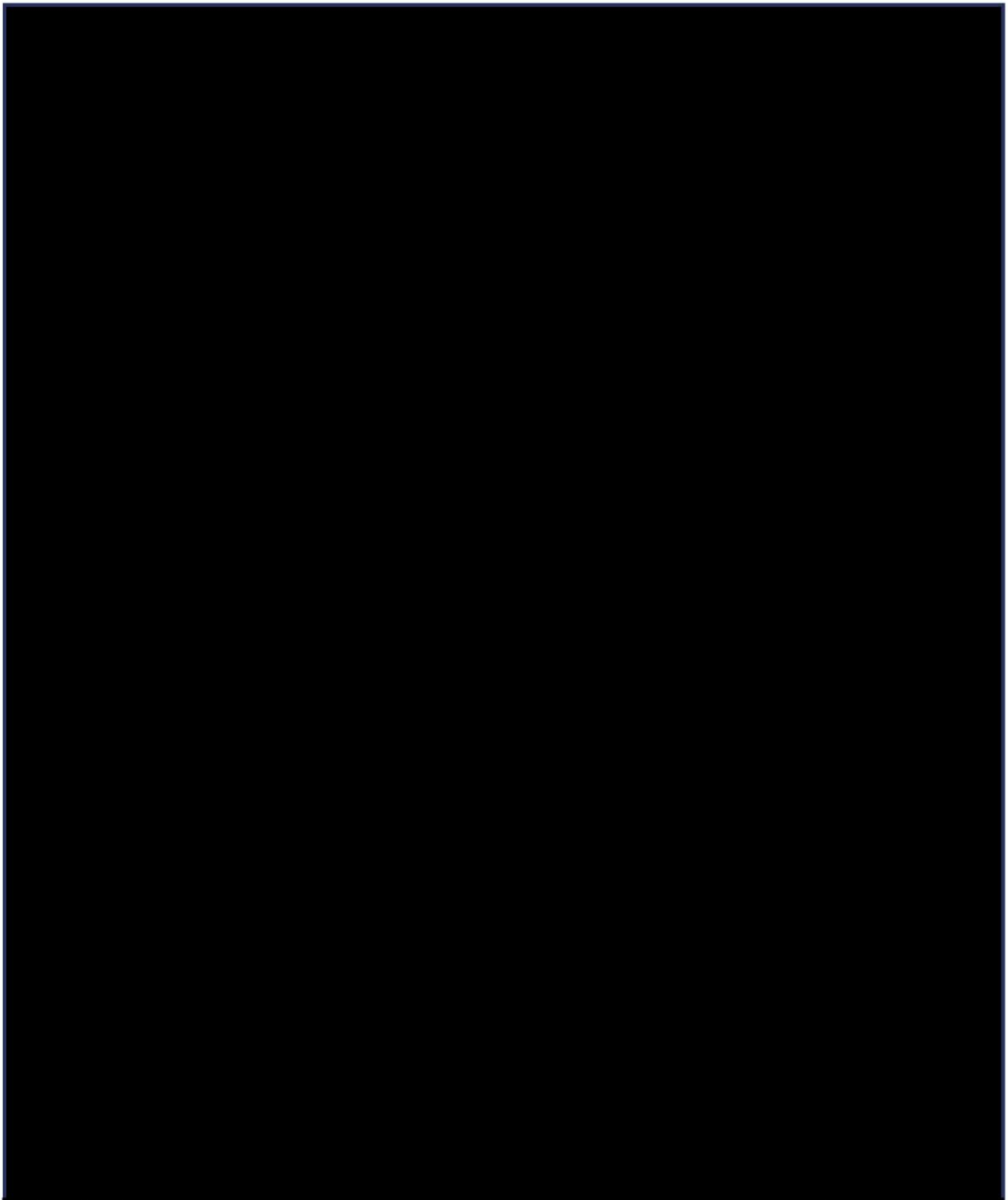
ELIMINADO: Tres renglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.



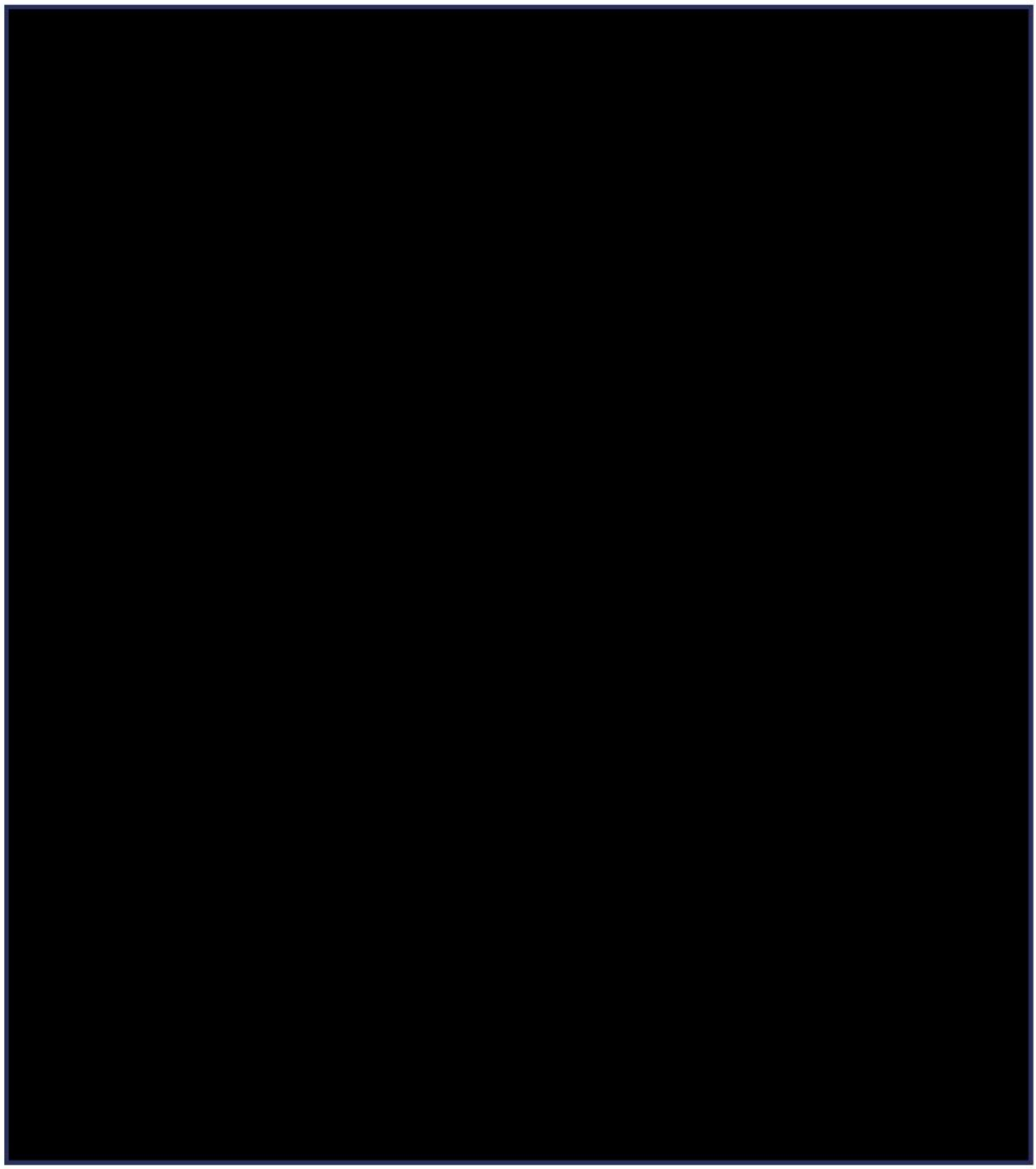
ELIMINADO: Veintiocho renglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.



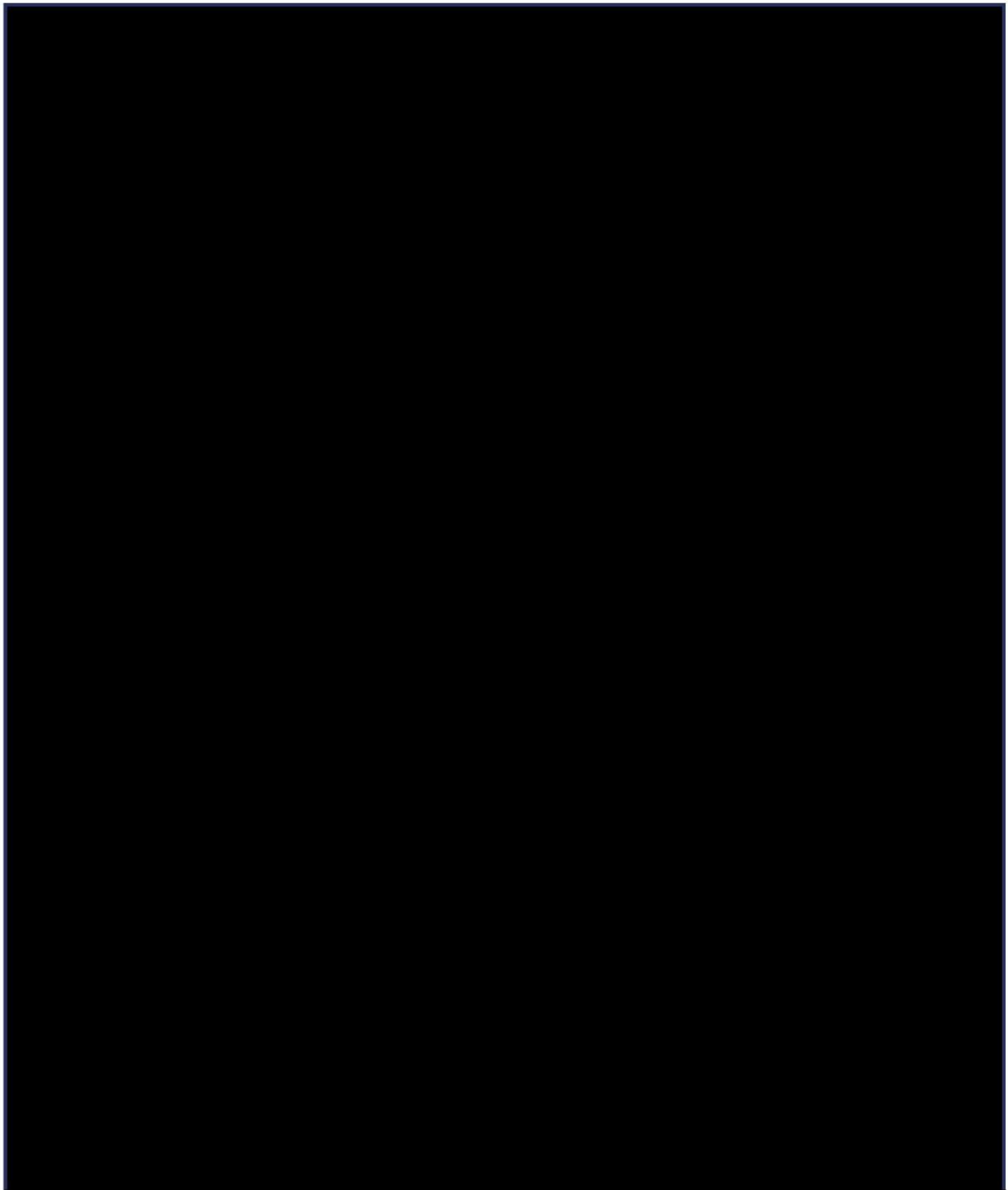
ELIMINADO: Treinta renglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.



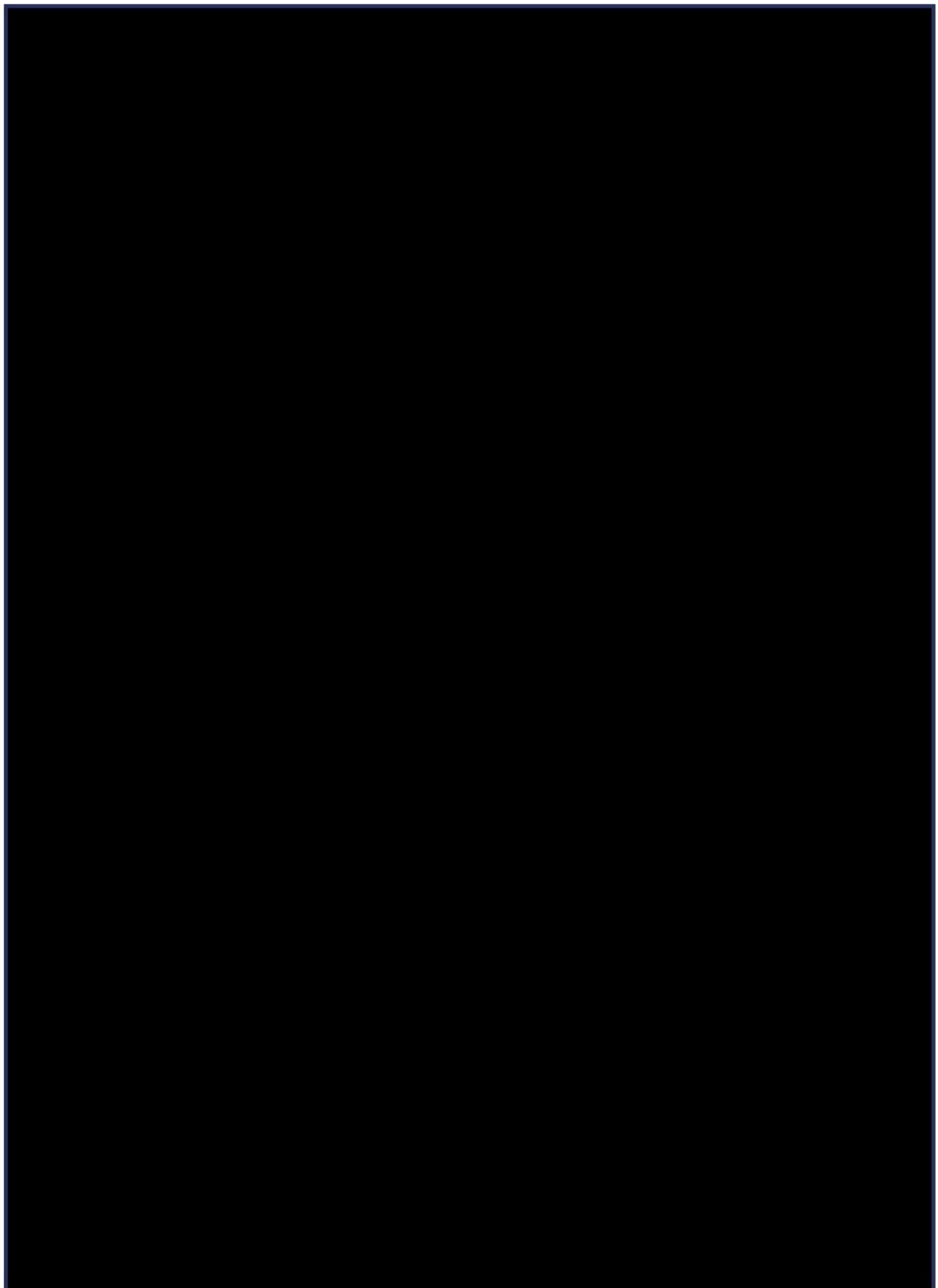
ELIMINADO: Tres renglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.



ELIMINADO: Veinte reglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.



ELIMINADO: Tres renglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.



ELIMINADO: Diecinueve renglones de información clasificada como reservada. Fundamento legal: Artículo 32 y 36 del Reglamento de Transparencia y Acceso a la Información Pública de la Universidad Nacional Autónoma de México, publicado en Gaceta UNAM el 25 de agosto de 2016. Fecha de clasificación aprobada por el Comité de Transparencia de la UNAM, 19 de agosto de 2022, Resolución CTUNAM/526/2022.

ANEXO 6
FORMATOS PARA EL CUMPLIMIENTO DE LAS MST

AUDITORÍA INTERNA Junio 2022

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato	**1**	**Verificación anual**	**Acción concluida**	(SÍ)
Medida de seguridad técnica:		**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			03/08/20	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	04/08/20
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**2**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			04/08/20	
Nombre y firma Administrador del sistema de información			**Fecha término**	
			05/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**3**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			05/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			11/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**4**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			11/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 13/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**5**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:		**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.		
Conocimientos requeridos:		Administración de sistema operativo. Comandos de borrado.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			13/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 14/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**6**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. II. a) Sincronizar la fecha y hora con el servidor NTP (Network Time Protocol) oficial de la UNAM**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		A fin de poseer información consistente, los sistemas de información deben estar sincronizados con una instancia central de tiempo, en este caso el servidor NTP de la UNAM.		
Proceso recomendado:		**A)** Realizar la verificación y configuración con privilegio de administrador del sistema operativo. **B)** En función del sistema operativo, acceder a la configuración de servidor de tiempo (NTP) en interfaz gráfica o por medio de línea de comandos. *Por ejemplo*, en el caso del sistema operativo Linux: - Verificar la existencia del archivo */etc/ntp.conf* - Editar el archivo *ntp.conf* incluyendo en la primera línea: *server ntpdgtic.redunam.unam.mx* ***ó*** *server 132.247.169.17* - Reiniciar el demonio del cliente NTP con el comando *sudo service ntp reload.* **C)** En caso de no tener el cliente NTP instalado, descargarlo del repositorio de aplicaciones del sistema operativo, instalarlo y regresar al punto B. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Los servidores virtuales y contenedores hospedados en el Centro de Datos en DGTIC son configurados de origen con sincronización al servidor NTP de la UNAM. **2.-** No se deben usar otros servidores de NTP distintos al de UNAM.		
Conocimientos requeridos:		Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			14/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 17/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**7**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:		**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			17/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			19/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**8**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:		**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			17/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			27/08/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**9**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM*. **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			27/08/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			03/09/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**10**	**Verificación anual**	**Acción concluida**	(SÍ)
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:		**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			03/09/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	07/09/20
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**11**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:		**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			07/09/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			09/09/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**12**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:		**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.		
Conocimientos requeridos:		Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			09/09/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			10/09/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**13**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:		**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy)*. **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server*. **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. **2.-** El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			10/09/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			18/09/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**14**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. **D)** En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **E)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			18/09/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			24/09/20	
Observaciones / anotaciones				

<table>
<tr><td colspan="3">Sistema Integral de Gestión de Auditorías</td><td colspan="2">AI - SIGA</td></tr>
<tr><td>Formato:</td><td>15</td><td>Verificación anual</td><td>Acción concluida</td><td>(SÍ)</td></tr>
<tr><td colspan="2">Medidas de seguridad técnicas</td><td colspan="3">Artículo 18. I. a) Utilizar los datos personales preexistentes que estén disponibles, de acuerdo con sus respectivas políticas de uso y acceso en bases de datos a cargo de otras áreas universitarias.</td></tr>
<tr><td colspan="2">Aplicable en:</td><td colspan="3">I. Bases de datos y sistemas de tratamiento.</td></tr>
<tr><td colspan="2">Tiempo estimado:</td><td colspan="3">Hito.</td></tr>
<tr><td colspan="2">Importancia de la acción:</td><td colspan="3">Optimizar y consolidar el uso y la protección de datos personales al hacer referencia a instancias universitarias que sean las principales responsables de su obtención, resguardo y protección.</td></tr>
<tr><td colspan="2">Proceso recomendado:</td><td colspan="3">A) Disponer del inventario de datos del sistema de información, esto es: documento con la descripción de tablas, campos, tipo de datos, relaciones y consultas.
B) Con la Área Universitaria que esté identificada como la instancia autoritativa en materia de datos personales, comparar el inventario de datos. <u>Por ejemplo</u>: La Dirección General de Administración Escolar es la dependencia autoritativa en materia de datos personales de estudiantes.
C) Establecer el acuerdo por escrito para el uso de campos específicos de datos personales de la instancia autoritativa.
D) Establecer el mecanismo de comunicación entre el sistema de información y el de la instancia autoritativa. <u>Por ejemplo</u>: Webservices, transferencia SFTP.
E) Llenar y firmar formato.</td></tr>
<tr><td colspan="2">Mejores prácticas, referencias:</td><td colspan="3">1.- El hacer referencia a instancias a cargo de la obtención de los datos personales y su protección se garantiza la homogeneidad de la información.</td></tr>
<tr><td colspan="2">Conocimientos requeridos:</td><td colspan="3">Administración de sistema de información. Gestión de bases de datos.</td></tr>
<tr><td colspan="3">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="3">Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022
Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022</td><td colspan="2">24/09/20</td></tr>
<tr><td colspan="3">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término
25/09/20</td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="4"></td></tr>
</table>

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**16**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:		**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			25/09/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 14/10/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**17**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:		**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			14/10/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			22/10/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**18**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnica:		**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:		**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			22/10/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			10/11/20	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**19**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. I. d) Impedir el uso de cuentas y servicios gestionados por personas físicas para el tratamiento de los datos personales.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Debe evitarse el riesgo que implica el depender de cuentas de control personal para acceder a servicios, fuentes de información o cualquier elemento del sistema de información que ponga en riesgo su estabilidad y confiabilidad.		
Proceso recomendado:		**A)** Realizar revisión integral del sistema de información en materia de accesos, cuentas y servicios. *Por ejemplo*: En caso de consultar vía un *Webservice* a un sistema autoritativo de datos personales en la DGAE, identificar la cuenta de acceso a ese sistema. **B)** Determinar si las cuentas de acceso a servicios locales o remotos están bajo el control de la administración del sistema. *Por ejemplo*: Si la cuenta de acceso a un *Webservice* – su usuario y contraseña – está bajo el control del administrador del sistema, o si un respaldo que se realiza en un equipo remoto es con una cuenta y contraseña controlada por el administrador del sistema. **C)** Si las cuentas de acceso a servicios locales o remotos pertenecen a personas del Área Universitaria, cambiarlas por cuentas institucionales dentro del control de la instancia universitaria. *Por ejemplo*: si la identificación para acceder a un respaldo remoto es del tipo correopersonal@google.com, deberá cambiarse por una cuenta del tipo cuentadegestion@unam.mx **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Nunca deben usarse cuentas, servicios, suscripciones, licencias o cualquier otro elemento informático cuyo control dependa de una sola persona.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			10/11/20	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			13/01/21	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**20**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:		**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			13/01/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			21/01/21	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**21**	**Verificación anual**	**Acción concluida**	(SÍ)
Norma Complementaria Técnica		**Artículo 19. IV. b) Supervisar los controles de seguridad en la red de datos donde opere el sistema para tratamiento de datos personales.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El control de seguridad de los equipos activos de red que suministran la conectividad al sistema de información es un elemento básico para la protección de los datos.		
Proceso recomendado:		**A)** Identificar los equipos activos de red que permiten la conexión del equipo de cómputo con el sistema de información, incluyendo marca, modelo, versión de software, vigencia de mantenimiento y capacidades de protección de las comunicaciones. **B)** Determinar las reglas de seguridad físicas (acceso restringido, cuartos de telecomunicaciones) y lógicas (cuentas de acceso, puertos activos, protocolos activos) para el equipo de red. **C)** Incluir en las acciones para aseguramiento de la red de datos aquellas que sean necesarias en función de los controles actuales. Definir un plan de regularización de la seguridad en caso de ser aplicable. **D)** Mantener actualizados los equipos activos de red y con un programa de mantenimiento. **E)** Identificar y en su caso programar la instalación de equipo para seguridad perimetral de la red de datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las ubicaciones físicas de los equipos activos de red deben estar protegidas con cerraduras y controles de acceso, cumplir las normas de operación y no emplearse para ningún otro equipo o uso.		
Conocimientos requeridos:		Administración de redes de datos.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			21/01/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 29/01/21	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**22**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:		**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			29/01/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	09/02/21
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**23**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:		**F)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **G)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **H)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar - equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **I)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.		
Conocimientos requeridos:		Administración de sistema de información. Desarrollo de aplicaciones.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			09/02/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 24/03/21	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**24**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. I. f) Cumplir con las especificaciones de seguridad informática previo a la puesta en operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Solo los sistemas de información revisados integralmente en su seguridad y estabilidad pueden ser publicados bajo el dominio .unam.mx .		
Proceso recomendado:		**A)** Una vez concluido el desarrollo o actualización de un sistema de información, solicitar al área de seguridad del Área Universitaria la revisión de seguridad informática del sistema, lo que incluye: pruebas de penetración, pruebas de estabilidad, pruebas de carga y endurecimiento de la seguridad. En caso de no contar con esa área, requerirlo a UNAM CERT al correo seguridad.tic@unam.mx . **B)** Una vez recibido el reporte del área de seguridad, aplicar las medidas de corrección que incluya el reporte. Regresar al punto A. **C)** Habiendo resuelto los hallazgos y sugerencias de mejora de la seguridad señalados por el área especializada, realizar la instalación del sistema en la plataforma definitiva de cómputo, extrayéndolo del entorno de desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El equipo de UNAM CERT puede asesorar a las entidades y dependencias en la aplicación de las medidas de corrección y mitigación a partir de los resultados de la revisión de seguridad.		
Conocimientos requeridos:		Administración de aplicaciones. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			24/03/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			13/05/21	
Observaciones / anotaciones				

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**25**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 18. III. a) Utilizar equipos con componentes actualizados, protegidos con garantías y soporte, y con la capacidad suficiente para atender la demanda del servicio y de los usuarios.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Hito.		
Importancia de la acción:		Mantener en adecuada condición de operación el equipo de cómputo incrementa la estabilidad y seguridad del sistema de información.		
Proceso recomendado:		**A)** Elaborar una lista del inventario de los equipos de cómputo, periféricos y de almacenamiento necesarios para la ejecución del sistema de información. **B)** Determinar la razón por la que el sistema de información requerirá estar localizado en un equipo físico y no en un servidor virtual. Con ello justificar una adquisición o actualización. Por ejemplo: por incompatibilidad con hipervisores, necesidades de comunicación exclusivamente locales en la entidad y dependencia o el no necesitar de un entorno de alta disponibilidad automática. **C)** Identificar en el inventario versiones, introducción en el mercado, vida útil, contratos de mantenimiento y soporte para todos y cada uno de los componentes, en el caso de emplear equipo físico. **D)** Adquirir los componentes y elementos necesarios para la actualización, vigencia de soporte y capacidad para atención a los usuarios en el equipo de cómputo físico. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** El mantenimiento preventivo debe contar con medidas de verificación.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			13/05/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** 14/05/21	
Observaciones / anotaciones				

<table>
<tr><td colspan="2">Sistema Integral de Gestión de Auditorías</td><td colspan="2">AI - SIGA</td><td colspan="2"></td></tr>
<tr><td>Formato:</td><td>26</td><td>Verificación anual</td><td>Acción concluida</td><td colspan="2">(SÍ)</td></tr>
<tr><td>Medidas de seguridad técnicas:</td><td colspan="5">Artículo 18. III. b) Definir el programa de mantenimiento preventivo.</td></tr>
<tr><td>Aplicable en:</td><td colspan="5">III. Equipos de cómputo.</td></tr>
<tr><td>Tiempo estimado:</td><td colspan="5">Hito.</td></tr>
<tr><td>Importancia de la acción:</td><td colspan="5">Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.</td></tr>
<tr><td>Proceso recomendado:</td><td colspan="5">A) De la lista de equipo de cómputo físico necesario para la operación del sistema de información, extraer las vigencias de mantenimiento.
B) En caso de no estar en posibilidad de aplicar el mantenimiento preventivo por el personal del Área Universitaria, cotizar pólizas de mantenimiento de acuerdo con el tipo de componente, preferentemente una sola póliza para el conjunto del equipo físico.
C) Adquirir las pólizas de mantenimiento preventivo y observar su vigencia. La vigencia no podrá ser menor de un año.
D) Llenar y firmar formato.</td></tr>
<tr><td>Mejores prácticas, referencias:</td><td colspan="5">1.- El programa de mantenimiento debe considerar los costos de contratos, refacciones, partes, actualizaciones y reemplazos.</td></tr>
<tr><td>Conocimientos requeridos:</td><td colspan="5">Administración de infraestructura.</td></tr>
<tr><td colspan="4">Ejecución</td><td colspan="2">Fecha inicio</td></tr>
<tr><td colspan="4">Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022
Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022</td><td colspan="2">14/05/21</td></tr>
<tr><td colspan="4">Nombre y firma
Administrador del sistema de información o servidor</td><td colspan="2">Fecha término</td></tr>
<tr><td colspan="4"></td><td colspan="2">17/05/21</td></tr>
<tr><td>Observaciones / anotaciones</td><td colspan="5">No se cuenta con un programa de mantenimiento preventivo contratado, sin embargo el personal de la Coordinación de Informática de esta Auditoría Interna realiza a demanda esta acción, en cambio se cuenta con un programa de mantenimiento correctivo permanente que se provee por parte de la Coordinación Administrativa del Patronato Universitario.</td></tr>
</table>

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**27**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Seis días hábiles.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			17/05/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			25/05/21	
Observaciones / anotaciones		No se cuenta con un programa de mantenimiento preventivo contratado, sin embargo el personal de la Coordinación de Informática de esta Auditoría Interna realiza a demanda esta acción, en cambio se cuenta con un programa de mantenimiento correctivo permanente que se provee por parte de la Coordinación Administrativa del Patronato Universitario.		

Sistema Integral de Gestión de Auditorías			AI - SIGA	
Formato:	**28**	**Verificación anual**	**Acción concluida**	(SÍ)
Medidas de seguridad técnicas:		**Artículo 21. Solo se permitirá el uso de servicios de nube pública para el resguardo de archivos cifrados que contengan respaldos de la información.**		
Aplicable en:		Servicios en la nube pública.		
Tiempo estimado:		Hito.		
Importancia de la acción:		No pueden conservarse o usarse datos personales que sean tratados por la UNAM en servicios de nube pública. Estos servicios sólo se permiten para el respaldo de archivos cifrados, no en producción.		
Proceso recomendado:		**A)** Identificar los respaldos que se tengan resguardados en servicios de nube pública. **B)** Verificar el cifrado en cada uno de los respaldos que se almacenen en nube pública. El cifrado no deberá ser de menor capacidad al equivalente a AES de 128 bits.		
Mejores prácticas, referencias:		**1.-** La DGTIC proporciona el servicio de respaldos en el Centro de Datos, por lo que se sugiere utilizarlo en lugar de respaldos en la nube pública.		
Conocimientos requeridos:		Administración de respaldos. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
Firmado digitalmente por Jonathan Neftali Calderón Díaz. Fecha: 30/06/2022 Firmado digitalmente por Roberto Carlos Pérez Medina. Fecha: 30/06/2022			25/05/21	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
			26/05/21	
Observaciones / anotaciones				

ANEXO 7
USUARIOS REGISTRADOS EN EL SIGA.

AUDITORÍA INTERNA Junio 2022

Usuarios registrados en el SIGA:

Usuario	Perfil
José Alfredo Montero Rojas	Auditor interno
Héctor Granados Villafuerte	Director de área
Miriam Susana Espinosa Rodrigo	Director de área
Jesús Miranda Iglesias	Director de área
Josué Armando Contreras Salcedo	Jefe de departamento
Diana Eréndira Díaz Arciniega	Jefe de departamento
Laura Alicia Guerrero Velázquez	Jefe de departamento
Carlo Ulises Navarrete Arellano	Jefe de departamento
Claudia Lozano Ramírez	Jefe de departamento
Antonio Nápoles Vázquez	Jefe de proyectista
Enrique Galicia Espinosa	Jefe de proyectista
Roberto Carlos Pérez Medina	Coordinador administrador
Jonathan Neftalí Calderón Díaz	Coordinador administrador
Alejandro Ávila Espinosa	Coordinador
Alejandra Judith González Rangel	Coordinador
Edgar Pérez González	Coordinador
Aurora Isela Chávez Zúñiga	Coordinador
Rubén Barajas Muñoz	Coordinador
Cecilia Romero	Coordinador
José Omar Suárez Martínez	Coordinador
Enrique Becerril Galindo	Coordinador
Aldo Aguirre Cendejas	Coordinador
Faride Emilia Asuad Sanén	Coordinador
Rubén Omar Sosa López	Coordinador
Edith Ramírez Hernández	Coordinador
Margarita Segura Martínez	Coordinador
Víctor Jesús Cruz Guzmán	Jefe de grupo
Jorge Manuel Granados Briones	Jefe de grupo
María del Rocío Alvarado Ferreyra	Jefe de grupo
José Agustín Montaño Barrón	Jefe de grupo
Eliud Jair Jiménez Martínez	Jefe de grupo
Javier Bautista Sánchez	Jefe de grupo
Nancy Leticia Rayas Rivera	Jefe de grupo
Alma Patricia Bolaños Stanley	Jefe de grupo
Juan José Legaria Parra	Jefe de grupo
Verónica Arias Bernal	Jefe de grupo
Jorge Alberto De la Cruz De la Cruz	Jefe de grupo
María Olympia Fabiola Ramírez Carrillo	Jefe de grupo
Olsen Jafet de Jesús Uribe Peña	Jefe de grupo
Alberto Gómez Orozco	Jefe de grupo
Rubén Alejandro Gallardo Martínez	Jefe de grupo
Isaac Isidro Guevara Mora	Jefe de grupo
Juan Fernando Quintanar Martínez	Jefe de grupo
Daniel Figueroa Sánchez	Jefe de grupo

Usuario	Perfil
Araceli Ramos Piña	Jefe de grupo
Jonathan Villalobos Gutiérrez	Jefe de grupo
David Alejandro Gutiérrez Sepúlveda	Jefe de grupo
Gabriela López Hernández	Jefe de grupo
Pamela Judith Martínez Coca	Jefe de grupo
Victor Merino Zárate	Jefe de grupo
Enrique Tovar Vázquez	Jefe de grupo
Teresa Otilia Vega Corona	Jefe de grupo
José Luis Calderón León	Auditor
Pablo Díaz Torres	Auditor
Israel Esteban Aguilar Landa	Auditor
Adelin Valeria García López	Auditor
Sandra Granados Rosas	Auditor
Alicia Citlali Aguilar Castellanos	Auditor
Viviana Imelda Flores Caballero	Auditor
Juan Manuel Montiel Cervantes	Auditor
Erick Olivares Torres	Auditor
Juan Eduardo Cocoletzi López	Auditor
Gabael Iván Barreto García	Auditor
Jesús Canales Pérez	Auditor
Marlene Guadalupe Mendoza García	Auditor
Isaac López Márquez	Auditor
Benjamín Chenistán Yañez Flores	Auditor
Mariana Robles Ceballos	Auditor
Luis Ruben Ortíz Amaya	Auditor
Brandon Gustavo Linares Rios	Auditor
Esperanza Santos Rubio	Auditor
Miroslava Vanessa Solís Jiménez	Auditor
Miriam Gutiérrez Anta	Auditor
David Sánchez Rodríguez	Auditor
Alejandra Nayetzin Castañeda Pérez	Auditor
Mónica Galindo Hernández	Auditor
José Carlos Ramirez Guevara	Auditor
Carlos Olivares Navarro	Auditor
Ivonne Ellizalde Cardiel	Auditor
Raymundo Ruiz Sánchez	Auditor
Mónica Valseca Sánchez	Jefe de departamento de transparencia
Diana Lisset Soto Palomo	Jefe de grupo de transparencia
Alejandra García Galicia	Jefe de grupo de transparencia
María Luisa Palacios Sandoval	Coordinador de recursos humanos
Yazmín Muciño González	Jefe de grupo coordinador
Marisol Olguín Malagón	Pool secretarial
María del Carmen Martínez González	Pool secretarial
Raquel Areli Zerecero Lucario	Pool secretarial

ANEXO 8
PLAN DE RESPALDOS

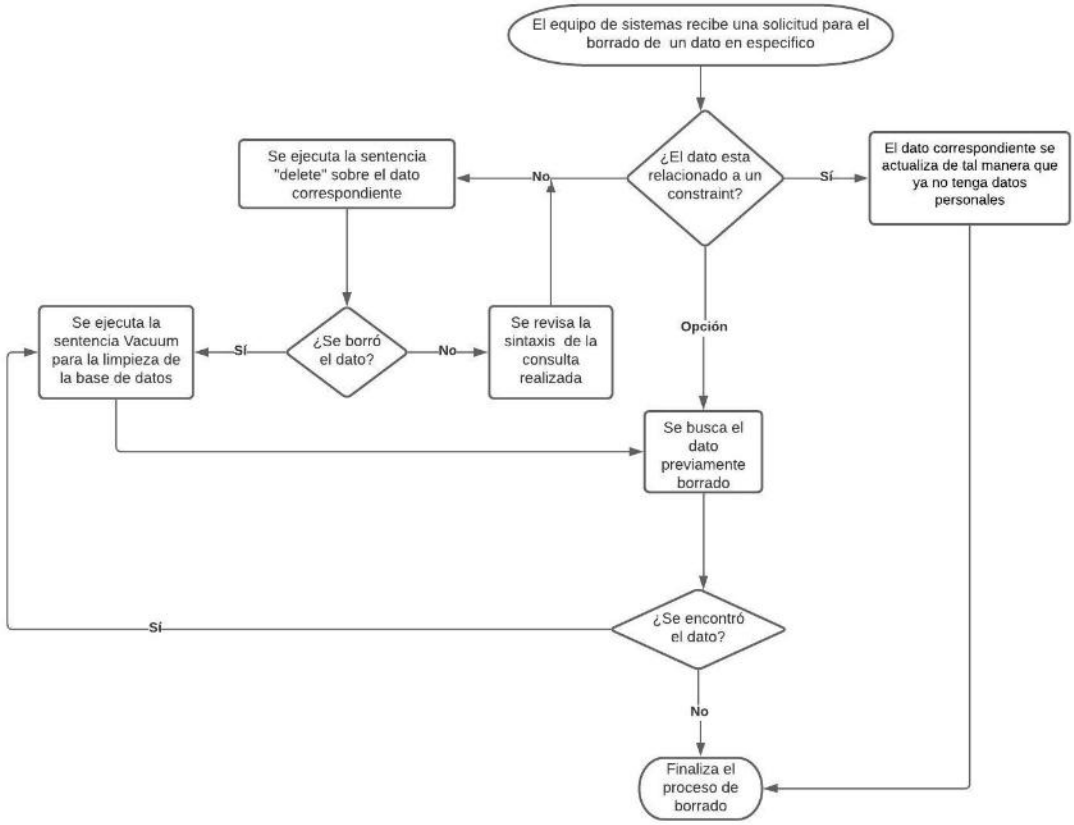
AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS					AI - SIGA					
PLAN DE RESPALDOS DE INFORMACIÓN										
Nomenclatura: **N/A = No aplica**										
Tipo de respaldo	**Descripción**	**Secuencia**	**Medios para el resguardo**	**Descripción**	**Responsable de cada tipo y medio de respaldo**	**Rotación de respaldos y medios.**	**Áreas de resguardo**	**Métodos de cifrado**	**Tiempo objetivo de recuperación**	**Punto objetivo de recuperación.**
Completo.	Durante este proceso se efectúa una copia de todos los archivos y bases de datos del sistema.	Diario 4 veces al día.	Respaldo como almacenamiento.	El respaldo generado se guarda en otro equipo de almacenamiento.	Ing. Jonathan Neftali Calderón Díaz.	Nulo.	Oficina de sistemas de Auditoría Interna.	N/A.	1 hora.	16 horas.
Incremental.	Durante este proceso se realiza el copiado de cualquier archivo o dato que haya cambiado desde la última copia de seguridad, independientemente de que la copia de seguridad fuera completa o incremental.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.
Diferencial.	Durante este proceso se realiza el copiado de cualquier archivo o dato que haya cambiado desde la última copia de seguridad, pero a diferencia de la copia incremental está se realiza de manera consecutiva.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.	N/A.

ANEXO 9
PLAN DE BORRADO SEGURO

AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA
HERRAMIENTA PARA BORRADO SEGURO DE LA BASE DE DATOS	
PROCEDIMIENTO PARA BORRADO SEGURO DE LA BASE DE DATOS	



ANEXO 10
PLAN DE MEJORA

AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA
MEDIDAS DE SEGURIDAD PARA REDUCIR EL RIESGO AL SISTEMA DE INFORMACIÓN	
Medidas físicas.	• Cámaras de videovigilancia. • Uso de biométrico. • Candado de cable para computadoras de escritorio y para laptops. • Cuarto cerrado con acceso mediante llave.

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA
PLAN DE MEJORAMIENTO DE LA PROTECCIÓN FÍSICA DE EQUIPOS	
Medidas físicas.	• Colocar puertas con cerraduras al servidor del sistema de datos personales. • Bloquear el uso de puertos USB o cualquier elemento físico que permita sustraer información. • Control de acceso al área de sistemas. • Implementación de alarmas y sensores.

ANEXO 11
PLAN DE SEGURIDAD PARA PERIODO VACACIONAL, CONTINGENCIAS Y VENTANAS DE MANTENIMIENTO.

AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA		
MEDIDAS NECESARIAS DE SEGURIDAD PARA PERÍODOS VACACIONALES, CONTINGENCIAS Y VENTANAS DE MANTENIMIENTO			
CONTROL DE ACCESO FÍSICO Y LÓGICO A LOS EQUIPOS, EJECUCIÓN DE RESPALDOS Y SISTEMAS DE ALTA DISPONIBILIDAD.			
TIPO DE ACTIVIDAD	**RESPONSABLE**	**CONTROL**	**MEDIDAS NECESARIAS**
Periodo vacacional.	L.I. Roberto Carlos Pérez Medina.	Consultar el: *Diagrama 1. Control vacacional.*	Se cierra el acceso a la puerta principal de la dependencia como también a la oficina de sistemas de Auditoría Interna; sin embargo, el sistema de información continua disponible.
Ventanas de mantenimiento.	Ing. Jonathan Neftali Calderón Díaz.	Consultar el: *Diagrama 2. Ventana de mantenimiento.*	Se comunica al coordinador que se realizará una ventana de mantenimiento. Este lo comunica a los usuarios, indicando fecha y hora. Durante este tiempo se realizan las acciones pertinentes.
Contingencias.	Ing. Jonathan Neftali Calderón Díaz.	Consultar el: *Diagrama 3. Contingencia.*	En caso de que la contingencia sea presente en periodo vacacional o día inhábil se conecta el responsable del sistema vía escritorio remoto y se atiende la incidencia. En caso de ser de manera presencial se solicita una ventana de mantenimiento, se

			soluciona la incidencia y se habilita nuevamente el sistema de información.

CASO DE CONTINGENCIA	
TIPO DE FALLA	**ACCIÓN**
Falla de servicio de red.	Se notifica al proveedor de red.
Falla de equipo de cómputo.	Se notifica al responsable de soporte técnico.
Falla lógica en sistema operativo.	Se notifica al responsable del sistema de información.
DIRECTORIO DE RESPONSABLES	
Apagado seguro.	Ing. Jonathan Neftali Calderón Díaz.
Apagado fortuito.	Ing. Jonathan Neftali Calderón Díaz.
Apagado programado.	Ing. Jonathan Neftali Calderón Díaz.
Verificación de integridad de información.	Ing. Jonathan Neftali Calderón Díaz.
Activación de servicios locales.	Ing. Jonathan Neftali Calderón Díaz.
Activación de servicios de respaldo.	Ing. Jonathan Neftali Calderón Díaz.

DIAGRAMAS

Diagrama 1. Control vacacional

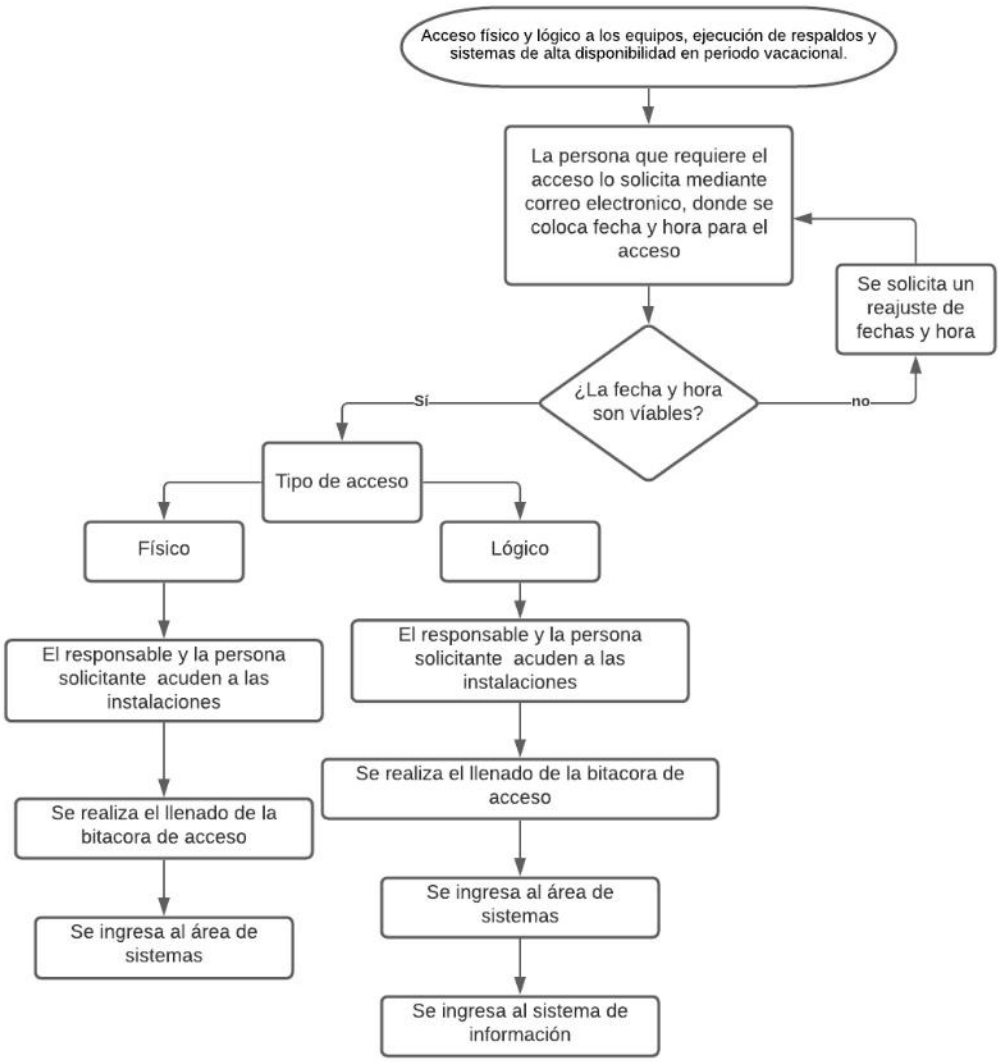


Diagrama 2. Ventanas de mantenimiento

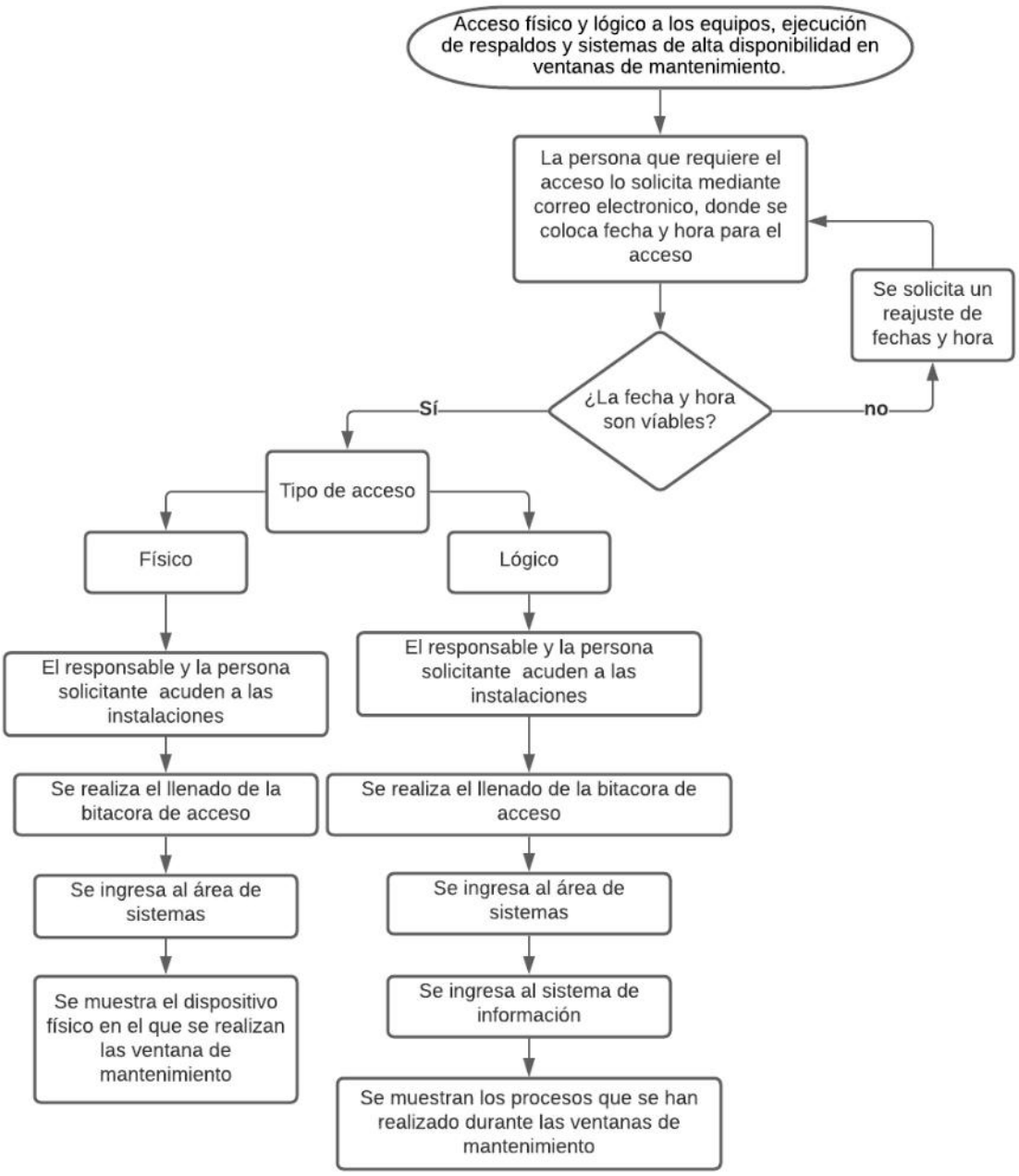
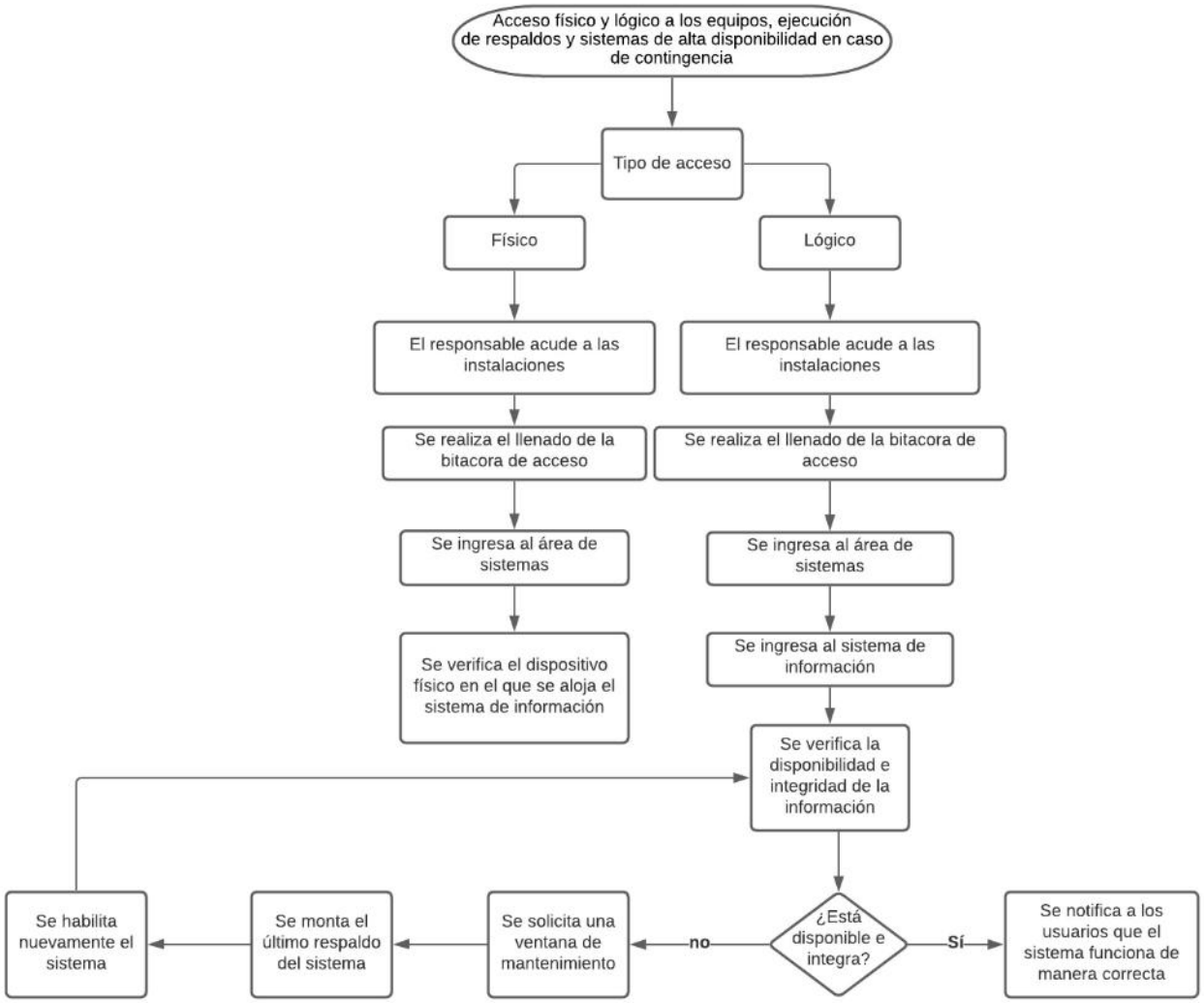


Diagrama 3. Contingencia



ANEXO 12
BITÁCORA DE CONTROL DE RESPALDOS

AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA
BITÁCORA DE CONTROL DE LOS RESPALDOS	
Responsable de respaldos	Ing. Jonathan Neftali Calderón Díaz.
Fecha.	Diario.
Hora.	16:00 pm. 16:20 pm. 23:00 pm. 23:30 pm.
Tipo de respaldo.	Completo.
Ejecutor del respaldo.	Ing. Jonathan Neftali Calderón Díaz.
Revisor del respaldo.	Ing. Jonathan Neftali Calderón Díaz.
Ubicación del respaldo.	Equipo de líder técnico y equipo provisional de respaldos del área de sistemas.
Medio.	Digital.
Etiqueta.	AñoMesDíaHora.nb3.
Responsable de verificación de respaldos	Ing. Jonathan Neftali Calderón Díaz.
Fecha.	Ultimo de viernes del mes.
Hora.	11:00 am.
Tipo de respaldo.	Completo.
Ejecutor del respaldo.	Ing. Jonathan Neftali Calderón Díaz.
Revisor del respaldo.	Ing. Jonathan Neftali Calderón Díaz.
Ubicación del respaldo.	Equipo de líder técnico y equipo provisional de respaldos del área de sistemas.
Medio	Digital.
Etiqueta	AñoMesDíaHora.nb3.

ANEXO 13
BITÁCORAS DE ACCESO AL SISTEMA DE INFORMACIÓN

AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA	
BITÁCORAS RELACIONADAS CON EL SISTEMA DE INFORMACIÓN		
MEDIO DIGITAL		
Nombre de la bitácora	**Ubicación**	
Bitácora de acceso de usuarios al sistema operativo.		
Bitácora de acceso de usuarios a la base de datos del sistema de información (Logs).		
MEDIO FÍSICO		
Nombre de la bitácora	**Ubicación**	
Bitácora de acceso.	Oficina de sistemas de Auditoría Interna.	
Bitácora de control de respaldos.	Oficina de sistemas de Auditoría Interna.	
Cronograma de revisión de integridad y respaldo de las bitácoras		
Diario.	No aplica.	
Semanal.	No aplica.	
Mensual.	Aplica	
PROCEDIMIENTO DE RESGUARDO DE LAS BITÁCORAS DIGITALES		
Nombre de la bitácora	**Protección**	**Ubicación del respaldo**
Bitácora de acceso de usuarios al sistema operativo	**Acceso restringido al área de servidores**	**Se encuentra en el servidor de producción**
Bitácora de acceso de usuarios a la base de datos del sistema de información (Logs)	**Acceso restringido al área de servidores**	**Se encuentra en el servidor de producción**
PROCEDIMIENTO DE RESGUARDO DE LAS BITÁCORAS FÍSICAS		
Nombre de la bitácora	**Protección**	**Respaldo**
Bitácora de acceso	Bajo llave en la oficina de sistemas de Auditoría Interna.	Se tiene de manera digital en la nube compartida de patronato universitario
Bitácora de control de respaldos	Bajo llave en la oficina de sistemas de Auditoría Interna.	Se tiene de manera digital en la nube compartida de patronato universitario

ANEXO 14
CONTROL DE SEGURIDAD DE LOS EQUIPOS ASOCIADOS A LA RED

AUDITORÍA INTERNA Junio 2022

SISTEMA INTEGRAL DE GESTIÓN DE AUDITORÍAS	AI - SIGA
Equipos que permiten la conexión del equipo de cómputo con el sistema de información:	
Características:	**Descripción**
• Marca • Modelo • Versión de software • Vigencia de mantenimiento • Capacidades de protección de comunicaciones	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.
Reglas de seguridad físicas:	
• Acceso restringido • Cuartos de telecomunicaciones	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.
Reglas de seguridad lógicas:	
• Cuentas de acceso • Puertos activos • Protocolos activos	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.
Acciones para aseguramiento de la red de datos	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.
Plan de regularización de la seguridad	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.
Actualización de los equipos activos de red y con un programa de mantenimiento.	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.
Instalación de equipo para seguridad perimetral de la red de datos.	La configuración de red es brindada por un tercero, en este sentido, se puede consultar está información con el administrador de la red del patronato universitario.

Esquema de Red
Auditoría Interna