Documento de Seguridad del Centro de Ciencias Genómicas

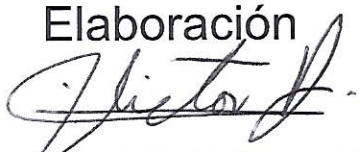
Sistemas de Gestión de Seguridad de Datos Personales

Agosto de 2022

Documento de seguridad

Tabla de autorización

Elaboración



Víctor Manuel Del Moral Chávez

Teléfono:777-3132063 Correo: victor@ccg.unam.mx

Coordinador de la Unidad de Administración de TI

Revisión

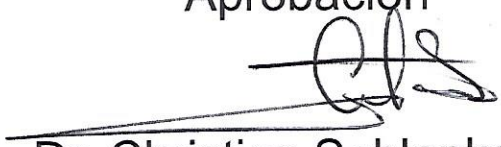
C.P. Felipe Nava Fabián

Teléfono: 777-3177479 Correo: fnava@ccg.unam.mx

Secretario Administrativo

Enlace de Transparencia

Aprobación



Dr. Christian Sohlenkamp

Teléfono: 777-3131697 Correo: chsohlen@ccg.unam.mx

Director del Centro de Ciencias Genómicas

En ausencia: Dr. Sergio Manuel Encarnación Guevara

Correo: encarnac@ccg.unam.mx

Secretario Académico

Fecha de aprobación: 16 de agosto de 2022

ÍNDICE

1. Presentación

El Centro de Ciencias Genómicas (CCG) de la Universidad Nacional Autónoma de México (UNAM) se encuentra ubicado en el Campus Morelos de la UNAM en Cuernavaca, Morelos. El 12 de noviembre de 2004, el Consejo Universitario de la UNAM aprobó el cambio de la denominación del Centro de Investigación sobre Fijación de Nitrógeno a Centro de Ciencias Genómicas — para mayor información ver “Nuestra Historia”.

Somos un grupo de investigadores relativamente pequeño, organizado en siete Programas o Laboratorios enfocados en las áreas de genómica microbiana y de plantas, investigación ecológica, y más recientemente en aspectos de genómica humana. La genómica microbiana incluye proyectos en dinámica del genoma en bacterias, genómica evolutiva y funcional (proteómica y transcriptómica), genómica y bioinformática de la regulación genética y bioinformática comparativa. La genómica funcional de eucariotes incluye la genómica funcional de plantas y más recientemente la investigación genómica y proteómica del genoma humano. De igual forma, se lleva a cabo investigación en biología molecular de interacciones entre bacterias y plantas, así como ecología y evolución microbiana y agricultura aplicada.

En el CCG tenemos un compromiso muy fuerte con la educación y enseñanza de las ciencias genómicas. Los Programas de Investigación están formados por investigadores, posdocs, técnicos y estudiantes de doctorado, maestría y licenciatura.

2. Introducción

Los sistemas que se encargan del manejo de datos personales son principalmente para fines académicos y son utilizados por investigadores, técnicos académicos y estudiantes. Así mismo, alguna información está disponible para el público en general para dar a conocer las líneas de investigación de interés . Estos sistemas son de utilidad para el tratamiento de datos personales relacionados a la producción y trayectoria académica.

El sistema Fundanet (ID: ccg-sacad-001-E-Fundanet) es un sistema de información para la producción científica de los investigadores y técnicos académicos del CCG. Así mismo, se detallan aspectos de la trayectoria profesional.

Los servidores de páginas de internet o sitios web (ID: ccg-uati-001-E-SitiosWeb) despliegan información sobre el Centro de Ciencias Genómicas y en algunas páginas se muestran datos personales.

El sitio web de intranet de la Licenciatura en Ciencias Genómicas (ID: ccg-uati-002-E-IntranetLCG) presenta información de interés solo para personal administrativo y académico, así como para estudiantes con acceso controlado.

Tenemos una serie de sistemas destinados a cursos y apoyo a los docentes y estudiantes (ID: ccg-uati-003-E-Cursos) que facilitan las tareas docentes como cursos y clases para las materias impartidas.

Para el manejo de acervo bibliotecario y el registro de préstamos contamos con un sistema dedicado (ID: ccg-biblioteca-001-E-Aleph). El personal administrativo de la biblioteca tiene acceso al sistema mencionado.

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

Titular de la dependencia: Asigna tareas y responsabilidades para los responsables del tratamiento de datos personales.

Secretario Administrativo: Se encarga de informar al personal del área administrativa respecto al tratamiento de datos personales.

Secretario Técnico: Se encarga de informar al personal del área técnica respecto al tratamiento de datos personales.

Secretario Académico: Se encarga de informar al personal del área académica y a los participantes externos respecto al tratamiento de datos personales.

Coordinador de la Unidad de Administración de TI: Encargado de coordinar la operación del tratamiento de datos y resguardar la información de las bases de datos y de los documentos de respuestas y de los servidores que contienen dicha información.

Personal de la Unidad de Administración de TI: Encargados de desarrollar actualizaciones al sistema de gestión, elaborar respaldos y actualizar los servidores que contienen dicha información.

4. Términos, definiciones y abreviaturas

CCG: Centro de Ciencias Genómicas

LCG: Licenciatura en Ciencias Genómicas

NNB: Nodo Nacional de Bioinformática

5. Inventario de Sistemas para el Tratamiento de Datos Personales

ALEPH (ccg-biblioteca-001-E-Aleph)

Sistema utilizado en la Biblioteca del CCG para llevar a cabo el control del préstamo de libros a la comunidad de usuarios.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

	BIBLIOTECA DEL CCG
Identificador único*	ccg-biblioteca-001-E-Aleph
(Nombre del sistema A1) *	ALEPH
Datos personales (sensibles o no) contenidos en el sistema*:	Nombre completo
Responsable*:	Biblioteca
Nombre*:	**Alexa Miley Gómez Restrepo**
Cargo*:	**Responsable de la biblioteca**
Funciones*:	Verificar que los datos personales estén completos, que sean llenados con exactitud.
Obligaciones*:	Verificar que las fechas de préstamos estén actualizadas y dar seguimiento en caso de retraso en la entrega de los libros.

	Encargados:
(Nombre del Encargado 1*)	**Javier Peza**
Cargo*:	**Asistente de biblioteca**
Funciones*:	Registrar datos personales de los solicitantes de libros.
Obligaciones*:	Registrar los solicitantes de los libros a través de una aplicación llamada CIRCULA que se conecta a la base de datos.
	Usuarios:
(Nombre del Usuario 1*)	NO APLICA
Cargo*:	N/A
Funciones*:	N/A
Obligaciones*:	N/A

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

BIBLIOTECA DEL CCG	
Identificador único¨*	ccg-biblioteca-001-E-Aleph
(Nombre del sistema A1*)	ALEPH
Tipo de soporte	Soporte electrónico
Descripción	Base de datos

Características del lugar donde se resguardan los soportes	Centro de cómputo donde se encuentra el servidor: - Acceso por medio de huella digital al laboratorio - Uso de llave para acceso al Centro de cómputo - Aire acondicionado de confort - Luz artificial - Piso falso - Alimentación eléctrica con equipos de respaldo de energía en línea Acceso al servidor: - Usuario y password

3. ANÁLISIS DE RIESGOS

Ver Anexo I: Análisis de riesgos

4. ANÁLISIS DE BRECHA

Ver Anexo II: Análisis de brecha

5. PLAN DE TRABAJO

Ver Anexo III: Plan de trabajo

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

BIBLIOTECA DEL CCG	
Identificador único*	ccg-biblioteca-001-E-Aleph
(Nombre del sistema A1)*	ALEPH
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No hay traslado de datos en soportes físicos.

Transferencias mediante el traslado de soportes electrónicos:	No hay transferencias de datos de los soportes electrónicos. Todos los datos se quedan en el servidor que los maneja.
Transferencias mediante el traslado sobre redes electrónicas:	Los datos personales son solo el nombre completo del usuario. No se trasladan datos ni a otro sistema ni a otra Dependencia. No hay un protocolo de transferencia pues no aplica.

I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No existen soportes físicos del sistema. No es necesario.

No existe un espacio para resguardar soporte físicos.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

Los accesos se realizan diariamente. Solo el responsable y el encargado acceden a estos datos. Las bitácoras corresponden a estadísticas de préstamos y listados de usuarios activos que consultan el acervo, pero estos nunca acceden a datos personales.
Estas bitácoras están dentro del sistema y no se trasladan a ninguna otra parte. Estas consultas se hacen mediante un módulo integrado al sistema llamado Mantale, que permite realizar las tareas de administración, mantenimiento y reportes. Solo el responsable del sistema es el encargado de analizar estos datos.

III. REGISTRO DE INCIDENTES:

Cuando hay un incidente, este se registra en un sistema de tickets llamado Request Tracker. Ahí se registra el problema y la solución. También se registra el nombre de la persona que resolvió el problema y si requirió ayuda de soporte técnico local o externo. Contamos con el soporte de la Dirección General de Bibliotecas que nos apoyan en la recuperación de datos. No hay soporte físico. Todo se maneja dentro del servidor de cómputo del sistema.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

En la puerta de entrada hay un vigilante las 24 horas. El vigilante se encarga de solicitar en el acceso que se identifique con credencial y el nombre de la persona que visita. Se le habla por teléfono a la persona de la dependencia para que vaya personalmente a recibir al visitante. Solo personal autorizado podrá ingresar al estacionamiento, pues se requiere tarjeta magnética.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso a la oficina es mediante una identificación biométrica de huella digital. Durante las 8 horas de jornada hay una asistente en la puerta que recibe a las personas y les pregunta el motivo de su visita. Así mismo hay cámaras de videovigilancia en la entrada de la oficina. Entonces llama al responsable del centro de cómputo para que le de la bienvenida. Para entrar al centro de cómputo solo el responsable de cómputo tiene la llave para dar acceso.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Solo el responsable y el encargado tienen la facultad para actualizar datos. Eso se hace mediante el uso de una aplicación llamada CIRCULA, que permite con usuario y contraseña hacer las modificaciones pertinentes. Se hacen los registros mediante el nombre de los usuarios, fechas de inicio de préstamos y terminación. Todos los días se hacen cambios y actualizaciones de acuerdo a la demanda de los préstamos de libros. Ni siquiera la gente de cómputo local podrá hacer modificaciones. Este es un sistema administrado por la DGB-UNAM.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

El responsable y encargado de actualizar los datos tienen asignadas sus contraseñas para el uso de la herramienta CIRCULA y los módulos de administración, mantenimiento y reportes en el módulo Mantale mediante usuario y contraseña.

Las contraseñas y usuarios no se cambian regularmente. Solo se hace un cambio en caso necesario a petición de los responsables y encargados. Estos responsables están debidamente identificados por funcionarios de mayor rango, como el Secretario Administrativo o la Jefa de Personal. En la actualidad no se tiene certificado SSL para el acceso al portal web de esta aplicación. En la siguiente versión del sistema llamado KOHA ya está considerado. Los nuevos perfiles se dan de alta por el área de soporte de la DGB. Para personal administrativo o de soporte del sistema el acceso remoto se hace mediante accesos controlados de “secure shell”. Así mismo, el acceso al hardware está controlado mediante usuarios y contraseña, y solo los responsables tienen estos controles. Los usuarios finales como los solicitantes de libros nunca tienen acceso a los datos personales. Solo tendrán acceso al acervo bibliográfico para seleccionar los libros de su interés con información pública.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Respaldos mensuales de Mantale

http://sitio.web.para.mantenimiento:

Ingresar con usuario y contraseña.

Menú: Administración del sistema
Seleccionar: Respaldar

Seleccionar:

Libros - centro de ciencias genómicas	l2401	l2450
Libros - instituto de biotecnología	l2601	l2650
Revistas - centro de ciencias genómicas	p2401	p2450
Revistas - instituto de biotecnología	p2601	p2650

Libros y Revistas y Obtener archivos de respaldo. Listado:

l2401.tar[fecha]
l2450.tar[fecha]
l2601.tar[fecha]
l2650.tar[fecha]
p2401.tar[fecha]
p2450.tar[fecha]
p2601.tar[fecha]
p2650.tar[fecha]

Los anteriores respaldos se copian en un folder de la interfase de un sitio en la nube de la cuenta “ati” del dominio “ccg.unam.mx”

RUTA
UATI-BC >> Respaldos >> ALEPH-MANTALE >>

NOMBRE DEL FOLDER
[MANTALE-FECHA-NOMBRE-DE-NAVEGADOR-DE-INTERNET]

Ejemplo: MANTALE-04082022-FIREFOX

El coordinador de cómputo se encarga de efectuar los respaldos completos mensualmente de manera manual. Contamos con el apoyo de la DGB para hacer la recuperación de datos.

IX. PLAN DE CONTINGENCIA

Tenemos soporte técnico de hardware y software. Tenemos equipo auxiliar de energía y dos acometidas de energía eléctrica. Pero no tenemos un plan de contingencia y no hay un sitio alterno. Se propondrá habilitar un sitio alterno considerando los costos que esto implica.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

BIBLIOTECA DEL CCG		
Identificador único*	ccg-biblioteca-001-E-Aleph	
(Nombre del sistema A1)*	ALEPH	
Recurso*	**Descripción***	**Control***
Pruebas de registro de datos con aplicación CIRCULA.	Esta aplicación permite dar de alta registros, hacer modificaciones y cancelaciones. Así como consultar el acervo.	Tanto el responsable como el encargado podrán acceder a esta aplicación la cual nos permitirá comprobar que los datos están actualizados. Esta aplicación será usada para verificar si otros pueden acceder sin autorización. La licencia está incluida con el producto ALEPH.
Generación de pruebas de monitoreo y administración usando herramienta MANTALE.	Esta herramienta permite el monitoreo de los programas que mantienen activa la aplicación ALEPH. Así mismo se tiene acceso al módulo de respaldos de la base de datos y para obtener reportes de registros.	Para acceder a esta herramienta se requiere de usuario y contraseña. Se podrá mover fácilmente entre los menús para obtener la información de interés. El responsable es el coordinador de cómputo.

Revisiones aleatorias.	Se hace un procedimiento de revisión junto con el personal encargado para verificar que se sigue el procedimiento definido para dar de alta registros, modificaciones y cancelaciones.	El responsable tendrá una sesión dedicada con el encargado de hacer las modificaciones para comprobar que los datos son correctos y completos. Se usarán las herramientas CIRCULA y MANTALE para verificar.

7.2. Procedimiento para la revisión de las medidas de seguridad

BIBLIOTECA DEL CCG		
Identificador único*	ccg-biblioteca-001-E-Aleph	
(Nombre del sistema A1)*	ALEPH	
Medida de seguridad*	**Procedimiento***	**Responsable***
Respaldos de la base de datos.	Se hace un respaldo total mensual de las bases de datos utilizando la herramienta MANTALE.	Unidad de Administración de TI. 1 día.
Se revisan bitácoras del servidor (logs).	Se revisan archivos de registros de accesos a las cuentas de usuarios del servidor.	Unidad de Administración de TI. 1 día.

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

BIBLIOTECA DEL CCG	
Identificador único*	ccg-biblioteca-001-E-Aleph

(Nombre del sistema A1)*	ALEPH	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Respaldos de la base de datos.	Se han revisado la integridad de los respaldos con el apoyo de la DGB. Todo en buen estado.	Unidad de Administración de TI. 1 día. Y con apoyo de la unidad de cómputo de la DGB.
Se revisan bitácoras del servidor (logs).	Se han registrado intentos de acceso. Todos los intentos ajenos han sido fallidos.	Unidad de Administración de TI. 1 día. Y con apoyo de la unidad de cómputo de la DGB.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

BIBLIOTECA DEL CCG		
Identificador único*	ccg-biblioteca-001-E-Aleph	
(Nombre del sistema A1)*	ALEPH	
Medida de seguridad*	**Acciones***	**Responsable***
Respaldos de la base de datos	Anotar en calendario de respaldos la realización de cada evento. Respaldar dos veces por mes.	Unidad de Administración de TI
Se revisan bitácoras del servidor (logs)	Instalar herramientas de bloqueo ante varios intentos fallidos.	Unidad de Administración de TI

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

BIBLIOTECA DEL CCG			
Identificador único*	ccg-biblioteca-001-E-Aleph		
(Nombre del sistema A1)*	ALEPH		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Introducción a la protección de datos personales	Se dará capacitación básica Se presentará material proporcionado por la Unidad de Transparencia	Duración, 2 horas. Noviembre de 2022	Responsables de las áreas internas que tratan con datos personales. Capacitación semestral.

8.2. Programa de difusión de la protección a los datos personales

BIBLIOTECA DEL CCG			
Identificador único*	ccg-biblioteca-001-E-Aleph		
(Nombre del sistema A1)*	ALEPH		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Correo electrónico.	Se enviará recordatorios sobre el tema de datos personales y se	Difusión regular trimestral. Iniciando en septiembre de 2022.	Público en general y responsables de tratamientos de datos personales.

	recordará dónde hallar información.		
Carteles.	Se colocarán carteles en lugares públicos para hacer conciencia de proteger los datos personales.	Difusión semestral iniciando en septiembre de 2022	Público en general.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

BIBLIOTECA DEL CCG			
Identificador único*	ccg-biblioteca-001-E-Aleph		
(Nombre del sistema A1)*	ALEPH		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de sistema de préstamos. Cambio de ALEPH a KOHA.	Se dispondrá de servidor, sistema operativo y sistema de información nuevos.	Inicio 1 de marzo de 2022. Fin el 1 de septiembre de 2022.	Este sistema de información será un sistema nuevo con software de distribución libre. Se ahorra el pago de licencias.

9.2. Actualización y mantenimiento de equipo de cómputo

BIBLIOTECA DEL CCG			
Identificador único*	ccg-biblioteca-001-E-Aleph		
(Nombre del sistema A1)*	ALEPH		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Mantenimiento de equipo.	Este sistema será actualizado con un hardware nuevo y con versiones de sistema operativo nuevas.	El equipo nuevo se instalará y se harán actualizaciones de sistema operativo y firmware. Esta actividad se hará en 5 días.	Tendremos hardware nuevo con garantía y soporte técnico adicional.

9.3. Procesos para la conservación, preservación y respaldos de información

BIBLIOTECA DEL CCG		
Identificador único*	ccg-biblioteca-001-E-Aleph	
(Nombre del sistema A1)*	ALEPH	
Proceso*	**Descripción***	**Responsable***
Los respaldos se guardan en la nube. Se revisará que haya espacio suficiente.	Se ingresa al servicio en la nube y se medirá el espacio disponible para respaldos. Los respaldos de más de tres años se borrarán para evitar saturación.	Unidad de Administración de TI

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

BIBLIOTECA DEL CCG		
Identificador único*	ccg-biblioteca-001-E-Aleph	
(Nombre del sistema A1)*	ALEPH	
Proceso*	**Descripción***	**Responsable***
Se formatean los discos con herramientas de S.O. Unix a bajo nivel.	En este caso se pueden usar herramientas de formateo como mkfs, fdisk o gpart. Se extraerán los discos y se formatean en otros sistemas con herramientas de bajo nivel.	Unidad de Administración de TI

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Cuando sea requerida la cancelación de un sistema de tratamiento de datos personales se deberá seguir el procedimiento aquí descrito.

A) ESPECIFICAR DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Identificador único
b) Denominación
c) Área responsable del sistema
d) Responsable del sistema
e) Motivo de la cancelación
f) Autorización de los responsables para la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

a) Solicitud y autorización de los responsables para llevar a cabo el bloqueo del sistema

b) Aviso a los responsables, encargados y usuarios del bloqueo del sistema
c) Fecha de inicio de bloqueo
d) Período de bloqueo
e) Se comunicará al responsable el procedimiento de bloqueo

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

a) Se especificará el motivo del bloqueo
b) Se verificará que existe un respaldo el mismo día que inicia el bloqueo
c) Se hará un procedimiento en caso de retorno al punto antes del bloqueo
d) Se verificará que todo está funcionando en el momento mismo del bloqueo
e) Se darán de baja los procesos del servidor de web o conexiones vía terminal para evitar accesos.
f) Solo se permitirá acceso a usuario único desde la consola del sistema
g) Se comunicará a los responsables, encargados y usuarios el tiempo que durará el bloqueo.
h) Se informará cuando termine el tiempo de bloqueo y se proceda a suprimir el sistema

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

a) Cuando se proceda a la supresión del sistema se avisará que el sistema dejará de operar definitivamente. La información del sistema que se suprimirá estará disponible en otras herramientas de consulta.
b) El servidor se desconectará de la red de datos para evitar cualquier acceso
c) Se darán de baja los procesos del manejador de base de datos.
d) Se desinstalarán los programas que mantenían el sistema operando.

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

a) Se borrarán los datos del sistema con comandos útiles del sistema operativo
b) Se desmontarán los discos para hacer el borrado seguro desde otra máquina
c) En caso de que no se pueda borrar en otra máquina debido a incompatibilidad entonces se destruirán los discos con medio mecánicos.
d) Se instalarán de nuevo los discos y se instalará otra versión de sistema operativo para darle uso al equipo en caso de que aun tenga utilidad para otros sistemas

FUNDANET (ccg-sacad-001-E-Fundanet)

Sistema para la gestión de la información académica de los investigadores y técnicos académicos del CCG.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONAL

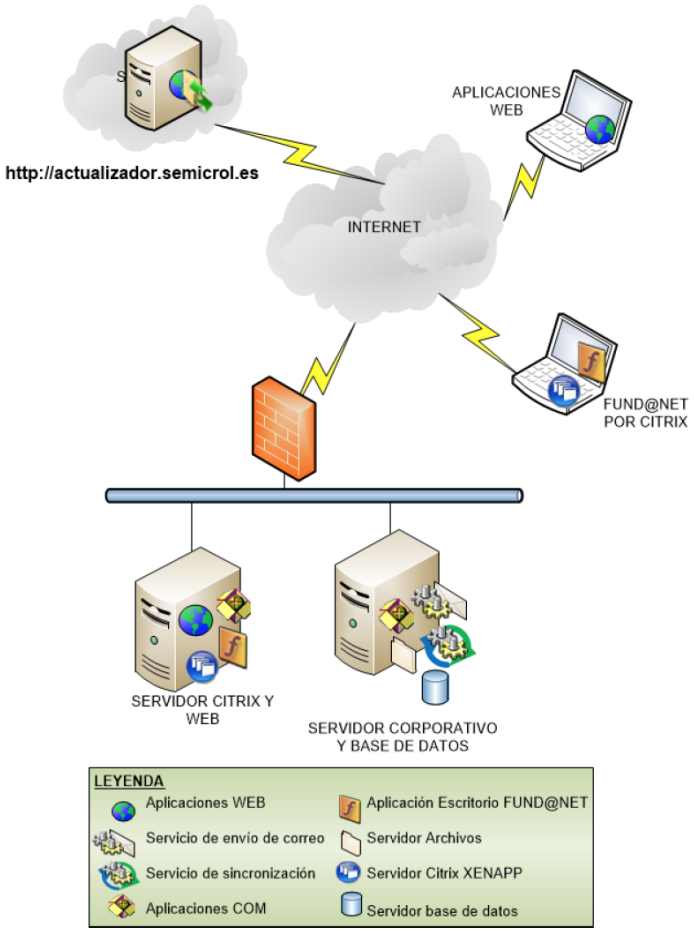
SECRETARÍA ACADÉMICA DEL CCG	
Identificador único*	ccg-sacad-001-E-Fundanet
(Nombre del sistema A1) *	Fundanet
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación, datos laborales y producción científica
Responsable*:	**Secretaría Académica**
Nombre*:	**Dr. Sergio Encarnación**
Cargo*:	**Secretario Académico**
Funciones*:	Verificar que la información académica se encuentre actualizada.
Obligaciones*:	Incentivar al personal académico a utilizar el sistema. Supervisar el cumplimiento de lineamientos para la protección de datos personales.
	Encargados:
(Nombre del Encargado 1*)	**Víctor Del Moral Chávez**

Cargo*:	**Coordinador de la UATI**
Funciones*:	Responsable de los datos personales del sistema del CCG
Obligaciones*:	Asegurar el cumplimiento de los lineamientos y normas en relación al tratamiento de los datos personales, y establecer medidas organizativas y técnicas para garantizar un nivel de seguridad adecuado
(Nombre del Encargado 2*)	**Vicente Osorio Mora**
Cargo*:	**Técnico por honorarios**
Funciones*:	Dar seguimiento al tratamiento de los datos personales del sistema
Obligaciones*:	Mantenimiento y actualización de información en el sistema
	Usuarios:
(Nombre del Usuario 1*)	Lorena García
Cargo*:	Asistente de la Secretaría Académica
Funciones*:	Consultora de información
Obligaciones*:	Verificadora de la integridad de la información, generación de informes

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

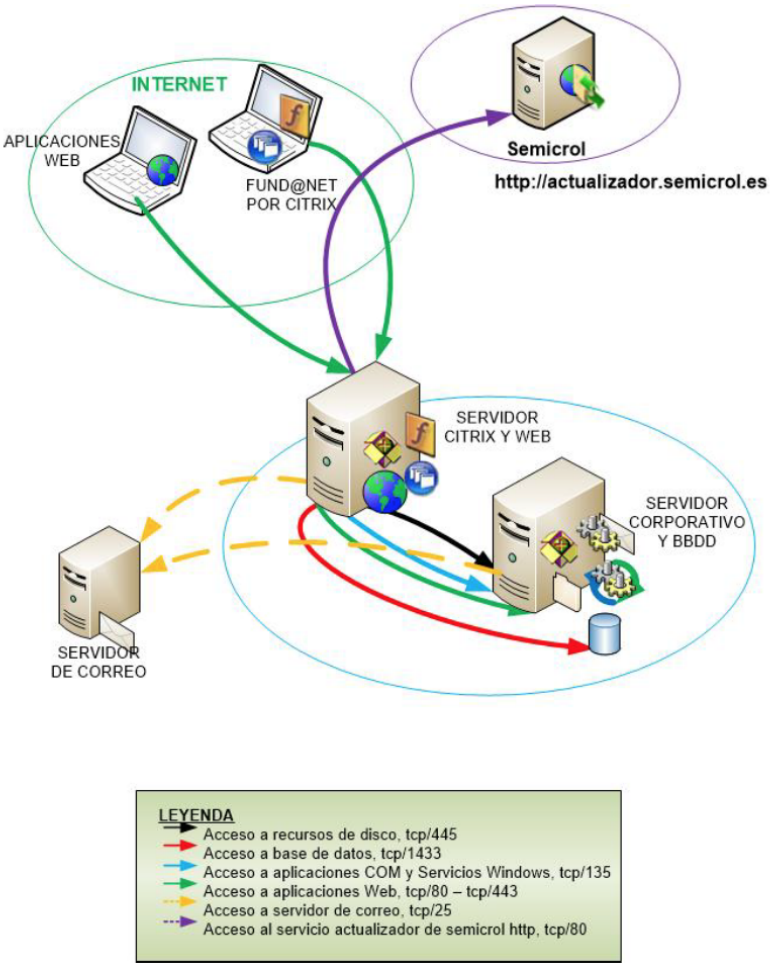
SECRETARÍA ACADÉMICA DEL CCG	
Identificador único¨*	ccg-sacad-001-E-Fundanet
(Nombre del sistema A1*)	Fundanet
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos relacional y servidor de alojamiento
Características del lugar donde se resguardan los soportes:*	Centro de cómputo donde se encuentra el servidor: - Acceso por medio de huella digital al laboratorio - Uso de llave para acceso al Centro de cómputo - Aire acondicionado de confort - Luz artificial - Piso falso - Alimentación eléctrica con equipos de respaldo de energía en línea Acceso al servidor: - Usuario y password - Uso de certificados SSL **ARQUITECTURA FÍSICA DEL SISTEMA.** A continuación, se describen los servidores que forman la solución genérica. **Servidor corporativo y de base de datos.** Como servidor corporativo: **Servicio de sincronización**. Servicio utilizado para sincronizar la aplicación de escritorio con los últimos binarios aprobados para actualizar. **Cliente actualizador**. Aplicación que descarga las actualizaciones disponibles del producto de http://actualizador.semicrol.es y las instala en los servidores. **Servicio de envío de correo**. Servicio que automatiza el envío de correos desde la aplicación. Este servicio permite enviar correos en grupos limitados y con cierta cadencia. **Gestores documentales**. Aplicaciones y servicios encargados de gestionar la información digital utilizada por Fund@net.

	Repositorio de documentos. Repositorio de documentos contiene los binarios, las imágenes, las plantillas de los documentos que se generan, una carpeta de parámetros donde se almacena la configuración personalizada de cada usuario y un archivo de registro de los errores que se produzcan. También contiene el paquete de instalación para la aplicación cliente de escritorio. Adicionalmente, almacena la información digital utilizada por Fund@net. Como servidor de bases de datos contiene un motor de bases de datos SQL Server que servirá a las bases de datos de producción de Fund@net. Adicionalmente, puede contener la base de datos de configuración de XenApp. **Servidor Web y Citrix XenApp** Servidor de aplicaciones para la ejecución en remoto a través de Internet de la aplicación de Escritorio mediante un canal seguro y de las aplicaciones Web de Fund@net.



Interconexión del sistema.

A continuación, se muestra un esquema de la interconexión de los componentes así como de los servidores externos a la aplicación que son necesarios:



3. ANÁLISIS DE RIESGOS

Ver Anexo I: Análisis de riesgos.

4. Análisis de Brecha

Ver Anexo II: Análisis de brecha.

5. PLAN DE TRABAJO

Ver Anexo III: Plan de trabajo.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Secretaría Académica del CCG	
Identificador único*	ccg-sacad-001-E-Fundanet
(Nombre del sistema A1)*	Fundanet
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza tratamiento de datos personales en soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza tratamiento de datos personales en soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Se realiza transferencia de datos entre este sistema y el sitio web principal del CCG, por medio de una conexión cifrada (HTTP+SSL) a la interfaz de programación de esta aplicación (API tipo REST) sobre la red local. Esta transferencia se realiza de forma manual cuando se requiere actualizar datos en el sitio web. En caso de que se requiera compartir la información con sistemas o entidades externas, esta es enviada a través de internet mediante servicios en la nube. En caso de que se realicen transferencias mediante el traslado sobre redes electrónicas se requiere un oficio de colaboración entre las dos partes. Sin estos oficios el traslado de información no puede realizarse.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se realiza tratamiento de datos personales en soportes físicos.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

No se cuenta con bitácoras de acceso al sistema por parte de los usuarios y gestores. Las bitácoras con las que se cuenta corresponden a los respaldos de la base de datos del sistema, contemplando fecha y hora de respaldo. Dichas bitácoras se encuentran en soporte electrónico y se encuentran disponibles para los responsables del sistema.

III. REGISTRO DE INCIDENTES:

Cuando se presenta un incidente, ya sea identificado por el responsable o encargado del sistema, este se registra en un sistema de tickets llamado Request Tracker para reportarlo al proveedor Semicrol. Se describe el problema y la solución a detalle. También, se registra el nombre de la o las personas que resolvieron el problema y si se requirió ayuda de soporte técnico local o externo. Una vez encontrada la solución se notifica a quien haya reportado el incidente (en caso de que haya sido por un usuario).

En caso de ser necesario, únicamente el Usuario del sistema será quien podrá realizar la solicitud de recuperación de datos, para lo cual los Encargados del sistema evaluarán las alternativas para llevar a cabo la recuperación correspondiente.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

En la puerta de entrada a la dependencia hay un vigilante las 24 horas. El vigilante se encarga de solicitar al visitante que se identifique mostrando una credencial oficial o documento de identidad, así como el nombre de la persona que visita. Además, se le pide al visitante que registre su entrada en una bitácora (fecha, hora de entrada, nombre, procedencia, nombre de la persona o área que visita, hora de salida).

Se le habla por teléfono a la persona de la dependencia para que vaya personalmente a recibir al visitante. Solo personal autorizado podrá ingresar al estacionamiento, ya que se requiere tarjeta magnética.

Adicionalmente, la dependencia cuenta con un sistema de cámaras de videovigilancia, al que solamente tiene acceso el personal de vigilancia y el Departamento de Servicios Generales.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso a la oficina o laboratorio es mediante una identificación biométrica de huella digital. Durante las 8 horas de jornada hay una asistente en la puerta que recibe a las personas y les pregunta el motivo de su visita. Así mismo, hay cámaras de videovigilancia en la entrada de la

oficina o laboratorio. Solo el responsable del centro de cómputo cuenta con la llave para acceder al centro de cómputo.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Solo los encargados tienen la facultad para actualizar datos en el sistema. La información se actualiza conforme al requerimiento de los usuarios finales del sistema (investigadores y/o técnicos académicos), quienes se encargan de hacer llegar su solicitud a través del sistema de tickets Request Tracker. Por otro lado, en el caso de los artículos, la actualización de la información correspondiente se realiza una vez al mes por parte del encargado del sistema.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

El sistema de Fundanet cuenta con los siguientes roles y permisos: usuario Web y usuario Gestor.

Los encargados de actualizar los datos tienen asignados sus datos de acceso (usuario y contraseña) para el uso del sistema.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

El servidor donde se encuentra instalado Fundanet cuenta con sistema operativo Windows Server 2012 R2 Standard, y se cuenta con la gestión de acceso al servidor mediante usuarios y contraseñas (cifradas por medio del sistema operativo).

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

Adicionalmente, el sistema del Fundanet se encarga de cifrar las contraseñas de los usuarios que se encuentran registrados.

Los usuarios finales, pueden cambiar su contraseña desde la liga para acceder a su información personal en el apartado de ¿Has olvidado tu contraseña?, donde se le enviará un correo electrónico para modificar su contraseña.

4. Administración de perfiles de usuario y contraseñas:

Respecto a la administración de perfiles de usuario y contraseñas, el usuario con el rol de gestor del sistema es quien cuenta con los permisos necesarios para crear los nuevos perfiles que se requieran. La Secretaría Académica de la dependencia es quien se encarga de solicitar y autorizar la creación de nuevos perfiles.

5. Acceso remoto al sistema de tratamiento de datos personales:

Los usuarios finales no requieren acceso remoto al equipo de cómputo para trabajar con el sistema, ya que opera vía web. A los usuarios finales, se les proporciona un enlace para hacer uso del mismo.

Para el mantenimiento, el encargado del sistema si requiere el acceso remoto para realizar tareas de administración y/o actualizaciones del sistema. El *encargado del sistema* requiere acceso a la aplicación de administración (Citrix Xenapp) mediante un acceso remoto vía una red privada virtual (Citrix Gateway).
Los encargados del sistema tienen acceso remoto al equipo mediante el servicio de escritorio remoto (RDP) propio del sistema operativo Windows.

Con la finalidad de evitar el acceso remoto no autorizado, se hace uso de las reglas de bloqueo del Firewall con el que cuenta el servidor donde se aloja el sistema.

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

Los respaldos de la base de datos del sistema se realizan por el encargado de manera semanal y en forma manual. Estos respaldos son resguardados en la nube, y son nombrados por la fecha en que fueron realizados, por ejemplo: CCGUNAM_Fundanet_backup_2022_08_11.bak

IX. PLAN DE CONTINGENCIA

Se cuenta con soporte técnico de hardware y software. Tenemos equipo auxiliar de energía y dos acometidas de energía eléctrica. Se trabajará en la definición de un plan de contingencia. Por el momento no se cuenta con un sitio redundante o alterno. Se propondrá habilitar un sitio alterno bajo la consideración de los costos que esto implica.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Secretaría Académica del CCG	
Identificador único*	ccg-sacad-001-E-Fundanet
(Nombre del sistema A1)*	Fundanet

Recurso*	Descripción*	Control*
Bitácora o registro de histórico de sucesos.	Registro en la base de datos de la aplicación de todas las operaciones realizadas por el gestor y los usuarios, incluyendo fecha, hora, acción.	Revisión periódica de forma manual, después de cierto tiempo el encargado podría detectar sucesos anómalos.
Herramientas para análisis de seguridad del servidor.	Herramientas para análisis de vulnerabilidades, escaneo de puertos y pruebas de penetración.	Pruebas periódicas realizadas por el CERT UNAM y aviso al responsable de TI de la dependencia en caso de encontrar alguna vulnerabilidad, para implementar los mecanismos de seguridad complementarios.

7.2. Procedimiento para la revisión de las medidas de seguridad

Secretaría Académica del CCG		
Identificador único*	ccg-sacad-001-E-Fundanet	
(Nombre del sistema A1)*	Fundanet	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos.	Realización del respaldo de la base de datos de forma manual, y de manera semanal, usando la herramienta de administración de la base de datos.	Encargado del sistema 2 días de la actividad

Actualización del certificado de seguridad.	Solicitud de la renovación del certificado a la DGTIC de manera anual (octubre).	Encargado del sistema 15 días
Actualización de la aplicación.	Actualización de los programas y base de datos de acuerdo al calendario de liberación de versiones del proveedor.	El responsable en este caso es un proveedor (la empresa externa) bajo la supervisión del Responsable del sistema. Tiempo variable

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Secretaría Académica del CCG		
Identificador único*	ccg-sacad-001-E-Fundanet	
(Nombre del sistema A1)*	Fundanet	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Respaldos.	Verificación del respaldo.	Encargado del sistema en conjunto con la UATI
Actualización del certificado de seguridad.	El certificado SSL está vigente hasta octubre 2022.	Encargado del sistema en conjunto con la UATI
Actualización de la aplicación.	De acuerdo al proveedor, la aplicación está actualizada a su versión estable más reciente.	Encargado del sistema en conjunto con la UATI

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Secretaría Académica del CCG		
Identificador único*	ccg-sacad-001-E-Fundanet	
(Nombre del sistema A1)*	Fundanet	
Medida de seguridad*	**Acciones***	**Responsable***
Respaldos.	Automatizar la generación del respaldo de la base de datos cada cierto tiempo (periodo fijo).	Encargado del sistema en conjunto con la UATI
Actualización del certificado de seguridad.	Definir un plan de actividades relacionadas a la administración, actualización y mantenimiento completo del sistema y servidor donde se aloja.	Encargado del sistema en conjunto con la UATI
Actualización de la aplicación.	Definir un plan de actividades relacionadas a la administración, actualización y mantenimiento completo del sistema y servidor donde se aloja.	Encargado del sistema en conjunto con la UATI

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

Secretaría Académica del CCG

Identificador único*	ccg-sacad-001-E-fundanet
(Nombre del sistema A1)*	Fundanet

Actividad*	Descripción*	Duración*	Cobertura*
Cursos en línea.	Cursos en línea ofrecidos por la DGTIC y la Unidad de Transparencia, por ejemplo Medidas de Seguridad Técnicas para la Protección de Datos Personales.	Según calendario de oferta de cursos de la DGTIC.	Responsables de TI y encargado de los sistemas de las dependencias de la UNAM.

8.2. Programa de difusión de la protección a los datos personales

Secretaría Académica del CCG	
Identificador único*	ccg-sacad-001-E-fundanet
(Nombre del sistema A1)*	Fundanet

Actividad*	Descripción*	Duración*	Cobertura*
Mensajes por correo electrónico.	Mensajes a los usuarios del sistema con recomendaciones sobre cuidado de sus datos personales, en particular sus contraseñas y protección frente a	1 día de manera periódica a lo largo del año	Toda la comunidad del CCG.

	mensajes de correo engañosos.		
Carteles.	Se colocarán carteles en lugares públicos para hacer conciencia de proteger los datos personales.	Difusión semestral iniciando en septiembre de 2022	Público en general.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Secretaría Académica del CCG			
Identificador único*	ccg-sacad-001-E-Fundanet		
(Nombre del sistema A1)*	Fundanet		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de la información de los investigadores y/o técnicos académicos.	Mejorar el sistema de información actual, a partir de peticiones de los usuarios, con motivo de un problema detectado o bien por la necesidad de actualización del mismo o de la información que se almacena en él.	De acuerdo a la necesidad de cada usuario, el cual realiza una petición a través de un correo electrónico (ticket) dirigido al encargado del sistema Fundanet.	Toda la comunidad del CCG.

9.2. Actualización y mantenimiento de equipo de cómputo

Secretaría Académica del CCG			
Identificador único*	ccg-sacad-001-E-Fundanet		
(Nombre del sistema A1)*	Fundanet		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Definir un plan de actividades relacionadas a la administración, actualización y mantenimiento completo del servidor donde se aloja el sistema.	Calendarizar las actividades relacionadas a la actualización del equipo de cómputo o servidor donde está hospedado el sistema.	1 semana (enero 2023)	Estado físico del servidor e interconexión con otros dispositivos, así como de las actualizaciones de software requeridas para su correcto funcionamiento.

9.3. Procesos para la conservación, preservación y respaldos de información

Secretaría Académica del CCG	
Identificador único*	ccg-sacad-001-E-fundanet

(Nombre del sistema A1)*	Fundanet	
Proceso*	**Descripción***	**Responsable***
Los respaldos se guardan en la nube. Se revisará que haya espacio suficiente.	Se ingresa al servicio en la nube y se medirá el espacio disponible para respaldos. Los respaldos de más de tres años se borrarán para evitar saturación.	Encargado del sistema 2 días

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Secretaría Académica del CCG		
Identificador único*	ccg-sacad-001-E-fundanet	
(Nombre del sistema A1)*	Fundanet	
Proceso*	**Descripción***	**Responsable***
Formateo a bajo nivel de los discos.	De acuerdo al sistema operativo, se selecciona la aplicación adecuada para realizar el formateo del disco asegurando que cuenten con la opción de borrado seguro de la información, por ejemplo, en el caso de sistema operativo Windows: SDelete o Eraser MacOS: Permanent eraser o Disk Utility.	Unidad de Administración de TI 2 días

Destrucción del medio.	Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo.	Unidad de Administración de TI 2 días

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Para llevar a cabo la cancelación del sistema Fundanet, se realiza el procedimiento que se describe a continuación.

Únicamente el director o directora de la entidad, junto con Secretaría Académica y Secretaría técnica podrán solicitar la cancelación del sistema, describiendo:

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

Dicha petición será realizada al Encargado de la UATI para determinar junto con el encargado del sistema las actividades a realizar.

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

Para cancelar el sistema se debe:

- Recibir la notificación de bloqueo del sistema por parte del director o directora de la entidad, la Secretaría Académica o la Secretaría Técnica
- Notificar a la comunidad de usuarios de la dependencia que el sistema no se encontrará activo, indicando la fecha en que ya no se podrá acceder a él, en principio se definen tres meses, sin embargo, queda a consideración de lo acordado entre el solicitante y los encargados del sistema
- Retirar el acceso a los usuarios por medio del servicio web (https) del sistema Windows Server

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE

- El encargado del sistema debe realizar el respaldo más actualizado de la base de datos
- El respaldo debe resguardarse bajo el procedimiento definido por la UATI

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

- Ingresar al servidor donde se aloja la base de datos Fundanet
- Eliminación, borrado o destrucción de datos personales de dicha base de datos
- Borrar la base de datos del sistema Fundanet

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

- Ingresar al servidor donde se aloja la base de datos Fundanet
- Eliminar la base de datos
- Eliminar las máquinas virtuales
- Formateo del sistema operativo Windows Server
- Formateo a bajo nivel de los discos directamente en el medio de almacenamiento

SITIOS WEB (ccg-uati-001-E-SitiosWeb)

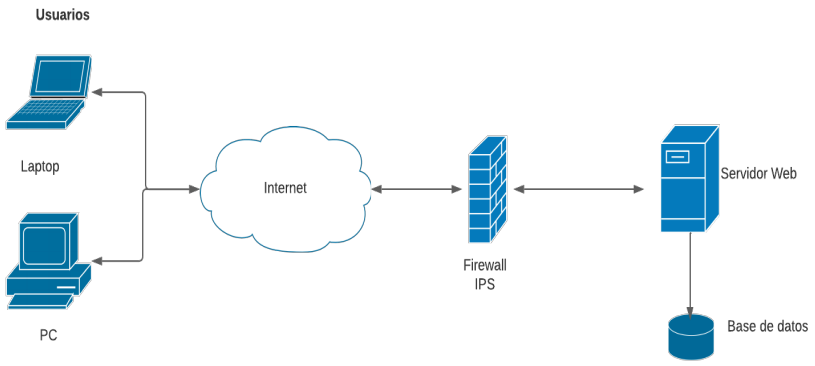
Conjunto de sitios web utilizados en el CCG, LCG y el NNB-CCG. Mediante estos sitios se publica información de interés sobre cada uno de los grupos mencionados, la información desplegada está disponible para todo el público.

1. **INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES**

UNIDAD DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN (UATI)	
Identificador único*	ccg-uati-001-E-SitiosWeb
(Nombre del sistema A1) *	Sitio Web del CCG
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación, datos laborales, producción científica.
Responsable*:	**Dirección**
Nombre*:	**Dr. Christian Sohlenkamp**
Cargo*:	**Director del CCG**
Funciones*:	Asignar funciones para el desarrollo del sistema y actualización de la información.
Obligaciones*:	Asegurar que los responsables del tratamiento de los datos personales cumplan con las normas definidas por la UNAM.
	Encargados:
Nombre*:	**Víctor Del Moral**
Cargo*:	**Coordinador de la UATI**
Funciones*:	Responsable de los datos personales del sistema del CCG.
Obligaciones*:	Asegurar el cumplimiento de los lineamientos y normas en relación al tratamiento de los datos personales, y establecer medidas organizativas y técnicas para garantizar un nivel de seguridad adecuado

(Nombre del Encargado 1*)	**Vicente Osorio Mora**
Cargo*:	**Técnico por honorarios**
Funciones*:	Dar seguimiento al tratamiento de los datos personales del sistema.
Obligaciones*:	Mantenimiento y actualización de información en el sistema.
(Nombre del Encargado 2*)	**Alfredo Hernández Álvarez**
Cargo*:	**Técnico Académico Titular A Tiempo Completo**
Funciones*:	Administración del servidor Web.
Obligaciones*:	Configuración, actualización y mantenimiento del sitio Web.
	Usuarios:
(Nombre del Usuario 1*)	**Lorena García Rivas**
Cargo*:	Asistente de Secretaria Académica
Funciones*:	Subir documentos que consultarán diferentes comités académicos.
Obligaciones*:	Asegurar que se suba la información correcta y que se elimine cuando ya no sea necesaria.

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

UATI	
Identificador único¨*	ccg-uati-001-E-SitiosWeb
(Nombre del sistema A1*)	Sitio Web del CCG
Tipo de soporte:*	Soporte electrónico
Descripción:*	Base de datos relacional y aplicación web
Características del lugar donde se resguardan los soportes:*	Centro de cómputo donde se encuentra el servidor y máquinas virtuales: - Acceso por medio de huella digital al laboratorio u oficina - Uso de llave para acceso al Centro de cómputo - Aire acondicionado de confort - Luz artificial - Piso falso - Alimentación eléctrica con equipos de respaldo de energía en línea Acceso al servidor: - Usuario y password - Uso de certificados SSL **Arquitectura general de los componentes de los sitios web**  - Los servidores donde se alojan las máquinas virtuales se encuentran detrás de un firewall configurado para dar acceso solo a ciertos puertos necesarios para el funcionamiento de los sitios web

	- El acceso tanto a la aplicación web como a las bases de datos correspondientes cuentan con usuario y password; solo los encargados de administrar los sistemas conocen dicha información

3. ANÁLISIS DE RIESGOS

Ver Anexo I: Análisis de riesgos.

4. ANÁLISIS DE BRECHA

Ver Anexo II: Análisis de brecha.

5. PLAN DE TRABAJO

Ver Anexo III: Plan de trabajo.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UATI	
Identificador único*	ccg-uati-001-E-SitiosWeb
(Nombre del sistema A1)*	Sitios web del CCG
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realiza tratamiento de datos personales en soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realiza tratamiento de datos personales en soportes electrónicos.

Transferencias mediante el traslado sobre redes electrónicas:	Se realiza transferencia de datos entre el sistema web del CCG y Fundanet, por medio de una conexión cifrada (HTTP+SSL) a la interfaz de programación de esta aplicación (API tipo REST) sobre la red local. Esta transferencia se realiza de forma manual cuando se requiere actualizar datos en el sitio web. El resto de los sitios web del CCG no realizan transferencias mediante el traslado sobre redes electrónicas. En caso de que se requiera compartir la información con sistemas o entidades externas, esta es enviada a través de internet mediante servicios en la nube. En caso de que se realicen transferencias mediante el traslado sobre redes electrónicas con otras entidades se requiere un oficio de colaboración entre las dos partes. Sin estos oficios el traslado de información no puede realizarse.

I. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se realiza tratamiento de datos personales en soportes físicos.

II. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. Los datos que se registran en las bitácoras:

Las bitácoras del servidor web registran los accesos o consultas públicas que incluyen fecha, hora, dirección IP del visitante, y ruta accedida. Además, existe un log donde se registran los accesos fallidos al sistema usando cuentas y contraseñas incorrectas.

Por otra parte, en el sistema operativo de la máquina virtual también hay bitácoras de logs /var/log (messages, secure, fail2ban) donde se registran los intentos exitosos y fallidos.

Las bitácoras mencionadas se encuentran en soporte electrónico, y solo tienen acceso a ellas los encargados del sistema y el administrador del servidor. Estos se encargan de realizar una inspección manual periódicamente.

III. REGISTRO DE INCIDENTES:

Cuando se presenta un incidente, ya sea identificado por el responsable o encargado del sistema, o bien por parte de los usuarios, este se registra en un sistema de tickets con el que

cuenta la UATI. Se describe el problema, pruebas realizadas y la solución a detalle. También, se registra el nombre de la o las personas que resolvieron el problema y si se requirió ayuda de soporte técnico local o externo. Una vez encontrada la solución se notifica a quien haya reportado el incidente.

En caso de ser necesario, únicamente el Usuario del sistema será quien podrá realizar la solicitud de recuperación de datos, para lo cual los Encargados del sistema evaluarán las alternativas para llevar a cabo la recuperación correspondiente.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

En la puerta de entrada a la dependencia hay un vigilante las 24 horas. El vigilante se encarga de solicitar al visitante que se identifique mostrando una credencial oficial o documento de identidad, así como el nombre de la persona que visita. Además, se le pide al visitante que registre su entrada en una bitácora (fecha, hora de entrada, nombre, procedencia, nombre de la persona o área que visita, hora de salida).

Se le habla por teléfono a la persona de la dependencia para que vaya personalmente a recibir al visitante. Solo personal autorizado podrá ingresar al estacionamiento, ya que se requiere tarjeta magnética.

Adicionalmente, la dependencia cuenta con un sistema de cámaras de videovigilancia, al que solamente tiene acceso el personal de vigilancia y el Departamento de Servicios Generales.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso a la oficina o laboratorio donde se encuentra el Centro de cómputo es mediante una identificación biométrica de huella digital. Adicionalmente, hay cámaras de videovigilancia en la entrada de la oficina o laboratorio. Solo el responsable del Centro de cómputo cuenta con la llave para acceder a él.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Solo los encargados tienen la facultad para actualizar datos en el sistema.

La información que se muestra en el sitio CCG se actualiza conforme al requerimiento y verificación del comité editorial del CCG; en el sitio de la LCG se requiere la solicitud y verificación de la Jefa de Sección Escolar, y la aprobación de la Coordinación de la LCG; y en el caso del sitio del NNB-CCG se actualiza la información con base a la petición del comité directivo.

Cualquier cambio se lleva a cabo en conjunto con el encargado de cada sistemas. Las peticiones se las hacen llegar a través del sistema de tickets Request Tracker de la UATI.

Por otro lado, en el sitio CCG, hay casos particulares en los que los usuarios finales pueden solicitar la actualización de su información de manera directa y en conjunto con el encargado del sistema se corrigen los datos. En el caso de la información que se despliega en relación a las publicaciones de los investigadores y técnicos académicos, la actualización de los datos correspondientes se realiza una vez al mes por parte del encargado del sistema dados los procedimientos establecidos en el sistema Fundanet.

VII. PERFILES DE USUARIO Y CONTRASEÑAS

En este rubro el área universitaria deberá describir el esquema de perfiles de usuario y contraseñas que tiene implementado para control de acceso mediante una red electrónica.

1. Modelo de control de acceso (alguno de los siguientes):

El control de acceso a los sistemas está basado en usuarios y roles, mediante una matriz de permisos.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:
Se cuenta con un sistema operativo tipo UNIX en el servidor del sistema, que cifra la contraseña del usuario y mantiene una política de contraseñas robustas.
De igual forma, las contraseñas definidas para las cuentas de acceso por parte de los encargados a los sistemas mantienen una política de contraseñas seguras

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

El sistema cifra la contraseña del usuario para almacenarla en la base de datos.

4. Administración de perfiles de usuario y contraseñas:

El encargado del sistema es quien cuenta con los permisos necesarios para crear los nuevos perfiles que se requieran.

Los usuarios de los sistemas, o bien, el comité editorial del CCG; en el sitio de la LCG la Jefa de Sección Escolar, y la aprobación de la Coordinación de la LCG; y en el caso del sitio del NNB-CCG el comité directivo, son las figuras encargadas que autorizan la creación de nuevos perfiles. Los sistemas mantienen un registro histórico de las operaciones realizadas.

5. Acceso remoto al sistema de tratamiento de datos personales:

Los usuarios finales no requieren acceso remoto al equipo de cómputo para trabajar con el

sistema. Tienen acceso directo al sistema vía web desde cualquier lugar a través de internet.
El administrador requiere acceso remoto al servidor para hacer tareas propias de administración.
El acceso remoto no autorizado tanto al sistema como al servidor se evita mediante el uso de usuario y contraseña, y una matriz de roles y permisos. En el caso del acceso a los servidores, se tiene restringido el acceso a la red local por medio del firewall y se hace mediante una red privada virtual (VPN) y una conexión cifrada (SSH).

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

En el caso de los sitios web del CCG y NNB se realizan respaldos completos de las máquinas virtuales, de forma manual.
El respaldo de la máquina virtual se guarda y levanta en otro servidor.
El respaldo de la máquina virtual se coloca en el disco duro de otro servidor.

En el caso del sitio web de la LCG se generan archivos comprimidos de un vaciado de la base de datos y un empaquetado de los archivos de la aplicación, usando un script que se ejecuta en una tarea programada. Posteriormente, se almacenan en un servidor de respaldos, donde se depuran cada cierto tiempo.
El responsable de hacer el respaldo es el área universitaria.

IX. PLAN DE CONTINGENCIA

Se cuenta con soporte técnico de hardware y software. Tenemos equipo auxiliar de energía y dos acometidas de energía eléctrica. Se trabajará en la definición de un plan de contingencia. Por el momento, no se cuenta con un sitio redundante o alterno.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

UATI	
Identificador único*	ccg-uati-001-E-SitiosWeb
(Nombre del sistema A1)*	Sitios web del CCG

Recurso*	Descripción*	Control*
Bitácora o registro de histórico de sucesos.	Registro en la base de datos de la aplicación de todas las operaciones realizadas por los usuarios.	Revisión periódica de forma manual, después de cierto tiempo el encargado podría detectar sucesos anómalos.
Herramientas para análisis de seguridad del servidor.	Herramientas para análisis de vulnerabilidades, escaneo de puertos y pruebas de penetración.	Pruebas periódicas realizadas por el CERT UNAM y aviso al responsable de TI de la dependencia en caso de encontrar alguna vulnerabilidad, para implementar los mecanismos de seguridad complementarios.

7.2. Procedimiento para la revisión de las medidas de seguridad

UATI		
Identificador único*	ccg-uati-001-E-SitiosWeb	
(Nombre del sistema A1)*	Sitios web del CCG	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos.	Realización del respaldo de los archivos de la aplicación y de la base de datos de forma manual o automática, y de manera semanal. Verificación del respaldo.	Encargado del sistema 2 días de la actividad

Actualización del certificado de seguridad.	Solicitud de la renovación del certificado a la DGTIC de manera anual (septiembre-octubre).	Encargado del sistema 15 días
Actualización de la aplicación.	Actualización de los archivos y base de datos de la aplicación si hay nuevas versiones por parte del desarrollador.	Encargado del sistema. Tiempo variable

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UATI		
Identificador único*	ccg-uati-001-E-SitiosWeb	
(Nombre del sistema A1)*	Sitios web del CCG	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos.	Verificación del respaldo.	Encargado del sistema en conjunto con la UATI.
Actualización del certificado de seguridad.	El certificado SSL está vigente hasta octubre 2022.	Encargado del sistema en conjunto con la UATI.
Actualización de la aplicación.	Se revisará el procedimiento de la actualización de la aplicación y sus diferentes complementos.	Encargado del sistema en conjunto con la UATI.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

UATI		
Identificador único*	ccg-uati-001-E-SitiosWeb	
(Nombre del sistema A1)*	Sitios web del CCG	
Medida de seguridad*	**Acciones***	**Responsable***
Generación de respaldos.	Definir formalmente un plan de respaldos para tener el control de la información y en caso de requerirse su recuperación.	Encargado del sistema en conjunto con la UATI.
Actualización del certificado de seguridad.	Definir un plan de actividades relacionadas a la administración, actualización y mantenimiento completo del servidor donde se alojan los sistemas.	Encargado del sistema en conjunto con la UATI.
Actualización de la aplicación.	Definir un plan de actividades relacionadas a la administración, actualización y mantenimiento completo de los sistemas.	Encargado del sistema en conjunto con la UATI.

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

UATI

Identificador único*	ccg-uati-001-E-SitiosWeb
(Nombre del sistema A1)*	Sitios web del CCG

Actividad*	Descripción*	Duración*	Cobertura*
Cursos en línea.	Cursos en línea ofrecidos por la DGTIC y la Unidad de Transparencia, por ejemplo Medidas de Seguridad Técnicas para la Protección de Datos Personales.	Según calendario de oferta de cursos de la DGTIC.	Responsables de TI y encargado de los sistemas de las dependencias de la UNAM.

8.2. Programa de difusión de la protección a los datos personales

UATI	
Identificador único*	ccg-uati-001-E-SitiosWeb
(Nombre del sistema A1)*	Sitios web del CCG

Actividad*	Descripción*	Duración*	Cobertura*
Mensajes por correo electrónico.	Mensajes a los usuarios del sistema con recomendaciones sobre cuidado de sus datos personales, en particular sus contraseñas y protección frente a	1 día de manera periódica a lo largo del año.	Toda la comunidad del CCG.

	mensajes de correo engañosos.		
Carteles.	Se colocarán carteles en lugares públicos para hacer conciencia de proteger los datos personales.	Difusión semestral iniciando en septiembre de 2022	Público en general .

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

UATI			
Identificador único*	ccg-uati-001-E-SitiosWeb		
(Nombre del sistema A1)*	Sitios web del CCG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Uso de plugins.	Investigar y probar complementos que ayuden a añadir funcionalidades adicionales de seguridad tanto en el acceso al sistema como en la manipulación de los datos.	Duración variable. Actividad regular	Permite estar protegido ante posibles ataques o accesos no permitidos.

Actualización de la información.	A partir de peticiones de los usuarios o roles autorizados, subir, modificar o eliminar información desplegada en los sitios web.	Duración variable. Actividad regular.	Permite contar con la información más actual para la comunidad del CCG y público en general.
Actualización de la aplicación.	Realizar el plan de actualización de las aplicaciones.	1 semana	Permite reforzar la seguridad usando versiones más actuales, con menos vulnerabilidades.

9.2. Actualización y mantenimiento de equipo de cómputo

UATI			
Identificador único*	ccg-uati-001-E-SitiosWeb		
(Nombre del sistema A1)*	Sitios web del CCG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Definir un plan de actividades relacionadas a la administración, actualización y mantenimiento completo del servidor o servidores donde se alojan los sistemas.	Calendarizar las actividades relacionadas a la actualización del equipo de cómputo o servidor donde está hospedado el sistema.	1 semana (enero 2023)	Estado físico del servidor e interconexión con otros dispositivos, así como de las actualizaciones de software requeridas para su correcto funcionamiento.

9.3. Procesos para la conservación, preservación y respaldos de información

UATI		
Identificador único*	ccg-uati-001-E-SitiosWeb	
(Nombre del sistema A1)*	Sitios web del CCG	
Proceso*	**Descripción***	**Responsable***
Los respaldos se guardan en la nube. Se revisará que haya espacio suficiente.	Se respaldan los archivos de la aplicación y la base de datos. En algunos casos se respalda la máquina virtual completa.	Encargado del sistema 2 días

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UATI		
Identificador único*	ccg-uati-001-E-SitiosWeb	
(Nombre del sistema A1)*	Sitios web del CCG	
Proceso*	**Descripción***	**Responsable***
Formateo a bajo nivel de los discos.	De acuerdo al sistema operativo, seleccionar la aplicación adecuada para realizar el formateo del disco asegurando	Unidad de Administración de TI 2 días

	que cuenten con la opción de borrado seguro de la información.	
Destrucción del medio.	Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo.	Unidad de Administración de TI 2 días

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

- El encargado del sistema debe contar con la solicitud y autorización del responsable del sistema para llevar a cabo la cancelación del mismo
- El encargado del sistema junto con la Unidad de Administración de TI, debe definir el periodo de bloqueo (en principio se puede manejar 3 meses) y las actividades específicas a realizar para la cancelación
- Comunicar a los usuarios sobre el bloqueo del sistema, así como el periodo en que este se cancelará el sistema, especificar fecha

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

- Verificar que la documentación del estado reciente del servidor esté actualizada: versiones de sistema operativo, servidor web, bases de datos, lenguajes de programación y aplicación
- Respaldar las configuraciones de los servicios de web, bases de datos y el lenguaje de programación
- Respaldar los archivos y bases de datos del sistema, transferir al espacio definido de respaldos y verificar

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Al terminar el periodo de bloqueo:

- Comunicar a los usuarios la cancelación inminente del sistema
- Suspender el acceso al sistema, bloqueando las cuentas de usuarios y/o deshabilitar el servicio web
- Realizar último respaldo, transferir al sitio definido para los respaldos y verificarlo
- En caso de contar ya con un nuevo sistema, consolidar el plan de migración de datos
- Deshabilitar servicios web y de base de datos
- Desconectar el servidor de la red
- Realizar la eliminación segura de los archivos y bases de datos del sistema
- Notificar al responsable del sistema

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

- Borrado de archivos con comandos del sistema operativo
- Borrado de tablas y bases de datos con comandos del sistema manejador de bases de datos
- Eliminación de los volúmenes lógicos o arreglos de discos
- Formateo a bajo nivel de los discos duros
- Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo
- Reinstalación del sistema operativo

INTRANET DE LA LCG (ccg-uati-002-E-IntranetLCG)

Sistema que presenta información de interés únicamente para personal administrativo y académico, así como para estudiantes de la LCG, con acceso controlado.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

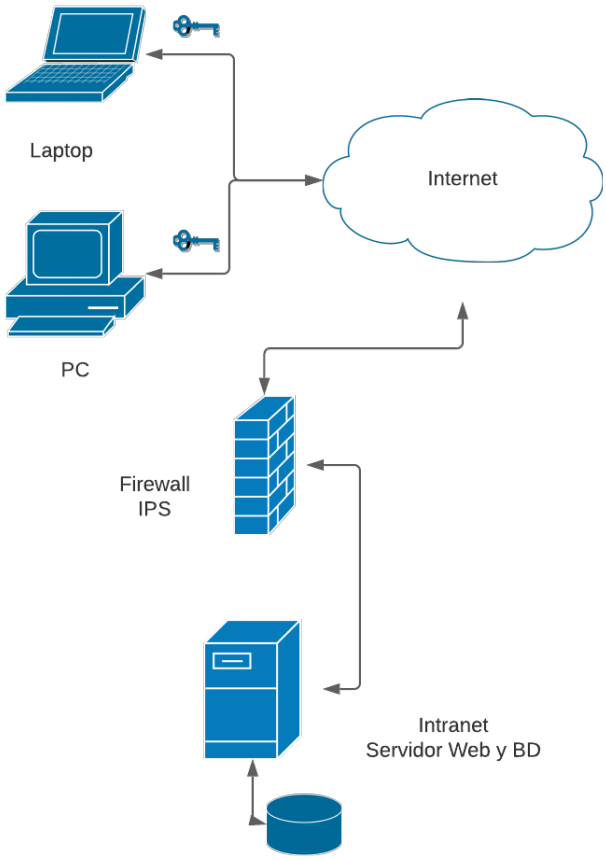
Licenciatura en Ciencias Genómicas	
Identificador único*	ccg-uati-002-E-IntranetLCG
(Nombre del sistema A1) *	Intranet de la LCG
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación, datos escolares, datos laborales.
Responsable*:	**Licenciatura en Ciencias Genómicas**
Nombre*:	Dr. Pablo Vinuesa Fleischmann
Cargo*:	Coordinador de la LCG
Funciones*:	Coordinación académica de las actividades de la LCG.
Obligaciones*:	Supervisar la publicación de información necesaria en la intranet LCG para aspirantes y alumnos.
	Encargados:
(Nombre del Encargado 1*)	**Alfredo José Hernández Alvarez**
Cargo*:	**Técnico Académico Titular A Tiempo Completo**
Funciones*:	Responsable del sitio web.
Obligaciones*:	Administración del sitio web, administración del servidor, establecer medidas técnicas de seguridad.

	Usuarios:
(Nombre del Usuario 1*)	Iliana Bahena Arellano
Cargo*:	Jefa de sección académica LCG
Funciones*:	Administración escolar de la LCG
Obligaciones*:	Consultar información de aspirantes, estudiantes y egresados; actualizar información de trámites escolares.
(Nombre del Usuario 2*)	Alumnos de la LCG
Cargo*:	
Funciones*:	
Obligaciones*:	Consultar información de trámites, actualizar información de algunos de estos trámites.

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

Licenciatura en Ciencias Genómicas	
Identificador único¨*	ccg-uati-002-E-IntranetLCG

(Nombre del sistema A1*)	Intranet de la LCG
Tipo de soporte:*	Soporte electrónico.
Descripción:*	Archivos de la aplicación web, imágenes, documentos, y base de datos relacional en el servidor
Características del lugar donde se resguardan los soportes:*	**Características** Del Centro de cómputo de la LCG: - aire acondicionado, - soporte de respaldo de energía, - acceso puerta aluminio/vidrio con llave, - puerta de madera de área previa con llave De acceso al servidor: - Usuario y contraseña - Protección de red perimetral equipo dedicado FortiGate (firewall y sistema de prevención de intrusiones) - Transmisión cifrada de datos por medio de certificados SSL **Componentes del sistema** - Servidor físico Sun - Sistema operativo tipo UNIX - Servidor web Apache - Servidor de base de datos MySQL - Sistema manejador de contenidos de código abierto **Diagrama de conexión**



3. ANÁLISIS DE RIESGOS

Ver Anexo I: Análisis de riesgos.

4. ANÁLISIS DE BRECHA

Ver Anexo II: Análisis de brecha.

5. PLAN DE TRABAJO

Ver Anexo III: Plan de trabajo.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

Licenciatura en Ciencias Genómicas	
Identificador único*	ccg-uati-002-E-IntranetLCG
(Nombre del sistema A1)*	Intranet de la LCG
TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias mediante traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias mediante traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Las transferencias se realizan mediante una conexión cifrada, esto es, mediante protocolo HTTP + SSL para acceso al sistema web a través de internet, y SSH para transferencia de los archivos de respaldo sólo en la red local. La conexión está protegida mediante un sistema de detección y protección de intrusiones en el firewall de red. Los accesos se registran en las bitácoras del firewall de red, el servidor y el sistema.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se realiza tratamiento de datos personales en soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   Las bitácoras del servidor web registran los accesos e incluyen fecha, hora, dirección IP del visitante, y ruta accedida
   Las bitácoras del sistema registran la siguiente información: accesos recientes, errores de “acceso denegado”, errores de “no encontrado”, referentes principales, visitantes principales, páginas visitadas; se incluye fecha, hora, IP del visitante y ruta accedida
2. **Si las bitácoras están en soporte físico o en soporte electrónico;**
   Las bitácoras se encuentran en soporte electrónico.
3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;**
   Las bitácoras del servidor se almacenan en un archivo de texto en el servidor web y se rotan cada semana.
   Las bitácoras del sistema se almacenan en la base de datos.
4. **La manera en que asegura la integridad de las bitácoras, y**
   Sólo el encargado del sistema y el administrador del servidor tienen acceso a las bitácoras.
   Las bitácoras están dentro del sistema y no se trasladan a ninguna otra parte.
5. **Respecto del análisis de las bitácoras:**
   El responsable de analizar las bitácoras es el área universitaria. El encargado del sistema y el administrador del servidor hacen una inspección manual periódicamente.

IV. REGISTRO DE INCIDENTES:

En la práctica cuando el usuario o el encargado del sistema identifican un incidente, lo reportan en un sistema de reporte de problemas y solicitudes (Request Tracker). Se describe el problema y qué servicio o sistema se ve afectado. Posteriormente el encargado o el personal técnico correspondiente, según el impacto, la urgencia y la prioridad del incidente, trabaja en la resolución del mismo. Cuando se resuelve, se describen las pruebas realizadas y la solución, se registra entre otras cosas la fecha, el sistema afectado, el nombre de la o las personas que intervinieron, el tiempo que llevó, y si se requirió ayuda de soporte técnico local o externo. Finalmente, se notifica la solución al usuario.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para acceso a la dependencia hay una caseta de vigilancia con un vigilante las 24 horas. El vigilante solicita al visitante que se identifique mostrando una credencial oficial o documento de identidad, y que registre su entrada en una bitácora (fecha, hora de entrada, nombre, procedencia, nombre de la persona o área que visita, hora de salida). El vigilante avisa por teléfono a la persona que visita y ésta autoriza el acceso.

Adicionalmente, la dependencia cuenta con un sistema de cámaras de videovigilancia, al que solamente tiene acceso el personal de vigilancia, autorizados por el Departamento de Servicios Generales.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso al centro de cómputo donde se ubica el servidor es mediante una primera puerta con llave, que da acceso a un área común, donde se cuenta con cámaras de videovigilancia. Posteriormente por una segunda puerta con llave se accede al centro de cómputo. Solamente los encargados de la administración de los servidores tienen acceso a ambas llaves. Los administradores son autorizados por la coordinación de la UATI.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización de la información contenida en el sistema requiere la solicitud y verificación con la Jefa de Sección Escolar, y la aprobación de la Coordinación de la LCG. Las actualizaciones se realizan de forma regular de acuerdo a las necesidades, conforme se va requiriendo, por ejemplo:

- En periodo de la apertura de la convocatoria de ingreso a la LCG, los aspirantes pueden agregar y editar su información personal y académica
- En el momento de su titulación, los alumnos agregan su información de titulación
- Después de titularse, el encargado actualiza la información académica del alumno

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

El control de acceso está basado en usuarios y roles, mediante una matriz de permisos.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

Se cuenta con un sistema operativo tipo UNIX en el servidor del sistema, que cifra la contraseña del usuario y mantiene una política de contraseñas robustas.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

El sistema cifra la contraseña del usuario para almacenarla en la base de datos.

4. Administración de perfiles de usuario y contraseñas:

El encargado del sistema crea los nuevos perfiles. La jefa de Sección Escolar y la Coordinación de la LCG autorizan la creación de nuevos perfiles. En ciertos períodos los propios usuarios pueden crear sus propios perfiles (p.ej los aspirantes en el periodo que se abre la convocatoria de ingreso). El sistema mantiene un registro histórico de las operaciones realizadas.

5. Acceso remoto al sistema de tratamiento de datos personales:

Los usuarios finales no requieren acceso remoto al equipo de cómputo para trabajar con el

sistema. Tienen acceso remoto directo al sistema vía web desde cualquier lugar en internet. El administrador requiere acceso remoto al servidor para hacer tareas propias de administración.
El acceso remoto no autorizado tanto al sistema como al servidor se evita mediante el uso de usuario y contraseña, y una matriz de roles y permisos. En el caso del acceso al servidor, se tiene restringido el acceso a la red local por medio del firewall y se hace mediante una red privada virtual (VPN) y una conexión cifrada (SSH).

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_**x**_, diferenciales ___ o incrementales___;
   b) De forma automática _**x**__ o Manual _____,
   c) Periodicidad con que los realiza: __semanal_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad:
   Disco duro.
3. Cómo y dónde archiva esos medios, y
   Se generan archivos comprimidos de un vaciado de la base de datos y un empaquetado de los archivos de la aplicación, usando un script que se ejecuta en una tarea programada. Posteriormente se almacenan en un servidor de respaldos, donde se depuran cada cierto tiempo.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

Como parte inicial de un plan de contingencia en desarrollo, se contempla que en el centro de cómputo donde está el servidor se cuenta con planta y equipo de respaldo de energía. Para el sistema se cuenta con los respaldos que pueden restaurarse en caso de una contingencia.

Por el momento no se cuenta con un sitio redundante o alterno.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

Licenciatura en Ciencias Genómicas

Identificador único*	ccg-uati-002-E-IntranetLCG	
(Nombre del sistema A1)*	Intranet de la LCG	
Recurso*	**Descripción***	**Control***
Bitácora o registro de histórico de sucesos.	Registro en la base de datos de la aplicación de todas las operaciones realizadas por los usuarios.	Revisión periódica de forma manual, después de cierto tiempo el encargado podría detectar sucesos anómalos.
Herramientas para análisis de seguridad del servidor.	Herramientas para análisis de vulnerabilidades, escaneo de puertos y pruebas de penetración.	Pruebas periódicas realizadas por el CERT UNAM y aviso al responsable de TI de la dependencia en caso de encontrar alguna vulnerabilidad, para implementar los mecanismos de seguridad complementarios.

7.2. Procedimiento para la revisión de las medidas de seguridad

Licenciatura en Ciencias Genómicas		
Identificador único*	ccg-uati-002-E-IntranetLCG	
(Nombre del sistema A1)*	Intranet de la LCG	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos.	Realización del respaldo de los archivos de la aplicación y de la base de datos de forma manual o	Encargado del sistema

	automática, y de manera semanal. Verificación del respaldo.	2 días de la actividad
Revisión de bitácoras.	Revisión del histórico de eventos del sistema, por ejemplo el registro de accesos.	Encargado del sistema 1 día
Actualización del certificado de seguridad.	Solicitud de la renovación del certificado a la DGTIC de manera anual (septiembre-octubre).	Encargado del sistema 15 días
Actualización de la aplicación.	Actualización de los archivos y base de datos de la aplicación si hay nuevas versiones por parte del desarrollador.	Encargado del sistema. Tiempo variable

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

Licenciatura en Ciencias Genómicas		
Identificador único*	ccg-uati-002-E-IntranetLCG	
(Nombre del sistema A1)*	Intranet de la LCG	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos.	Se verificaron los archivos de respaldos.	Encargado del sistema en conjunto con la UATI.

Revisión de bitácoras.	Se detectaron registros de intentos de acceso. Todos los intentos han sido fallidos.	Encargado del sistema en conjunto con la UATI.
Actualización del certificado de seguridad.	El certificado SSL está vigente hasta octubre 2022.	Encargado del sistema en conjunto con la UATI.
Actualización de la aplicación.	La aplicación se encuentra desactualizada y ya no es posible actualizarla. Se debe considerar un nuevo desarrollo y una migración de información.	Encargado del sistema en conjunto con la UATI.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

Licenciatura en Ciencias Genómicas		
Identificador único*	ccg-uati-002-E-IntranetLCG	
(Nombre del sistema A1)*	Intranet de la LCG	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización de la aplicación.	Desarrollar una nueva aplicación con tecnologías más actuales y seguras.	Personal externo bajo supervisión de la Coordinación y personal de la LCG. 1 año

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

Licenciatura en Ciencias Genómicas			
Identificador único*	ccg-uati-002-E-IntranetLCG		
(Nombre del sistema A1)*	**Intranet de la LCG**		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos en línea .	Cursos en línea ofrecidos por la DGTIC y la Unidad de Transparencia, por ejemplo Medidas de Seguridad Técnicas para la Protección de Datos Personales.	Según calendario de oferta de cursos de la DGTIC.	Responsables de TI y encargado de los sistemas de las dependencias de la UNAM.

8.2. Programa de difusión de la protección a los datos personales

Licenciatura en Ciencias Genómicas			
Identificador único*	ccg-uati-002-E-IntranetLCG		
(Nombre del sistema A1)*	**Intranet de la LCG**		
Actividad*	**Descripción***	**Duración***	**Cobertura***

Mensajes por correo electrónico.	Mensajes a los usuarios del sistema con recomendaciones sobre cuidado de sus datos personales, en particular sus contraseñas y protección frente a mensajes de correo engañosos.	1 día de manera periódica a lo largo del año.	Toda la comunidad del CCG.
Carteles.	Se colocarán carteles en lugares públicos para hacer conciencia de proteger los datos personales.	Difusión semestral iniciando en septiembre de 2022.	Público en general.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

Licenciatura en Ciencias Genómicas			
Identificador único*	ccg-uati-002-E-IntranetLCG		
(Nombre del sistema A1)*	Intranet de la LCG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de información.	Crear, modificar o eliminar información de aspirantes, alumnos,	Duración variable Actividad regular	Permite contar con la información más actual.

	egresados, sobre los procedimientos y trámites escolares.		
Actualización de la aplicación.	Desarrollar una nueva aplicación con tecnologías más actuales y seguras.	1 año	Permite reforzar la seguridad usando tecnologías más actuales.

9.2. Actualización y mantenimiento de equipo de cómputo

Licenciatura en Ciencias Genómicas			
Identificador único*	ccg-uati-002-E-IntranetLCG		
(Nombre del sistema A1)*	Intranet de la LCG		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Migración del servidor.	Análisis y planeación de una migración de servidor a uno nuevo o a una máquina virtual, con sistema operativo y herramientas más actuales.	1 mes	Permite estar protegido frente a posibles fallas de hardware del equipo actual.

9.3. Procesos para la conservación, preservación y respaldos de información

Licenciatura en Ciencias Genómicas		
Identificador único*	ccg-uati-002-E-IntranetLCG	
(Nombre del sistema A1)*	Intranet de la LCG	
Proceso*	**Descripción***	**Responsable***
Realización de respaldos.	Se realiza un respaldo completo de los archivos y base de datos del sistema, de forma automática y semanalmente. Se transfiere el respaldo a un servidor local de respaldos. Se mantienen todos los archivos de respaldo semanales de los últimos 3 meses, y el último respaldo de cada mes de los últimos 3 años.	Encargado del sistema. 1 día para hacer el respaldo

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

Licenciatura en Ciencias Genómicas		
Identificador único*	ccg-uati-002-E-IntranetLCG	
(Nombre del sistema A1)*	Intranet de la LCG	
Proceso*	**Descripción***	**Responsable***

Formateo a bajo nivel de los discos.	De acuerdo al sistema operativo, seleccionar la aplicación adecuada para realizar el formateo del disco asegurando que cuenten con la opción de borrado seguro de la información.	Unidad de Administración de TI. 2 días
Destrucción del medio.	Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo.	Unidad de Administración de TI. 2 días

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

- El encargado del sistema debe contar con la solicitud y autorización del responsable del sistema, en este caso la Coordinación de la LCG.
- El encargado del sistema junto con la Unidad de Administración de TI, debe definir el periodo de bloqueo (en principio se puede manejar como 3 meses) y las actividades específicas a realizar para la cancelación
- Comunicar a los usuarios que al terminar el periodo de bloqueo se cancelará el sistema, especificar fecha

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

- Verificar que la documentación del estado reciente del servidor esté actualizada: versiones de sistema operativo, servidor web, bases de datos, lenguajes de programación y aplicación
- Respaldar las configuraciones de los servicios de web, bases de datos y el lenguaje de programación
- Respaldar los archivos y bases de datos del sistema, transferir a servidor de respaldos y verificar

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Al terminar el periodo de bloqueo,

- Comunicar a los usuarios la cancelación inminente del sistema
- Suspender el acceso al sistema, bloqueando las cuentas de usuarios o deshabilitando el servicio web
- Realizar último respaldo, transferir a servidor de respaldos y verificar
- En caso de contar ya con un nuevo sistema, consolidar el plan de migración de datos
- Deshabilitar servicios web y de base de datos
- Desconectar el servidor de la red
- Realizar la eliminación segura de los archivos y bases de datos del sistema
- Notificar al responsable del sistema, en este caso la Coordinación de la LCG

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

- Borrado de archivos con comandos del sistema operativo
- Borrado de tablas y bases de datos con comandos del sistema manejador de bases de datos
- Eliminación de los volúmenes lógicos o arreglos de discos
- Formateo a bajo nivel de los discos duros
- Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo
- Reinstalación del sistema operativo

CURSOS (ccg-uati-003-E-Cursos)

Conjunto de sistemas dedicados a la gestión de cursos y apoyo a los docentes y estudiantes, facilitando las tareas docentes relacionadas con las materias que son impartidas en la LCG, programas de doctorados o talleres.

1. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

UNIDAD DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN (UATI)	
Identificador único*	ccg-uati-003-E-Cursos
(Nombre del sistema A1) *	Plataformas de Cursos
Datos personales (sensibles o no) contenidos en el sistema*:	Datos de identificación, datos escolares de estudiantes y egresados de la Licenciatura en Ciencias Genómicas y del Centro de Ciencias Genómicas, y para asistentes a talleres del Nodo Nacional de Bioinformática.
Responsable*:	**Licenciatura en Ciencias Genómicas**
Nombre*:	Dr. Pablo Vinuesa Fleischmann
Cargo*:	Coordinador de la LCG
Funciones*:	Coordinación académica de las actividades de la LCG.
Obligaciones*:	Proporcionar y validar la información de los cursos de la LCG que se manejan en la plataforma.
Responsable*:	**Programa de Doctorado en Ciencias Biomédicas**
Nombre*:	Dra. Eria Rebollar

Cargo*:	Responsable del PDCBm en el CCG.
Funciones*:	Coordinación de las actividades académicas del PDCBm en el CCG.
Obligaciones*:	Validar la información de los cursos y alumnos del PDCBm que se manejan en la plataforma.
Responsable*:	**Nodo Nacional de Bioinformática CCG**
Nombre*:	Dra. Irma Martínez Flores
Cargo*:	Presidenta del NNB
Funciones*:	Coordinación de las actividades académicas del NNB, en particular de los Talleres Internacionales de Bioinformática.
Obligaciones*:	Proporcionar y validar la información de los talleres y participantes que se manejan en la plataforma.
	Encargados:
(Nombre del Encargado 1*)	**Alfredo Hernández**
Cargo*:	**Técnico Académico Titular A Tiempo Completo**
Funciones*:	Responsable de las plataformas de cursos.

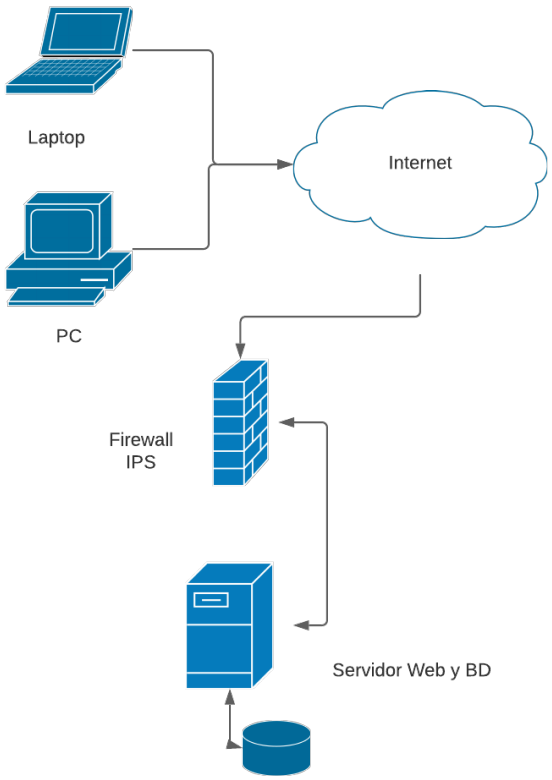
Obligaciones*:	Administración de la aplicación web, administración del servidor, establecer medidas técnicas de seguridad, actualización de la información.
(Nombre del Encargado 2*)	**Joel Gómez Espíndola**
Cargo*:	**Técnico por honorarios**
Funciones*:	Actualización de información de cursos y estudiantes de la LCG.
Obligaciones*:	Generación de cuentas para alumnos de nuevo ingreso, creación de cursos, asignación de estudiantes a cursos, actualización de la información.
(Nombre del Encargado 3*)	**Shirley Alquicira Hernández**
Cargo*:	**Técnico Académico Titular A Tiempo Completo**
Funciones*:	Actualización de información de cursos y estudiantes del NNB.
Obligaciones*:	Actualización de la información de los espacios para cursos de los Talleres Internacionales de Bioinformática del NNB.
	Usuarios:
(Nombre del Usuario 1*)	Alumnos y participantes
Cargo*:	Estudiantes
Funciones*:	

Obligaciones*:	Consultar información de los cursos, actualizar información su información relacionada a las actividades de los cursos (p.ej. subir tareas o ejercicios).
(Nombre del Usuario 2*)	Profesores y ayudantes
Cargo*:	Profesores
Funciones*:	Docencia
Obligaciones*:	Subir información del curso, consultar información, calificar.

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

UATI	
Identificador único¨*	ccg-uati-003-E-Cursos
(Nombre del sistema A1*)	Plataformas de Cursos
Tipo de soporte:*	Soporte electrónico
Descripción:*	Archivos de la aplicación web, imágenes, documentos, y base de datos relacional en servidores.

Características del lugar donde se resguardan los soportes:*	**Características** Del centro de cómputo: - aire acondicionado - soporte de respaldo de energía - acceso puerta aluminio/vidrio con llave - puerta de madera de área previa con llave en la LCG, puerta con acceso mediante lector de huella digital en el CCG De acceso al servidor: - Usuario y contraseña - Protección de red perimetral equipo dedicado FortiGate (firewall y sistema de prevención de intrusiones) en el caso de la LCG - Transmisión cifrada de datos por medio de certificados ssl **Componentes del sistema** - Servidores con sistema operativo Linux - Servidor web Apache - Servidor de base de datos MySQL - Aplicación web para cursos (sistema de gestión de aprendizaje) de código abierto **Diagrama de interconexión**



3. ANÁLISIS DE RIESGOS

Ver Anexo I: Análisis de riesgos.

4. ANÁLISIS DE BRECHA

Ver Anexo II: Análisis de brecha.

5. PLAN DE TRABAJO

Ver Anexo III: Plan de trabajo.

6. MEDIDAS DE SEGURIDAD IMPLEMENTADAS

I. TRANSFERENCIAS DE DATOS PERSONALES

UATI	
Identificador único*	ccg-uati-003-E-Cursos
(Nombre del sistema A1)*	Plataformas de Cursos

TRANSFERENCIAS DE DATOS PERSONALES	
Transferencias mediante el traslado de soportes físicos:	No se realizan transferencias mediante traslado de soportes físicos.
Transferencias mediante el traslado de soportes electrónicos:	No se realizan transferencias mediante traslado de soportes electrónicos.
Transferencias mediante el traslado sobre redes electrónicas:	Las transferencias se realizan mediante una conexión cifrada, esto es, mediante protocolo HTTP + SSL para acceso al sistema web a través de internet, y SSH para acceso a la consola del servidor y transferencia de los archivos de respaldo sólo en la red local. La conexión está protegida mediante un sistema de detección y protección de intrusiones en el firewall de red en el caso de la LCG. Los accesos se registran en las bitácoras del firewall de red, el servidor y el sistema.

II. RESGUARDO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES CON SOPORTES FÍSICOS

No se realiza tratamiento de datos personales en soportes físicos.

III. BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

1. **Los datos que se registran en las bitácoras:**
   Las bitácoras del servidor web registran los accesos e incluyen fecha, hora, dirección IP del visitante, y ruta accedida
   Las bitácoras del sistema registran la siguiente información: fecha, hora, dirección IP, usuario del sistema, tipo de evento, descripción del evento
2. **Si las bitácoras están en soporte físico o en soporte electrónico;**
   Las bitácoras se encuentran en soporte electrónico.
3. **Lugar dónde almacena las bitácoras y por cuánto tiempo;**
   Las bitácoras del servidor se almacenan en un archivo de texto en el servidor web.
   Las bitácoras del sistema se almacenan en la base de datos.
4. **La manera en que asegura la integridad de las bitácoras, y**
   Sólo el encargado del sistema y el administrador del servidor tienen acceso a las bitácoras.
   Las bitácoras están dentro del sistema y no se trasladan a ninguna otra parte.
5. **Respecto del análisis de las bitácoras:**
   El responsable de analizar las bitácoras es el área universitaria. El encargado del sistema y el administrador del servidor hacen una inspección manual periódicamente.

IV. REGISTRO DE INCIDENTES:

En la práctica cuando el usuario o el encargado del sistema identifican un incidente, lo reportan en un sistema de reporte de problemas y solicitudes (Request Tracker). Se describe el problema y qué servicio o sistema se ve afectado. Posteriormente el encargado o el personal técnico correspondiente, según el impacto, la urgencia y la prioridad del incidente, trabaja en la resolución del mismo. Cuando se resuelve, se describen las pruebas realizadas y la solución, se registra entre otras cosas la fecha, el sistema afectado, el nombre de la o las personas que intervinieron, el tiempo que llevó, y si se requirió ayuda de soporte técnico local o externo. Finalmente se notifica la solución al usuario.

V. ACCESO A LAS INSTALACIONES

1. **Seguridad perimetral exterior** (las instalaciones del área universitaria):

Para acceso a la dependencia hay una caseta de vigilancia con un vigilante las 24 horas. El vigilante solicita al visitante que se identifique mostrando una credencial oficial o documento de identidad, y que registre su entrada en una bitácora (fecha, hora de entrada, nombre, procedencia, nombre de la persona o área que visita, hora de salida). El vigilante avisa por teléfono a la persona que visita y ésta autoriza el acceso.

Adicionalmente, la dependencia cuenta con un sistema de cámaras de videovigilancia, al que solamente tiene acceso el personal de vigilancia, autorizados por el Departamento de Servicios Generales.

2. **Seguridad perimetral interior** (oficina, almacén o bodega para soportes físicos, centro de datos para soportes electrónicos):

El acceso al centro de cómputo del CCG donde se ubican los servidores es por una primera puerta protegida mediante un lector de huella digital. En el caso del centro de cómputo del CCG, se cuenta con una primera puerta con llave. Posteriormente para ambos casos se cuenta con una segunda puerta con llave por la que se accede al centro de cómputo. En ambos casos se cuenta con cámaras de videovigilancia. Solamente los encargados de la administración de los servidores tienen registrada su huella digital y acceso a ambas llaves. Los administradores son autorizados por la coordinación de la UATI.

VI. ACTUALIZACIÓN DE LA INFORMACIÓN CONTENIDA EN EL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

La actualización de la información contenida en el sistema requiere la solicitud, verificación y aprobación del responsable del sistema.
Las actualizaciones se realizan de forma regular de acuerdo a las necesidades, conforme se va requiriendo, por ejemplo:

- En periodo de ingreso de una nueva generación de alumnos, o inicio de un nuevo semestre de la LCG o del PDCBm
- En el momento de la realización de los talleres del NNB, una o dos veces al año

VII. PERFILES DE USUARIO Y CONTRASEÑAS

1. Modelo de control de acceso (alguno de los siguientes):

El control de acceso está basado en usuarios y roles, mediante una matriz de permisos.

2. Perfiles de usuario y contraseñas en el sistema operativo de red:

Se cuenta con sistema operativo Linux en los servidores del sistema, que cifra la contraseña del usuario y mantiene una política de contraseñas robustas.

3. Perfiles de usuario y contraseñas manejados por el software aplicativo del sistema de tratamiento de datos personales:

El sistema cifra la contraseña del usuario para almacenarla en la base de datos.

4. Administración de perfiles de usuario y contraseñas:

El encargado del sistema crea los nuevos perfiles. El responsable del sistema valida la información de los nuevos perfiles para su creación. El sistema mantiene un registro histórico de las operaciones realizadas.

5. Acceso remoto al sistema de tratamiento de datos personales:

Los usuarios finales no requieren acceso remoto al equipo de cómputo para trabajar con el sistema. Tienen acceso remoto directo al sistema vía web desde cualquier lugar en internet. El administrador requiere acceso remoto al servidor para hacer tareas propias de administración.

El acceso remoto no autorizado tanto al sistema como al servidor se evita mediante el uso de usuario y contraseña, y una matriz de roles y permisos. En el caso del acceso a los servidores, se tiene restringido el acceso a la red local por medio del firewall y se hace mediante una red privada virtual (VPN) y una conexión cifrada (SSH).

VIII. PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN DE DATOS

1. Señalar si realiza respaldos
   a) Completos_**x**_, diferenciales ___ o incrementales___;
   b) De forma automática _**x**__ o Manual _**x**____,
   c) Periodicidad con que los realiza: __semanal_____
2. El tipo de medios (por ejemplo: cintas magnéticas, discos duros, CD-ROM, entre otros) que utiliza para almacenar las copias de seguridad;
   Disco duro.
3. Cómo y dónde archiva esos medios, y
   Se generan archivos comprimidos de un vaciado de la base de datos y un empaquetado de los archivos de la aplicación, usando un script que se ejecuta manualmente o en una tarea programada en los servidores. Posteriormente, se almacenan en un servidor de respaldos, donde se depuran cada cierto tiempo.
4. Quién es el responsable de realizar estas operaciones (el área universitaria o un tercero). El área universitaria.

IX. PLAN DE CONTINGENCIA

Como parte inicial de un plan de contingencia en desarrollo, en la práctica para los servidores se cuenta con contrato de garantía y soporte técnico en fallas de hardware, además en el centro de cómputo se cuenta con planta y equipo de respaldo de energía. Para los sistemas se cuenta con los respaldos que pueden restaurarse en caso de una contingencia.

Por el momento no se cuenta con sitios redundantes o alternos.

7. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

7.1. Herramientas y recursos para monitoreo de la protección de datos personales

UATI	
Identificador único*	ccg-uati-003-E-Cursos

(Nombre del sistema A1)*	Plataformas de Cursos	
Recurso*	**Descripción***	**Control***
Bitácora o registro de histórico de sucesos.	Registro en la base de datos de la aplicación de todas las operaciones realizadas por los usuarios.	Revisión periódica de forma manual, después de cierto tiempo el encargado podría detectar sucesos anómalos.
Herramientas para análisis de seguridad del servidor.	Herramientas para análisis de vulnerabilidades, escaneo de puertos y pruebas de penetración.	Pruebas periódicas realizadas por el CERT UNAM y aviso al responsable de TI de la dependencia en caso de encontrar alguna vulnerabilidad, para implementar los mecanismos de seguridad complementarios.

7.2. Procedimiento para la revisión de las medidas de seguridad

UATI		
Identificador único*	ccg-uati-003-E-Cursos	
(Nombre del sistema A1)*	Plataformas de Cursos	
Medida de seguridad*	**Procedimiento***	**Responsable***
Generación de respaldos.	Realización del respaldo de los archivos de la aplicación y de la base de datos de forma manual o automática, y de manera semanal.	Encargado del sistema. 2 días de la actividad

	Verificación del respaldo.	
Revisión de bitácoras.	Revisión del histórico de eventos del sistema, por ejemplo el registro de accesos.	Encargado del sistema. 1 día
Actualización del certificado de seguridad.	Solicitud de la renovación del certificado a la DGTIC de manera anual (septiembre-octubre).	Encargado del sistema. 15 días
Actualización de la aplicación.	Actualización de los archivos y base de datos de la aplicación si hay nuevas versiones por parte del desarrollador.	Encargado del sistema. Tiempo variable

7.3. Resultados de la evaluación y pruebas a las medidas de seguridad

UATI		
Identificador único*	ccg-uati-003-E-Cursos	
(Nombre del sistema A1)*	Plataformas de Cursos	
Medida de seguridad*	**Resultado de evaluación***	**Responsable***
Generación de respaldos.	Se verificaron los archivos de respaldos.	Encargado del sistema en conjunto con la UATI.
Revisión de bitácoras.	Se detectaron registros de intentos de acceso. Todos los intentos han sido fallidos.	Encargado del sistema en conjunto con la UATI.

Actualización del certificado de seguridad.	El certificado SSL está vigente hasta octubre de 2022.	Encargado del sistema en conjunto con la UATI.
Actualización de la aplicación.	Las aplicaciones se encuentran desactualizadas. En el caso de la LCG se debe preparar un plan de actualización. En el caso de las plataformas de cursos del CCG y NNB ya no es posible actualizarlas, se debe considerar una nueva instalación.	Encargado del sistema en conjunto con la UATI.

7.4. Acciones para la corrección y actualización de las medidas de seguridad

UATI		
Identificador único*	ccg-uati-003-E-Cursos	
(Nombre del sistema A1)*	Plataformas de Cursos	
Medida de seguridad*	**Acciones***	**Responsable***
Actualización de la aplicación en LCG.	Preparar un plan de actualización: realizar respaldo, verificar requerimientos de software, verificar cambios y posibles afectaciones, avisar a los usuarios, realizar actualización, realizar pruebas, y liberar.	Encargado del sistema en conjunto con la UATI. 1 semana en periodo vacacional.
Actualización de la aplicación en CCG y NNB.	Realizar una instalación aparte de la versión más reciente de la aplicación. Se comenzará de nuevo con la información más actual, es decir no se migrará la información de las aplicaciones	Encargado del sistema en conjunto con la UATI. 1 semana en periodo vacacional.

	anteriores. El sistema anterior quedará como histórico o se cancelará.	

8. PROGRAMA ESPECÍFICO DE CAPACITACIÓN

8.1. Programa de capacitación a los responsables de tratamiento de datos personales

UATI			
Identificador único*	ccg-uati-003-E-Cursos		
(Nombre del sistema A1)*	Plataformas de Cursos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Cursos en línea.	Cursos en línea ofrecidos por la DGTIC y la Unidad de Transparencia, por ejemplo Medidas de Seguridad Técnicas para la Protección de Datos Personales.	Según calendario de oferta de cursos de la DGTIC.	Responsables de TI y encargado de los sistemas de las dependencias de la UNAM.

8.2. Programa de difusión de la protección a los datos personales

UATI	
Identificador único*	ccg-uati-003-E-Cursos
(Nombre del sistema A1)*	Plataformas de Cursos

Actividad*	Descripción*	Duración*	Cobertura*
Mensajes por correo electrónico.	Mensajes a los usuarios del sistema con recomendaciones sobre cuidado de sus datos personales, en particular sus contraseñas y protección frente a mensajes de correo engañosos.	1 día de manera periódica a lo largo del año.	Toda la comunidad del CCG.

9. MEJORA CONTINUA

9.1. Actualización y mantenimiento de sistemas de información

UATI			
Identificador único*	ccg-uati-003-E-Cursos		
(Nombre del sistema A1)*	Plataformas de Cursos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Actualización de información.	Crear, modificar o eliminar información de alumnos, profesores, cursos y categorías. En el caso del NNB se habla de participantes,	Duración variable Actividad regular	Permite contar con la información más actual.

	instructores, talleres y eventos.		
Actualización de la aplicación.	Realizar el plan de actualización de las aplicaciones	1 semana	Permite reforzar la seguridad usando versiones más actuales, con menos vulnerabilidades.

9.2. Actualización y mantenimiento de equipo de cómputo

UATI			
Identificador único*	ccg-uati-003-E-Cursos		
(Nombre del sistema A1)*	Plataformas de Cursos		
Actividad*	**Descripción***	**Duración***	**Cobertura***
Migración de servidores.	Análisis y planeación de una migración de servidor a uno nuevo o a una máquina virtual, con sistema operativo y herramientas más actuales.	1 mes	Permite estar protegido frente a posibles fallas de hardware de los equipos actuales.

9.3. Procesos para la conservación, preservación y respaldos de información

UATI	
Identificador único*	ccg-uati-003-E-Cursos

(Nombre del sistema A1)*	Plataformas de Cursos	
Proceso*	**Descripción***	**Responsable***
Realización de respaldos.	Se realizan respaldos completos de los archivos y base de datos del sistema, de forma manual o automática y semanalmente. Se transfiere el respaldo a un servidor local de respaldos. Se mantienen todos los archivos de respaldo semanales de los últimos 3 meses, y el último respaldo de cada mes de los últimos 3 años.	Encargado del sistema 1 día para hacer el respaldo

9.4. Procesos de borrado seguro y disposición final de equipos y componentes informáticos

UATI		
Identificador único*	ccg-uati-003-E-Cursos	
(Nombre del sistema A1)*	Plataformas de Cursos	
Proceso*	**Descripción***	**Responsable***
Formateo a bajo nivel de los discos.	De acuerdo al sistema operativo, seleccionar la aplicación adecuada para realizar el formateo del disco asegurando que cuenten con la opción de borrado seguro de la información.	Unidad de Administración de TI. 2 días

Destrucción del medio.	Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo.	Unidad de Administración de TI. 2 días

10. PROCEDIMIENTO PARA LA CANCELACIÓN DE UN SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

A) DATOS DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES QUE SERÁ CANCELADO:

a) Denominación
b) Motivo de la cancelación

B) PLAZOS Y CONDICIONES PARA EL BLOQUEO DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

- El encargado del sistema debe contar con la solicitud y autorización del responsable del sistema
- El encargado del sistema junto con la Unidad de Administración de TI, debe definir el periodo de bloqueo (en principio se puede manejar como 3 meses) y las actividades específicas a realizar para la cancelación
- Comunicar a los usuarios que al terminar el periodo de bloqueo se cancelará el sistema, especificar fecha

C) MEDIDAS DE SEGURIDAD PARA EL BLOQUEO Y POSTERIOR SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES:

- Verificar que la documentación del estado reciente del servidor esté actualizada: versiones de sistema operativo, servidor web, bases de datos, lenguajes de programación y aplicación
- Respaldar las configuraciones de los servicios de web, bases de datos y el lenguaje de programación
- Respaldar los archivos y bases de datos del sistema, transferir a servidor de respaldos y verificar

D) PROCEDIMIENTO PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

Al terminar el periodo de bloqueo,

- Comunicar a los usuarios la cancelación inminente del sistema
- Suspender el acceso al sistema, bloqueando las cuentas de usuarios o deshabilitando el servicio web
- Realizar último respaldo, transferir a servidor de respaldos y verificar
- En caso de contar ya con un nuevo sistema, consolidar el plan de migración de datos
- Deshabilitar servicios web y de base de datos
- Desconectar el servidor de la red
- Realizar la eliminación segura de los archivos y bases de datos del sistema

- Notificar al responsable del sistema

E) MECANISMOS PARA LA SUPRESIÓN DEL SISTEMA DE TRATAMIENTO DE DATOS PERSONALES

- Borrado de archivos con comandos del sistema operativo
- Borrado de tablas y bases de datos con comandos del sistema manejador de bases de datos
- Eliminación de los volúmenes lógicos o arreglos de discos
- Formateo a bajo nivel de los discos duros
- Si ya no es posible realizar el formateo, retirar temporalmente el disco duro del equipo y realizar la incapacitación física del mismo
- Reinstalación del sistema operativo