FORMATOS PARA CUMPLIMIENTO DE LAS MST

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato	**1**	**Verificación anual**	**Acción concluida**	(X)
Medida de seguridad técnica:		**Artículo 18. I. c) Utilizar datos no personales durante el desarrollo y pruebas de los sistemas.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Evitar usar datos personales mientras se está desarrollando, actualizando o modificando el código fuente de un sistema de información.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información, por medio de formato o comandos. **C)** Verificar que los datos usados en el desarrollo no correspondan a personas identificables. **D)** Si se usan datos de personas identificables, cambiar por datos genéricos o datos ficticios y regresar al punto B. **E)** Si no se usan datos de personas identificables, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Se recomienda al desarrollar un sistema de información no usar datos personales sino ficticios. **2.-** Se sugiere incluir en la documentación del desarrollo de un sistema de información el inventario de datos y el tipo de información de prueba.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de tablas.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			DICIEMBRE 01-2021	
Nombre y firma Programador, desarrollador o diseñador del sistema de información			**Fecha término**	
			DICIEMBRE 01-2021	
Observaciones / anotaciones		En las pruebas de funcionamiento no se utilizaron datos reales. En el proceso de desarrollo y pruebas, no se utilizan datos personales. Se hace uso de cadenas de caracteres que correspondan al tipo, longitud y formato correspondiente a los campos y con ello se realizan los procesos de prueba correspondientes		

I.

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**2**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 18. I. e) Asignar o revocar los privilegios de acceso para los usuarios teniendo como base el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		No se deben asignar privilegios de acceso a los usuarios en niveles que no estén relacionados con su responsabilidad en el tratamiento de datos.		
Proceso recomendado:		**A)** Realizar respaldo completo de la base de datos. **B)** Ejecutar consulta en el sistema de información de la lista de usuarios y sus niveles o privilegios de acceso. **C)** Validar que los niveles de acceso son acordes a la relación del usuario con el tratamiento de datos personales. **D)** Si hay usuarios con privilegios mayores a los que les son necesarios, cambiar al mínimo indispensable e informarlo al usuario. Regresar al punto B. **E)** Si los privilegios de acceso son correctos para los usuarios, llenar formato con nombre y firma de quien realizó la acción, fecha de inicio y de conclusión.		
Mejores prácticas, referencias:		**1.-** Definir niveles de acceso adecuados para cada perfil o tipo de usuario. **2.-** Tener un mínimo de administradores o usuarios con altos privilegios en el sistema.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			DICIEMBRE 02, 2021	
Nombre y firma Administrador del sistema de información			**Fecha término** DICIEMBRE 02, 2021	
Observaciones / anotaciones		Se otorgan privilegios a la base de datos, solo al desarrollador, en el caso de los usuarios finales, se asignan dependiendo de la actividad a desarrollar. El sistema tiene distintos niveles de acceso asociados a perfiles por área: difusión, presupuesto, secretaría técnica, cómputo y solo los perfiles que requieren el acceso a los datos personales se les otorga		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**3**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 18. I. g) Instalar y mantener vigentes certificados de comunicación segura SSL en el caso de servicios basados en Web.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		El instalar un certificado SSL en servidores web incrementa la seguridad al encriptar la transferencia de datos y la unicidad del sitio para los usuarios.		
Proceso recomendado:		**A)** En caso de no tener un certificado SSL vigente, enviar correo electrónico al Departamento de Firma Electrónica de DGTIC a firma.tic@unam.mx solicitando la asignación. **B)** El Departamento de Firma Electrónica Avanzada envía procedimiento para obtención de CSR del servidor, formato de la solicitud y costos de recuperación en función del tipo de certificado requerido (organizacional, comodín o corporativo). **C)** Completar documentación, proceso y pago de costo de recuperación. Enviar comprobantes a firma.tic@unam.mx. **D)** Al recibir el certificado SSL, instalarlo en el servidor de acuerdo con las instrucciones recibidas junto con el certificado.		
Mejores prácticas, referencias:		**1.-** Los certificados SSL deben tener una vigencia de al menos un año. **2.-** En caso de tener varios sistemas de información bajo un mismo dominio, se recomienda obtener un certificado SSL del tipo comodín (*wildcard*). **3.-** Se debe realizar el proceso de renovación del certificado al menos 10 días hábiles antes de su vencimiento.		
Conocimientos requeridos:		Administración de sistema operativo. Administración de servicios Web.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			27/10/2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			29/10/2021	
Observaciones / anotaciones		El Instituto dispone de certificado SSL del tipo comodín (*wildcard*), este sistema en línea, dispone de conexión segura. El certificado ya forma parte de los insumos que se tienen que cubrir anualmente.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)		IIBI-S2019		
Formato:	**4**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 18. I. h) Definir el plan de respaldos de la información, incluyendo periodicidad y alcance.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		En todo sistema de información es indispensable contar con un plan de respaldos periódicos, y especialmente en aquellos que contienen datos personales.		
Proceso recomendado:		**A)** Elaborar documento con la secuencia de respaldos al menos con el siguiente orden: - Diario – incremental. - Semanal – incremental. - Mensual – total. **B)** Establecer en el plan los medios para resguardo del respaldo y su forma de identificación: - En línea: mismo equipo donde se ejecuta el sistema. - Respaldo como servicio: otro equipo de almacenamiento. - Fuera de línea: medios magnéticos (cintas, discos) y/u ópticos. **C)** Incluir en el plan: - Responsables de cada tipo y medio de respaldo. - Rotación de respaldos y medios. - Áreas de resguardo. - Métodos de cifrado. - RTO: *Recovery Time Objective*. Tiempo objetivo de recuperación. - RPO: *Recovery Point Objective*: Punto objetivo de recuperación. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben tener al menos 3 respaldos del sistema y sus bases de datos en distintos medios.		
Conocimientos requeridos:		Administración de sistema operativo. Gestión y programación de respaldos.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Diciembre 08, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Diciembre 08, 2021	
Observaciones / anotaciones		Se realizan respaldos semanales, en línea en un equipo distinto al que aloja el sistema, mensualmente se realiza un respaldo en medio magnético externo al servidor (fuera de línea). También se realizan respaldos históricos cuando hay una actualización en la funcionalidad del sistema, no hay periodicidad ya que se realiza según la necesidad. Sin incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**5**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 18. I. i) Definir el procedimiento para el borrado seguro.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Al igual que el procedimiento de respaldo, el borrado seguro de la información debe estar definido en cualquier sistema de información.		
Proceso recomendado:		**A)** Elaborar documento con el procedimiento y la herramienta para borrado seguro en función del tipo de base de datos para registros, tablas y base de datos. **B)** Incluir en el documento de borrado seguro el proceso de verificación de la no existencia del dato, generalmente por medio de consultas y de copias de respaldo. **C)** El borrado seguro debe incluirse en los respaldos incrementales y totales y en cualquiera de los medios de respaldo, así como máquinas virtuales o contenedores. **D)** Concluir este documento, adjuntarlo a SGPDP, llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Para el caso de baja de equipo, se debe llenar el formato con la declaración de borrado seguro del Patronato Universitario, disponible en: http://www.patrimonio.unam.mx/patrimonio/descargas/formato_responsiva_borrado_datos.pdf **2.-** Se recomienda utilizar herramientas de borrado seguro por medio de sobre escritura aleatoria, llenado de ceros (0x00), llenado de unos o protocolos de borrado del estándar *DOD-5220.22-M*.		
Conocimientos requeridos:		Administración de sistema operativo. Comandos de borrado.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Diciembre 09,2021	
Nombre y firma Administrador del sistema de información o servidor			**Fecha término** Diciembre 09,2021	
Observaciones / anotaciones		El sistema no ha estado en la situación de cambio de infraestructura, pero en el caso, se realizan procedimientos de escritura aleatoria. Sin incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**7**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 18. II. b) Instalar y mantener actualizado el software antimalware.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener protecciones instaladas para mitigar la inserción de *malware* (*rootkits, backdoors o* códigos maliciosos) que pueda alterar su operación o la integridad y seguridad de los datos.		
Proceso recomendado:		**A)** En función del sistema operativo, instalar uno o varios programas para la contención de malware. *Por ejemplo*, para el caso del sistema operativo Linux existen herramientas de código abierto y uso libre como *chkrootkit, rootkit hunter, bothunter, clamAV, avast*, entre otros, que se pueden instalar desde el repositorio correspondiente a la distribución de Linux en uso. **B)** Disponer de comandos para la localización de amenazas. *Por ejemplo*, para el caso de Linux, se recomienda usar el comando *grep* para la detección de cadenas regulares de texto en las invocaciones al *shell*. **C)** Una vez instalada la solución, verificar periódicamente su actualización **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** UNAM-CERT puede asesorar en la selección de las herramientas *anti malware* más adecuadas para el servidor donde se aloje el sistema de información. Contactar al correo seguridad.tic@unam.mx.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Diciembre 09, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Diciembre 10, 2021	
Observaciones / anotaciones		Se realizan revisiones de logs de aplicaciones, de acceso y de instalación de aplicaciones. Se utiliza el antivirus que dispone el firewall. Hasta el momento no se han tenido incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**8**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 18. II. c) Instalar las actualizaciones de seguridad más recientes disponibles.**		
Aplicable en:		II. Sistemas operativos y servicios.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		El servidor que hospede el sistema de información debe tener vigentes todas las actualizaciones de seguridad proporcionadas por el fabricante o desarrollador del sistema operativo.		
Proceso recomendado:		**A)** En función del sistema operativo, se debe revisar la vigencia y actualización de las herramientas de seguridad de la información. *Por ejemplo*, en el sistema operativo Linux ejecutar *apt-get update* para obtener la lista de actualizaciones, especialmente en el repositorio *security* de la respectiva distribución. **B)** Realizar un respaldo del sistema para garantizar retorno a versión anterior en caso de incompatibilidad con alguna aplicación de las actualizaciones de seguridad. **C)** Instalar las actualizaciones en el sistema operativo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe verificarse la actualización de seguridad del sistema operativo al menos una vez a la semana y configurar la actualización o notificación inmediata en caso de complementos de seguridad urgentes.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 17, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Noviembre 20, 2021	
Observaciones / anotaciones		Se realiza actualización de parches y aplicaciones, también actualización de la versión del sistema operativo cuando hay versión posterior estable, esta acción se realiza conforme surgen actualizaciones y también se toma en cuenta los avisos que proporciona el sistema operativo al respecto. Sin incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS - GINEA)			IIBI-S2019	
Formato:	**9**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 19. I. a) Aplicar un mecanismo de autenticación para las personas autorizadas con base en el principio del menor privilegio.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Partiendo de la asignación o niveles de acceso a la información con el principio del menor privilegio, debe haber en operación en el sistema al menos un mecanismo para la validación de los usuarios autorizados.		
Proceso recomendado:		**A)** Verificar el tipo de control de acceso al sistema, esto es: a través de contraseñas, claves, identificadores, nombres de usuario, nombres de dominio, entre otros. Según sea aplicable al sistema de información en lo particular. En caso de no tener un control de acceso establecer al menos uno como: usuarios de sistema operativo, cuenta y contraseña de sistema. **B)** Revisar que los privilegios de acceso sean los adecuados en función del rol del usuario. *Por ejemplo:* el usuario de conexión a la base de datos no debe estar asignado a alguna cuenta del personal que tiene acceso al sistema. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un esquema estándar de acceso a sistemas que están vinculados, por ejemplo: por medio de Directorio Activo (*Active Directory*), *LDAP* u *OpenAIM.* **2.-** Las contraseñas deben ser de 12 caracteres o más con uso de signos, letras mayúsculas y minúsculas y números.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 22, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Noviembre 25, 2021	
Observaciones / anotaciones		Se tienen accesos controlados, a la base de datos, al sistema operativo y al sistema en sí. También se limita el nivel perfil de claves. Se tiene un protocolo de cancelación de claves ante cambio de adscripción, jubilación, baja laboral. Se revisó que los privilegios de acceso sean los adecuados en función del rol del usuario. Se solicitó la actualización de contraseñas indicando el formato requerido. Sin incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS - GINEA)			IIBI-S2019	
Formato:	**10**	**Verificación anual**	**Acción concluida**	(x)
Medida de seguridad técnica:		**Artículo 19. II. b) Evitar la instalación de cualquier elemento de software que implique algún riesgo para el tratamiento de datos personales.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Por la relevancia de los sistemas de información con datos personales se debe minimizar o erradicar el riesgo de seguridad que implica instalar aplicaciones no verificadas.		
Proceso recomendado:		**A)** Dependiendo del sistema operativo, configurar las actualizaciones solamente para versiones maduras o revisiones certificadas de las aplicaciones. *Por ejemplo*: en sistemas Linux desactivar la instalación de versiones *beta, test, debug, non-official.* **B)** De la lista de software instalado, verificar el consumo de recursos de aplicaciones *TSR (Terminal and Stay Resident)*. Identificar demonios que ocupen excesiva RAM o tiempo de ejecución en el procesador. *Por ejemplo*: En sistemas Windows usar el Administrador de Tareas para identificar programas de alto consumo. **C)** Desinstalar toda aquella aplicación, librería, programa, paquetería o servicio que no sea estrictamente necesario para la operación del sistema. *Por ejemplo*, si el servidor Linux no proporcionará direcciones IP, el demonio o servicio *dchpd* no debe estar instalado. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** En ningún caso puede instalarse software de procedencia desconocida. Se debe impedir a los usuarios en sus privilegios de acceso instalar software o inyectar código a la aplicación del sistema de información. y se debe realizar un control estricto de los puertos de comunicación (USB, Red, etc) para evitar la extracción no autorizada de datos.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA				
Nombre y firma Administrador del sistema de información o servidor			**Fecha término**	
Observaciones / anotaciones		En el caso del servidor donde se aloja la aplicación solo se instala el software necesario para el funcionamiento de las aplicaciones, se evita en lo posible el uso de ambiente gráfico Se instalan versiones estables y los parches adecuados si es el caso. El acceso físico a los servidores está totalmente restringido a personal ajeno al área de cómputo. Antes de hacer alguna instalación o actualización por el personal de cómputo se analiza y verifica el impacto		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS - GINEA)			IIBI-S2019	
Formato:	**11**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 19. III. a) Establecer las medidas físicas de seguridad que controlen el acceso a los equipos.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Dos días hábiles.		
Importancia de la acción:		Además de las protecciones de tipo lógico, deben implementarse medidas de seguridad para reducir el riesgo al sistema de información por accesos físicos no autorizados.		
Proceso recomendado:		**A)** Identificar las medidas físicas que restrinjan el acceso físico a equipos, tales como chapas, puertas, biométricos. **B)** En función de la ubicación del equipo de cómputo, hacer una relación de las condiciones más adecuadas para su protección que aún sean necesarias implementar. **C)** Establecer y seguir un plan de mejoramiento de la protección física de equipos. *Por ejemplo*; cámaras de videovigilancia, bitácoras, vigilantes, cuartos cerrados, racks con puerta y chapa, candados en equipos, bloqueo o desconexión física de puertos USB, alarmas y sensores, según sea lo más conveniente como mínimo para la protección de los datos. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas físicas de seguridad deben revisarse regularmente y formar parte de plan de continuidad de operaciones, así como ser del conocimiento de la Comisión local de seguridad.		
Conocimientos requeridos:		Administración de bases de datos. Consulta y actualización de usuarios.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 29, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Noviembre 29, 2021	
Observaciones / anotaciones		Se dispone de un área exclusiva para servidores y equipo de comunicaciones, el acceso es con llave y previo hay una puerta con chapa de seguridad. Se tiene sistema de cámaras para la vigilancia tanto del acceso como de seguridad en el área. Se cuenta con las medidas de seguridad adecuadas.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**12**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. b) Restringir la salida de equipos de las instalaciones de cada área universitaria.**		
Aplicable en:		III. Equipo de cómputo.		
Tiempo estimado:		Un día hábil.		
Importancia de la acción:		Se debe tener un mecanismo de control para la entrada y salida de equipos de cómputo y eliminar extracciones no autorizadas.		
Proceso recomendado:		**A)** Diseñar una bitácora o formato para el registro de entrada y salida de equipos de cómputo y periféricos asociados como discos duros, cintas, unidades *flash*, discos ópticos, monitores, teclados, ratones y en lo general todo componente de un equipo. **B)** La bitácora de entrada y salida debe incluir el registro de número de serie e inventario UNAM. responsable de ingreso o egreso del componente y firma autorizada del responsable del área. **C)** Incluir en el procedimiento la revisión periódica (al menos una vez al mes) de la consistencia del inventario registrado contra la bitácora de entrada y salida. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar un formato estándar de control de entrada y salida de bienes proporcionado por las áreas administrativas de las entidades y dependencias y conservar una copia en el área responsable del equipo de cómputo. **2.-** En la bitácora se debe incluir la razón de la entrada o salida del equipo. En el caso de baja, se deberá firmar la declaración de borrado seguro de Patrimonio Universitario.		
Conocimientos requeridos:		Gestión de Tecnología de información, control de entrada y salida de equipo y materiales.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Diciembre 01, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Diciembre 01, 2021	
Observaciones / anotaciones		Se mantiene el sistema de control de entrada y salida del equipo de cómputo con la Secretaría Administrativa. Sin incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**13**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 19. IV. a) Realizar la transmisión de datos personales a través de un canal cifrado.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		La comunicación del sistema de información con otros sistemas o servicios, así como el acceso de administración para ejecución de procesos por comandos, debe estar encriptada para evitar el envío o recepción de datos susceptibles de ser interceptados en tránsito.		
Proceso recomendado:		**A)** Identificar, mediante el administrador de aplicaciones que corresponda al sistema operativo, los protocolos y aplicaciones instalados para comunicación cifrada. *Por ejemplo*: *SFTP (Secure File Transfer Protocol), SSH (Secure Shell), SCP (Secure Copy*). **B)** Instalar con el administrador de aplicaciones o comando similar los protocolos de comunicación cifrada que sean necesarios para el tipo de transacciones y accesos del sistema. *Por ejemplo*, en el caso de requerir ejecutar comandos de forma remota en un servidor Linux, instalarlo con el comando *apt-get install openssh-server.* **C)** Activar los protocolos de comunicación encriptada en el servidor. *Por ejemplo*: en Linux con el comando *sudo systemctl enable ssh*. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben mantener actualizados los protocolos de comunicación por canal cifrado al igual que las utilerías de seguridad. 2.- El protocolo de comunicación cifrada requiere puertos específicos TCP, los cuales deberán estar permitidos en la configuración del equipo activo de red.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Administración de red.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 29, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Noviembre 29, 2021	
Observaciones / anotaciones		Toda la comunicación para el servidor que aloja la aplicación se realiza por canales seguros. Se utiliza *SSH y SCP* El acceso vía web es por medio de https Sin incidents.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**14**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 20. Aplicar el procedimiento de borrado seguro que impida la recuperación en las bases de datos y todos sus respaldos.**		
Aplicable en:		Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Tres días hábiles.		
Importancia de la acción:		Se debe verificar que el procedimiento de borrado seguro es funcional y que el dato no persiste en función del tipo de borrado (registro, tabla, base, sistema).		
Proceso recomendado:		**A)** Realizar una copia integral del sistema de información y colocarla en un servicio temporal. *Por ejemplo:* máquina virtual directorio temporal en el servidor. **B)** Ingresar a la copia del sistema de información y realizar el borrado de un registro. Verificar que el dato no persiste en la base de datos por medio de forma de consulta o comando. **C)** Realizar el mismo proceso del punto B para una tabla y finalmente para la base de datos completa. D) En caso de persistencia del dato, instalar y ejecutar herramientas para borrado seguro. *Por ejemplo*: en Linux se dispone *de shred, wipe, secure-delete, srm, sfill, sswap, sdmem,* que se pueden instalar desde el administrador de aplicaciones. **D)** Llenar y firmar este formato.		
Mejores prácticas, referencias:		**1.-** Se recomienda usar al menos un comando a nivel de sistema operativo para el borrado seguro de conformidad con el procedimiento establecido.		
Conocimientos requeridos:		Administración de sistema operativo. Instalación de aplicaciones. Gestión de archivos.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 29, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Diciembre 01, 2021	
Observaciones / anotaciones		El borrado de información de la base de datos se realiza a nivel físico. se aplican comandos de escritura aleatoria		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**16**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. d) Permitir el acceso al código fuente de los sistemas exclusivamente a la administración del sistema y personal para el desarrollo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Evitar el uso de códigos originales de los sistemas de información que posteriormente implique un riesgo a la seguridad de estos.		
Proceso recomendado:		**A)** Recopilar el código fuente y documentación del sistema de información en todas sus versiones disponibles. **B)** Depositar en un equipo central de desarrollo todas las versiones de código fuente y su documentación (inventario de datos, manual de administración, manual de programador). **C)** Establecer control de acceso por usuario y contraseña hacia el equipo central de desarrollo **D)** Activar bitácoras de acceso (*log*) hacia el equipo central de desarrollo. **E)** Proporcionar las credenciales de acceso al equipo central de desarrollo exclusivamente al personal a cargo de programación y mantenimiento de código y manuales. **F)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se debe documentar todo el proceso de desarrollo y actualización de un sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Gestión de bases de datos.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 29, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Diciembre 03, 2021	
Observaciones / anotaciones		El acceso al código fuente está disponible sólo para los desarrolladores y el responsable del área. Se centralizan y resguardan las versiones estables y vigentes		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**17**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnicas:		**Artículo 19. I. b) Establecer las medidas de seguridad en los periodos de inactividad o mantenimiento.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Garantizar la continuidad de la operación y disponibilidad de los sistemas de información especialmente durante períodos vacacionales, contingencias o ciclos de mantenimiento.		
Proceso recomendado:		**A)** Elaborar documento con las medidas necesarias de seguridad para períodos vacacionales, contingencias y ventanas de mantenimiento, incluyendo: control de acceso físico y lógico a los equipos, ejecución de respaldos, sistemas de alta disponibilidad (redundancia). **B)** Incluir en el documento la descripción de los procedimientos en caso de contingencia por falla de servicio de red, falla de equipo de cómputo, falla lógica en sistema operativo. **C)** Incluir en el documento el directorio de responsables de cada uno de los puntos a atender: apagado seguro, apagado fortuito, apagado programado, verificación de integridad de información, activación de servicios locales o de respaldo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las medidas de seguridad durante períodos de mantenimiento deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 29, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Diciembre 03, 2021	
Observaciones / anotaciones		Para los periodos de inactividad se realiza revisión previa de los elementos de soporte eléctrico, revisiones aleatorias de la aplicación en periodo de inactividad. Se tienen mecanismos automatizados de respaldo que permiten el restablecimiento de la aplicación en horas, dependiendo del entorno de sistema operativo y aplicaciones. Se organizan guardias, por parte del personal de cómputo para atender alguna situación emergente tanto a la distancia como en sitio.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**18**	**Verificación anual**	**Acción concluida**	(x)
Medidas de seguridad técnica:		**Artículo 19. I. c) Generar respaldos y aplicar los mecanismos de control y protección para su resguardo.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Ocho días hábiles.		
Importancia de la acción:		Verificar que el plan de respaldos opera adecuadamente para su utilización en caso de contingencia.		
Proceso recomendado:		**A)** De acuerdo con el plan de respaldos establecido, ejecutar la secuencia de respaldos. **B)** Designar responsables de respaldos y responsables de verificación de respaldos. **C)** Completar bitácora de control de los respaldos, indicando fecha, hora, tipo de respaldo (integral, total, parcial de registros), ejecutor y revisor del respaldo, ubicación del respaldo, medio y etiqueta. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** La generación de respaldos, su control y protección deben formar parte de un plan de continuidad de operaciones y de recuperación ante desastres (**DRP**).		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 8, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Noviembre 16, 2021	
Observaciones / anotaciones		Se dispone de un protocolo para el resguardo del sistema y de la información, además de las configuraciones necesarias del entorno operativo. También se tiene un proceso automatizado de respaldo y a su vez se realizan procedimientos posteriores para verificar tanto la integridad y consistencia del respaldo.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**20**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. II. a) Proteger ante manipulaciones indebidas y accesos no autorizados las bitácoras y los dispositivos donde se almacenan.**		
Aplicable en:		II. Sistemas operativos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Las bitácoras son un elemento esencial para determinar acciones que atentan contra la estabilidad del sistema de información y la protección de los datos personales.		
Proceso recomendado:		**A)** Elaborar una lista de las bitácoras relacionadas con el sistema de información, tanto en medio digital como físico. *Por ejemplo*: En el equipo de cómputo las bitácoras de acceso de usuarios al sistema operativo y al sistema de información (*logs*), de forma física las bitácoras de acceso al área donde está el equipo de cómputo. **B)** Junto a la lista elaborar el cronograma de revisión de integridad y respaldo de las bitácoras. *Por ejemplo*: diario, semanal, mensual. **C)** Establecer en el documento el procedimiento de resguardo de las bitácoras. *Por ejemplo*: respaldo y protección de *logs* en el caso de equipo de cómputo o zonas seguras de almacenamiento de bitácoras en papel, digitalización de registros. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Las bitácoras digitales y en papel deben resguardarse preferentemente en una zona independiente de la ubicación del sistema de información.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Noviembre 15, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Noviembre 19, 2021	
Observaciones / anotaciones		Se dispone bitácora a nivel de sistema operativo, también del webserver y de la aplicación. El sistema envía mensajes por correo electrónico ante algunos movimientos que son relevantes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)		IIBI-S2019		
Formato:	**22**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. IV. c) Proporcionar exclusivamente el acceso desde redes y servicios autorizados.**		
Aplicable en:		IV. Red de datos.		
Tiempo estimado:		Cuatro días hábiles.		
Importancia de la acción:		Es necesario reducir el mínimo necesario los puertos de comunicación para el funcionamiento del sistema de información.		
Proceso recomendado:		**A)** Revisar los puertos de comunicación (*TCP y UDP*) que requiera el sistema de información para su operación. *Por ejemplo*: para servicios *Web* los puertos 80 y 8080 son los convencionales. **B)** Activar en el sistema operativo la herramienta correspondiente para el control de puertos de comunicación. *Por ejemplo*, en Linux puede tratarse de un *firewall* a nivel de software o las herramientas que para tal efecto contenga la distribución correspondiente del sistema operativo. **C)** Dejar activos solamente los puertos necesarios para la operación del sistema. **D)** Activar el filtrado de la comunicación por direccionamiento IP en caso de ser posible para la operación del sistema. *Por ejemplo*: Permitir el acceso al puerto de *SSH* solamente a direcciones IP en una subred de la UNAM (132.248.x.y) o a un grupo de direcciones IP específicas. **E)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** No se deben tener activos accesos que no son necesarios vía la red de datos.		
Conocimientos requeridos:		Administración de sistema de información. Administración de sistema operativo.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			NOVIEMBRE 15, 2021	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			NOVIEMBRE 19, 2021	
Observaciones / anotaciones		En el caso de acceso y puertos utilizados, se Tienen abiertos los que son indispensables. Se cuenta con *firewall*, sólo se da acceso por *SSH* a IP del IIBI y se restringe cualquier otro puerto Sin incidentes.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**23**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 18. I. b) Contar con entornos para desarrollo, pruebas y operación.**		
Aplicable en:		I. Bases de datos y sistemas de tratamiento.		
Tiempo estimado:		Veinte días hábiles.		
Importancia de la acción:		Para evitar riesgos innecesarios a la información, el desarrollo y actualización de los mismos deberá ser realizado siempre en una plataforma y ambientes por separado.		
Proceso recomendado:		**A)** Instalar y configurar equipos similares en características, preferentemente virtuales, a los equipos donde se instalará el sistema de información en su nueva o actualizada versión. **B)** Crear un repositorio en un equipo central de desarrollo para el resguardo de códigos, documentación, inventarios de datos y manuales de usuario, administrador y programador. **C)** Ejecutar las pruebas de nuevas versiones o actualizaciones del sistema de información en el equipo dispuesto para tal efecto. Nunca usar -equipos físicos o virtuales con el sistema actualmente en producción como las plataformas para evaluación de versiones en desarrollo. **D)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Se deben realizar respaldos de la información en los sistemas en desarrollo del mismo modo que como se realicen con el sistema en producción.		
Conocimientos requeridos:		Administración de sistema de información. Desarrollo de aplicaciones.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Aplicación constante	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Aplicación constante	
Observaciones / anotaciones		Se tiene ambiente de pruebas con características equivalentes al ambiente de producción. En este entorno se realizan pruebas, mejoras, actualizaciones.		

(GESTIÓN INTEGRAL DE EVENTOS ACADÉMICOS- GINEA)			IIBI-S2019	
Formato:	**27**	**Verificación anual**	**Acción concluida**	(X)
Medidas de seguridad técnicas:		**Artículo 19. III. c) Aplicar el programa de mantenimiento preventivo a los equipos.**		
Aplicable en:		III. Equipos de cómputo.		
Tiempo estimado:		Seis días hábiles.		
Importancia de la acción:		Garantizar que el plan de mantenimiento de equipo se realiza en tiempo y forma.		
Proceso recomendado:		**A)** En caso de que el personal del Área Universitaria pueda realizar el mantenimiento preventivo, definir el calendario de inactividad del sistema de información, notificar a los usuarios y aplicar el plan en caso de mantenimiento o inactividad. **B)** En caso de que sea a través de un proveedor que se proporcione el mantenimiento al equipo de cómputo, ejecutar el calendario de acciones preventivas en un período no superior a cada 3 meses hasta la conclusión del contrato o póliza respectivo. **C)** Llenar y firmar formato.		
Mejores prácticas, referencias:		**1.-** Debe actualizarse el equipo de cómputo de manera suficiente para continuar la operación del sistema y considerar en el mantenimiento preventivo sistemas paralelos de manera temporal hasta la conclusión de los trabajos.		
Conocimientos requeridos:		Administración de infraestructura.		
Ejecución			**Fecha inicio**	
RENÉ PÉREZ ESPINOSA			Junio 20, 2022	
Nombre y firma			**Fecha término**	
Administrador del sistema de información o servidor			Junio 24, 2022	
Observaciones / anotaciones		Se da seguimiento al Plan de Recuperación de Información ante Desastres. Sin incidentes.		