UNIVERSIDAD NACIONAL DE ASUNCIÓN

Facultad de Derecho y Ciencias Sociales

Consejo Directivo

Acta N° 15/2023.-

Sesión Ordinaria de fecha 13 de junio de 2023. -

Resolución H.C.D. N° 548 /2023.-

"POR LA CUAL SE APRUEBA EL REGLAMENTO INTERNO DE GESTIÓN, USO Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES-UNA". ----------

V I S T O:

El DÉCIMOTERCER punto del Orden del Día de la Sesión Ordinaria de la fecha, y; ----------

C O N S I D E R A N D O:

Que, en fecha 11 de mayo de 2023, el Director de Tecnología e Informática de la Facultad de Derecho y Ciencias Sociales de la UNA, presentó el proyecto de "REGLAMENTO DE GESTIÓN, USO Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN", que tiene por objeto establecer el marco regulatorio de la actividad informática, su correcta administración y la optimización del uso y aprovechamiento de todos los recursos informáticos de la Facultad. También se establecen las medidas administrativas sobre seguridad informática de cumplimiento obligatorio para todos los funcionarios, docentes y estudiantes, en todas las sedes y filiales. Además, se definen las responsabilidades, tanto de los usuarios como de los administradores, en cuanto a la seguridad informática, física, lógica, operativa y el plan de contingencia ante eventos catastróficos. Asimismo, todo lo relativo al manejo preventivo en relación a las vulnerabilidades, sistemas informáticos utilizados, uso del correo institucional y las prohibiciones, así como la tipificación del tipo de falta, ante infracciones cometidas y su remisión al "Reglamento General Disciplinario Único para las Autoridades Universitarias, Docentes, Graduados, Estudiantes y Funcionarios de la UNA". ----------

Que, la Ley N° 1535/99 "De Administración Financiera del Estado", y su Decreto Reglamentario N° 8127/2000, "Por el cual se Establecen las Disposiciones Legales y Administrativas que Reglamentan la Implementación de la Ley N° 1535/99" y, el funcionamiento del Sistema Integrado de Administración Financiera-SIAF"; el Decreto N° 6234/2016 "Por el cual se declara de Interés Nacional la aplicación y el uso de las Tecnologías de la Información y Comunicación (TIC) en la Gestión Pública", se define la estructura mínima con la que deberá contar y se establecen otras disposiciones para su efectivo funcionamiento; la Ley N° 4995/2013 "De Educación Superior"; el Estatuto de la Universidad Nacional de Asunción, la Resolución H.C.D. N° 1469/2021 "Por la cual se aprueba el Plan Estratégico Institucional (PEI) de la Facultad de Derecho y Ciencias Sociales de la UNA 2021-2025", son disposiciones que generalizan el uso de TICs para el desarrollo y cumplimiento de las actividades institucionales y las contempladas para el logro de los objetivos estratégicos enmarcados en el PEI 2021-2025 de la Facultad de Derecho y Ciencias Sociales UNA, por lo que es necesario establecer la normativa interna que defina las

responsabilidades y la aplicación de las políticas institucionales aplicables al uso de las Tecnologías de la Información y Comunicación.

Que, la Decana elevó a consideración de los señores Consejeros la cuestión; quienes por unanimidad, aprobaron el proyecto de REGLAMENTO INTERNO DE GESTIÓN, USO Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES, De conformidad al Estatuto, entre los "Deberes y atribuciones del Consejo Directivo", Art. 56° inciso m) *"Aprobar los reglamentos internos de Facultad y proceder a su comunicación"*. ----------

Que, el tema fue tratado en Sesión Ordinaria del Consejo Directivo, **Acta N° 15/2023, de fecha 13 de junio de 2023.** ----------

POR TANTO, en uso de sus atribuciones legales, estatutarias y reglamentarias; ----------

EL HONORABLE CONSEJO DIRECTIVO DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES DE LA UNIVERSIDAD NACIONAL DE ASUNCIÓN;

R E S U E L V E:

Art. 1°.- APROBAR el REGLAMENTO INTERNO DE GESTIÓN, USO Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES-UNA, de cumplimiento obligatorio para todos los funcionarios, docentes y estudiantes de la FDCS; el cual se transcribe a continuación:

REGLAMENTO INTERNO DE GESTIÓN, USO Y SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE LA FACULTAD DE DERECHO Y CIENCIAS SOCIALES

El presente reglamento tiene por objeto establecer el marco regulatorio de la actividad informática, su correcta administración y la optimización del uso y aprovechamiento de todos los recursos informáticos de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Asunción.

1. SIGLAS

FDCS: Facultad de Derecho y Ciencias Sociales
UNA: Universidad Nacional de Asunción
DTI: Dirección de Tecnología e Informática
CNC: Centro Nacional de Computación
E-ALU: Modulo del Sistema Académico para Consultas de Alumnos Vía Web.
CTAD: Coordinación de Tecnologías Aplicadas al Derecho.

2. DEFINICIONES

- **USUARIO:** persona que utiliza uno o varios recursos informáticos de la FDCS para el desarrollo de sus tareas específicas.
- **CÓDIGO DE USUARIO:** designación alfabética, compuesta por las iniciales del nombre y apellido del usuario, asignado por la DTI, autorizado para la utilización de herramientas informáticas (sistemas informáticos, correo, etc.).

- **CONTRASEÑA O PASSWORD:** designación alfanumérica compuesta por letras mayúsculas, minúsculas, números o caracteres especiales, con una longitud mínima de 7 caracteres, definidas por el usuario.
- **ACCESOS:** combinación del código de usuario y la contraseña asignada al usuario para la utilización de las herramientas informáticas.
- **BACKUPS:** copia de seguridad de las bases de datos de los sistemas utilizados.
- **HARDWARE:** componentes físicos de un equipo informático (teclado, mouse, monitor, impresora, etc.).
- **SOFTWARE:** programas informáticos utilizados en la institución.
- **INFORMACIÓN/ES:** toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, papel, en pantallas de computadoras, audiovisual u otros.
- **TECNOLOGÍA DE INFORMACIÓN:** software y hardware operados por la FDCS para procesar información a su nombre, para llevar a cabo una función propia de la FDCS, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- **VULNERABILIDAD:** debilidad de un sistema, permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.
- **SERVIDORES DE DATOS:** computadoras de gran porte que contienen las bases de datos de todos los sistemas utilizados.
- **ROUTERS:** computadoras o equipos informáticos cuya función es la de manejar el tráfico de datos en forma externa (VPN) o interna (WIFI).
- **SEGURIDAD INFORMÁTICA**: conjunto de medidas administrativas, organizativas, físicas, técnicas, legales y educativas dirigidas a prevenir, detectar y responder ante acciones que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información que se procese, intercambie, reproduzca y conserve, a través de las tecnologías de información.
- **SWITCH:** dispositivo que permite la conexión de múltiples dispositivos a una red.

CAPÍTULO I - NORMATIVAS

3. INTRODUCCIÓN

Los equipos y sistemas informáticos son recursos de vital importancia para la FDCS de la UNA, pues sin estas herramientas, la operatividad cotidiana estaría comprometida. Por esta razón, la DTI deberá tomar las acciones apropiadas para proteger los equipos y datos, para asegurar que la información esté debidamente protegida contra cualquier amenaza o daño que podrían conducir a la pérdida, modificación o divulgación ilegal de las mismas. Con este fin se deberá contar con estas tres características determinantes:

a) **Integridad**: la información y los datos serán protegidos contra modificaciones no autorizadas.
b) **Confidencialidad**: la información y los datos serán divulgados solamente para situaciones específicas y bajo autorización.
c) **Disponibilidad**: los sistemas de aplicación estarán disponibles y utilizables cuando sea preciso.

4. OBJETIVOS Y ALCANCE

a) Establecer los principios, criterios y requerimientos de seguridad informática, que garanticen la confidencialidad, integridad y disponibilidad de la información que se procesa, intercambia

reproduce y conserva, mediante el uso de las tecnologías de información, siendo el jefe de cada dirección, departamento y sedes de la Institución, los responsables del cumplimiento de todo lo dispuesto en este reglamento.

b) Establecer las responsabilidades, directivas y requerimientos, a fin de implementar un nivel de protección de las plataformas tecnológicas y sistemas informáticos de la Institución.
c) La información que se procese, intercambie, reproduzca y conserve, a través de los medios técnicos de computación se considerará un bien de la Institución.
d) Los usuarios deberán hacer un uso racional y seguro de la infraestructura informática y los servicios de red de la Institución.
e) Este reglamento será de cumplimiento obligatorio en todas las sedes, filiales y dependencias de la FDCS que cuenten con tecnologías de información.
f) Este reglamento deberá ser revisado con una periodicidad mínima anual o, cuando se originen cambios en la FDCS, que puedan afectar la operatividad de los servicios de la DTI.

5. ÁMBITO DE APLICACIÓN

a) Este reglamento será de cumplimiento obligatorio para todos los funcionarios, docentes y estudiantes de la FDCS. Su inobservancia tendrá como consecuencia, la instrucción de un sumario administrativo, del que podrán derivar sanciones previstas en el "Reglamento General Disciplinario Único para las Autoridades Universitarias, Docentes, Graduados, Estudiantes y Funcionarios de la UNA", aprobado por Resolución del CSU N° 0149-00-2021, Acta N° 13/2021.
b) Todo usuario que utilice los equipos y sistemas informáticos de la FDCS, deberá observar lo prescripto en este reglamento, su desconocimiento no lo exime de las sanciones ocasionadas por su incumplimiento.

6. RESPONSABILIDADES

a) Todo usuario que utilice las herramientas informáticas, sin distinción de jerarquía, será responsable del cumplimiento de las políticas y procedimientos vigentes, con respecto a la seguridad informática, cuidado de equipos, correcta utilización y manejo de la información.
b) El acceso otorgado a los usuarios para el uso de los sistemas, será de exclusiva responsabilidad de los mismos. Cada operación realizada es registrada en la Auditoría de los Sistemas, con el código de usuario correspondiente, a fin de deslindar responsabilidades, por cualquier problema que pudiese ocurrir. El usuario podrá solicitar el cambio de la contraseña a la DTI, en caso de necesidad.
c) Las cuentas de correos institucionales, tanto de funcionarios como docentes de la FDCS, serán de exclusiva responsabilidad de los mismos. Todos los documentos remitidos, a través de este medio, serán considerados como documentación oficial de la FDCS.
d) Los directores y jefes de departamentos, serán responsables del control de la correcta utilización de los equipos por parte de los usuarios, con referencia al acceso a páginas de Internet, visualización de películas, descargas, etc., a fin de evitar la proliferación de virus informáticos que podrían afectar a todos los equipos conectados a la red interna.
e) El usuario deberá comunicar a la DTI, cualquier deficiencia o funcionamiento anómalo que observe en el proceso de utilización de equipos y sistemas, a fin de tomar los recaudos pertinentes. En las filiales, el usuario deberá comunicar al Encargado de la Seguridad Informática, y éste a su vez, a la DTI.

f) Las Direcciones de Gestión de Capital Humano y de Talento Humano - Área Docente, deberán comunicar a la DTI cuando el funcionario o docente, deje de pertenecer al plantel de la FDCS, a fin de eliminar todas las cuentas y accesos creados para el mismo.

CAPÍTULO II
DE LAS MEDIDAS ADMINISTRATIVAS SOBRE LA SEGURIDAD INFORMÁTICA

7. POLÍTICAS DE SEGURIDAD INFORMÁTICA Y DE CONTINGENCIA
POLÍTICAS SOBRE SEGURIDAD INFORMÁTICA

a) El establecimiento de las políticas apunta a garantizar la seguridad informática, para lo cual se analizará la gestión informática de cada dependencia, la que abarcará: el flujo de la información, tecnologías de información disponibles, alcance de la actividad informática, dentro y fuera de la entidad, clasificación de la información que se procesa, determinación de la información sensible para la actividad fundamental y aplicación de los controles establecidos; para evaluar la vulnerabilidad de los sistemas y los principales riesgos.

b) Las políticas de seguridad de la información y de los sistemas utilizados, deberán cumplir con los siguientes requerimientos:

- Identificación del usuario y contraseña para los sistemas utilizados.
- Responsabilidad del usuario en la protección de contraseñas personales (cambio periódico), para evitar accesos no autorizados.
- Seguridad de las computadoras personales, incluyendo protección, reporte y eliminación de virus.
- Normas de acceso y utilización de Internet (CAPÍTULO VI).
- Normas para el uso de los correos institucionales (CAPÍTULO VI).
- Normas para el uso de los sistemas utilizados por cada dependencia (CAPÍTULO VI).

POLÍTICAS SOBRE PLAN DE CONTINGENCIA PARA LA SEGURIDAD INFORMÁTICA

a) El plan de contingencia para la seguridad informática es una exigencia para la Institución, con el fin de garantizar la continuidad de los procesos informáticos ante la eventualidad de un siniestro.

b) El plan de contingencia deberá contener las medidas que permitan la evacuación, preservación y traslado de los medios y soportes destinados al procesamiento, intercambio y conservación de información clasificada o sensible.

c) El plan de contingencia será socializado en todas las dependencias de la FDCS, para su correcta aplicación por los usuarios y responsables.

d) El plan de contingencia está establecido en los ítems 8) SEGURIDAD FÍSICA, y 9) SEGURIDAD LÓGICA (sistemas).

8. SEGURIDAD FÍSICA

Requerimientos de protección física en áreas vitales:

a) El superior jerárquico será el responsable de los equipos informáticos asignados a su dependencia, por lo cual deberá tomar los recaudos pertinentes para su salvaguarda.

b) Se considerarán áreas vitales, aquellas donde se encuentren los principales equipos de la institución: servidores de datos, routers, switches, etc., por medio de las cuales se procesan las

informaciones, a través de las tecnologías, donde se aplicarán las siguientes medidas de protección física:

- Estarán ubicados en lugares de construcción sólida, con puertas y ventanas provistas de cierres seguros; debiendo cumplir con los requerimientos básicos, que reduzcan al mínimo las probabilidades de captación de irradiaciones electromagnéticas que los medios técnicos de computación y comunicaciones emiten.
- El área donde se encuentren los servidores, deberá contar con una temperatura ambiente de no más de 22° C, debido al calor constante que emiten dichos equipos.
- Las locaciones que tengan ventanas con comunicación al exterior, deberán contar con medidas que eviten la visibilidad hacia el interior de la instalación.
- Se deberán instalar sistemas de detección y alarma de incendios en todos los lugares que lo requieran.

c) El manejo de los equipos informáticos, deberán seguir las pautas detalladas a continuación:

- Los equipos solo podrán utilizarse para actividades propias del trabajo. Queda terminantemente prohibido su uso para otros fines, tales como: juegos, pasatiempos, cuestiones personales, etc.
- No podrán modificarse ni el hardware y ni el software instalados, proveídos e instalados por el Departamento de Redes y Equipos de la FDCS.
- No estará permitido fumar, comer o beber durante la utilización de un equipo informático.
- Los equipos informáticos deberán ser protegidos de riesgos del medio ambiente (polvo, agua, incendio, etc.).
- Los equipos informáticos utilizados, deberán contar con fuentes de poder ininterrumpibles (UPS), siempre que exista disponibilidad.
- Todo medio de almacenamiento a ser utilizado en el equipo informático, deberá ser previamente verificado por un software antivirus.
- El usuario que detecte cualquier falla en los equipos o en la red interna, deberá ser reportado inmediatamente a la DTI. En las Filiales deberá reportarse al Encargado de la Seguridad Informática.
- La pérdida o robo de cualquier componente del hardware, deberá ser reportado inmediatamente por el responsable de la dependencia a la DTI y al Departamento de Patrimonio, a fin de deslindar responsabilidades.

d) El ingreso y permanencia de funcionarios en las áreas vitales, será permitido de acuerdo al nivel de acceso que se les haya otorgado y el trabajo desempeñado. El personal de servicio, mantenimiento de equipos u otro, que eventualmente precise permanecer en el área, lo hará siempre en presencia de las personas responsables y con la identificación visible.

e) El traslado de equipos informáticos, en todos los casos, deberá realizarse respetando las normas de conservación de los mismos, con el objetivo de garantizar la integridad y confidencialidad de la información que contienen y cumplirán las medidas de protección establecidas de acuerdo a la clasificación de la misma.

f) El traslado de equipos fuera de la Institución, ya sea para mantenimiento o reparación, deberá ser autorizado por el Departamento de Redes y Equipos de la Institución. En las Filiales, el Encargado de la Seguridad Informática deberá solicitar el traslado de los equipos al Departamento de Redes y Equipos de la Institución.

g) El costo de la reparación por daños o la pérdida de equipos, serán cubiertos por quien lo haya ocasionado, cuando se comprobare que los mismos ocurrieron por el uso irregular de los mismos o por no guardar las medidas de seguridad establecidas en este reglamento. Sin perjuicio del

proceso disciplinario que se pudiera ocurrir como consecuencia de la inobservancia de las medidas de seguridad establecidas en este reglamento.

9. SEGURIDAD LÓGICA (SISTEMAS)

a) Las medidas para garantizar la seguridad lógica, establecidas en este capítulo, se implementarán a nivel de software y estarán en correspondencia directa con las informaciones que se manejen o trabajos desarrollados en cada dependencia.

b) Se implementarán mecanismos de control que permitan contar con un registro (auditoría) de los principales eventos que se ejecuten y puedan ser de interés para la detección o esclarecimiento, ante vulneraciones de la seguridad informática.

c) Cuando un funcionario sea trasladado de dependencia, se deberá informar a la DTI, por escrito, a los efectos de la cancelación o adecuación de los accesos informáticos otorgados.

d) Todos los sistemas destinados al procesamiento de información, deberán contar con las siguientes medidas de seguridad:

- Incluir los niveles de accesos a los sistemas informáticos, que, por las características propias de las dependencias, sean necesarias aplicar.
- Llevar registro con los distintos niveles de acceso otorgados a los usuarios, que se permita para el uso de los sistemas, acorde a los trabajos realizados;
- El superior jerárquico de cada sede o dependencia, deberá informar a la DTI, los nombres de los funcionarios asignados para la utilización de los sistemas, con el nivel de acceso otorgado a los mismos. Para el efecto, se deberá completar y remitir, la "Planilla de registro de usuarios y sistemas asignados", detallado en los anexos del presente reglamento.
- Los sistemas deberás contar con la capacidad de registrar todas las operaciones realizadas.

e) Se deberán salvar externamente, todas las informaciones del servidor de red (backups de bases de datos), en forma diaria, con el fin de recuperarlas o restaurarlas, en los casos de pérdida o destrucción de los equipos.

f) La DTI será la encargada de realizar las copias de seguridad del servidor (backup), en discos externos al servidor, en forma diaria; en la Sede Central.

g) El Encargado de la Seguridad Informática de las Filiales, tendrá a su cargo realizar las copias de seguridad del servidor (backup), en discos externos al servidor, en forma diaria.

h) Cada funcionario que utilice una computadora para realizar sus trabajos, será responsable de realizar las copias de respaldo de los documentos que considere importantes, para su restauración, ante cualquier falla que pudiese tener el equipo. La DTI y los encargados de realizar las copias de seguridad en las sedes o filiales, no serán responsables de los archivos contenidos en las computadoras del usuario, pero sí serán responsables de las bases de datos de los sistemas utilizados.

i) Las copias (backup) de las bases de datos diarias, serán registradas en un formulario por cada Encargado designado, cuya copia deberá ser remitido a la DTI, en forma semanal, a través del correo electrónico institucional.

j) El usuario que se vea impedido de realizar las copias de seguridad, deberá informar de ello a la DTI o al Encargado de la Seguridad Informática en las Filiales, a fin de tomar los recaudos pertinentes.

CAPITULO III – DE LA SEGURIDAD Y RESPONSABLES

10. SEGURIDAD DE OPERACIONES

a) La Institución deberá mantener identificadas las tecnologías de información y sistemas que posea (detallados en el TÍTULO V – GENERALIDADES).
b) La reparación y mantenimiento de los equipos destinados al procesamiento de información, estará a cargo de la empresa adjudicada, a través de un proceso de contratación pública, siendo la única responsable de la reparación o retiro del equipo, en caso necesario.
c) En el caso de retiro de cualquier equipo informático, esto deberá ser comunicada a la DTI, ya sea por memorando o vía correo institucional. El registro de los equipos retirados y/o devueltos, será a través de la "Planilla de movimiento de equipos informáticos", que será habilitado por el Encargado en cada sede o filial.
d) La actualización o mantenimiento de los sistemas informáticos utilizados en todas las sedes o filiales, estará a cargo del CNC, Institución proveedora de los sistemas informáticos para toda la UNA.

11. RESPONSABLE DE LA SEGURIDAD INFORMÁTICA

a) El Director del área de Tecnologías e Informática y el Jefe del Departamento de Comunicaciones, Redes y Equipos, serán los responsables de la seguridad informática en la sede Central y filiales, a través de un Encargado.
b) En las filiales, se designará a un Encargado de la Seguridad Informática, que ejercerá sus funciones bajo la supervisión de la DTI y del Departamento de Comunicaciones, Redes y Equipos. Este será propuesto por el Director de cada sede o filial, lo que deberá ser informado a la DTI, a través de la "Planilla de designación de responsables del backup".
c) El Encargado de la Seguridad Informática de sedes o fililaes, tendrá a su cargo las tareas de: realizar las copias de seguridad, de las bases de datos del servidor.
d) En las filiales, se deberá asignar a uno o más funcionarios, sin perjuicio de sus labores en otras dependencias, para realizar las copias de seguridad. Esta situación deberá ser informada a la DTI; a través de la misma "Planilla de designación de responsables del backup".

12. FUNCIONES DEL ENCARGADO DE LA SEGURIDAD INFORMÁTICA EN FILIALES Y EDIFICIO HISTÓRICO

a) Administrar la conexión de red y los equipos informáticos
b) Realizar las copias de seguridad (backups) de las bases de datos del servidor diariamente.
c) Aplicar los planes de seguridad informática y de contingencia.
d) Comunicar a la DTI cuando no se cuenten con los elementos o recursos para garantizar la seguridad informática, de acuerdo a las normas del presente reglamento y a las condiciones de trabajo del área.
e) Proponer y controlar la capacitación del personal vinculado a las labores de seguridad, con el objetivo de contribuir al conocimiento y cumplimiento de las medidas establecidas en el plan de seguridad informática y en este reglamento.

CAPÍTULO IV - TRABAJO EN REDES

13. SEGURIDAD DE OPERACIONES EN EL AMBIENTE DE LAS REDES DE DATOS

a) Estará prohibida la conexión de equipos informáticos a la red interna, sin la autorización de la DTI.
b) Toda solicitud de conexión de equipos a la red interna para la utilización de sistemas, internet y/o correo institucional, será solicitado, por el superior jerárquico de la dependencia, sede o filial a la DTI, indicando los datos del funcionario a ser habilitado, el detalle del o los sistemas a ser utilizados y el nivel de acceso al mismo.
c) Todo indicio de mal uso de los sistemas u equipos conectados a la red interna, deberá ser comunicado al superior jerárquico de la dependencia, sede o filial y, éste a la DTI.

14. FUNCIONES DEL ADMINISTRADOR DE UNA RED, EN RELACIÓN CON LA SEGURIDAD INFORMÁTICA

a) Toda red de computadoras deberá contar, para su operación, con un administrador que tendrá las siguientes funciones básicas:
- Velar por la aplicación de mecanismos implementados por las políticas de seguridad de la red.
- Velar por la utilización correcta, conforme a los fines perseguidos.
- Activar los mecanismos técnicos y estratégicos de respuesta, ante los distintos tipos de acciones nocivas identificadas.

CAPÍTULO V – SOBRE LAS VULNERACIONES DETECTADAS EN EL FUNCIONAMIENTO Y USO DE LAS TECNOLOGÍAS Y SISTEMAS INFORMÁTICOS.

15. VULNERACIONES DE FUNCIONAMIENTO.

Serán consideradas vulneraciones de funcionamiento, aquellas acciones que conlleven al daño, avería o destrucción de los sistemas, equipos, redes y accesorios informáticos de la Institución.

16. USO DE LA TECNOLOGÍA Y/O SISTEMAS PARA VULNERACIONES DEL FUNCIONAMIENTO.

También serán consideradas vulneraciones de funcionamiento, el uso de tecnologías y sistemas para realizar cargas o modificaciones, sin contar con los respaldos documentales correspondientes.

17. DETECCIÓN DE VULNERACIONES DE FUNCIONAMIENTO.

El usuario que detecte una vulneración al funcionamiento de sistemas, equipos, redes y accesorios informáticos, deberá informar inmediatamente de ello a la DTI y, en las filiales, al Encargado de la Seguridad Informática, quien informará a la DTI y al Director de la Filial. A los efectos de deslindar responsabilidades, se conformará una comisión para realizar las investigaciones preliminares necesarias y comunicarlo al Decanato, ante posibles infracciones de las medidas de protección establecidas en este reglamento.

18. INTEGRACIÓN DE LA COMISIÓN DE INVESTIGACIONES.

La comisión encargada de realizar la investigación preliminar, ante la ocurrencia de una vulneración al funcionamiento, estará integrada por el Director de Tecnología e Informática, el Asesor Jurídico y dos personas, que cuenten con los conocimientos técnicos e informáticos del área donde se haya producido

la falta, siempre que no estén implicados en las mismas, con el fin de esclarecer lo ocurrido y deslindar responsabilidades.

Verificada la comisión de una vulneración del funcionamiento, se remitirán los antecedentes para la instrucción del sumario administrativo, conforme al Reglamento General Disciplinario Único para las Autoridades Universitarias, Docentes, Graduados, Estudiantes y Funcionarios de la Universidad Nacional de Asunción, aprobado por Resolución del CSU N°.0149-00-2021, Acta N° 13/2021.

CAPÍTULO VI - NORMAS PARA LA UTILIZACIÓN DE HERRAMIENTAS WEB Y SISTEMAS INFORMÁTICOS

19. ACCESO Y UTILIZACIÓN DE INTERNET

a) El superior jerárquico de la dependencia será responsable de la correcta utilización de la conexión a Internet, poniendo especial cuidado para evitar la proliferación de virus informáticos que podrían afectar seriamente a toda la red de la FDCS.
b) El control de la correcta utilización de la conexión incluye no acceder a páginas ajenas a las actividades laborales, bajar películas o visualizarlas on line u otro tipo de acciones que puedan perjudicar a la red interna.
c) En caso de requerir la instalación de algún software; para realizar los trabajos propios de la dependencia, éste deberá ser solicitarlo a la DTI.
d) El usuario será responsable de la actualización del antivirus instalado en el equipo, así como la verificación periódica del mismo. Ante cualquier duda deberá recurrir al Departamento de Redes y Equipos.
e) La solicitud de nuevas conexiones a la red interna, deberá ser remitida a la DTI, detallando el motivo del pedido, a través del "Formulario para conexión a la red interna".

20. CORREOS INSTITUCIONALES

a) El correo institucional será asignado a los funcionarios y docentes, para uso en cuestiones laborales y académicas, por lo cual no podrá ser utilizado para asuntos particulares.
b) El usuario será el único responsable de las diligencias realizadas desde su correo institucional.
c) El usuario garantizará a la FDCS que no utilizará el correo institucional con fines ilícitos o prohibidos.
d) La solicitud de creación de un correo nuevo, deberá ser remitido a la DTI, detallando el motivo del pedido y los datos del funcionario: nombre completo, número de cédula, número de teléfono, sede y dependencia. Los docentes deberán detallar además: materia, turno y sección. Se utilizará para el efecto el "Formulario para cuentas institucionales".
e) Cada correo electrónico institucional está limitado a un espacio de almacenamiento de 5 GB por cuenta, por lo que la DTI no será responsable por la pérdida de datos que pudiera ocasionarse por exceder este límite de espacio o por las dificultades de acceso.

21. SISTEMAS INFORMÁTICOS

a) El usuario de los sistemas informáticos será el único responsable de los trabajos que realice en el sistema utilizado.
b) Cada usuario contará con una contraseña para el acceso y uso de los sistemas en cada dependencia, lo que permitirá registrar los movimientos realizados, a fin de recuperar las acciones ejecutadas, ante cualquier eventualidad.

CAPÍTULO VII. PROHIBICIONES

Estarán expresamente prohibidas las siguientes acciones:

a) Dañar los sistemas o equipos conectados a la red de la FDCS.
b) Diseminar virus, gusanos u otro tipo de programas dañinos para los sistemas de proceso de la información.
c) Congestionar los enlaces, comunicaciones o sistemas informáticos por la transferencia indebida de archivos, ejecución de programas, accesos a páginas de Internet, etc., ajenos a los objetivos de la Institución.
d) Utilizar los recursos de la FDCS para acceder a sitios de pornografía, audios en formato mp3 u otros, juegos en línea, horóscopos, chistes, apuestas o juegos de azar en general, o cualquier otra página web que no responda a los objetivos institucionales.
e) Afectar o paralizar algún servicio tecnológico ofrecido por la FDCS. El usuario tendrá prohibido descargar archivos de ningún tipo o instalar programas, ver películas, compras por internet, usar programas de intercambio de archivos o realizar otras acciones que puedan saturar la red interna.
f) Conectar equipos informáticos a la red interna, sin la autorización de la DTI.
g) Utilizar los medios de la FDCS con fines de propaganda política o comercial.
h) Usar las tecnologías y sistemas para realizar cargas o modificaciones en las bases de datos, sin contar con los respaldos documentales correspondientes.

La contravención de las prohibiciones contenidas en los incisos a), b), c), d), e) y f), serán consideradas como faltas leves y, la infracción a los incisos g) y h), serán consideradas faltas graves.
En general, la no aplicación de las medidas de seguridad establecidas en este reglamento, que pudieran acarrear daños, colapsos o interrupciones en los servicios proveídos por los sistemas informáticos, podrán acarrear procesos disciplinarios, conforme a la investigación preliminar.

CAPÍTULO VIII. GENERALIDADES

22. LA DIRECCIÓN DE TECNOLOGÍAS E INFORMÁTICA Y SUS DEPARTAMENTOS

La DTI de la FDCS de la UNA, está integrada por cuatro departamentos, con alcance en todas las sedes, filiales y Postgrado:

1) DEPARTAMENTO DE SISTEMAS (ÁREA ACADÉMICA)

Dependencia encargada del área académica – uso del sistema. Además, tiene a su cargo, el sistema automatizado de corrección de exámenes, a través de hojas especiales para selección múltiple de respuestas. Servicio que es utilizado también, por otras Instituciones, para la corrección de sus exámenes. Las tareas desarrolladas por este departamento, tienen relación directa con la Dirección Académica, de acuerdo a las reglamentaciones académicas vigentes.

2) DEPARTAMENTO DE COMUNICACIONES, REDES Y EQUIPOS (NOC)

Dependencia encargada de gestionar y/o realizar las acciones necesarias para garantizar el mantenimiento y operatividad de redes, equipos, sistemas, enlaces VPN, sistemas de CCTV, acceso a internet vía WIFI para estudiantes, apoyo informático, instalaciones de sistemas, etc. en todas las dependencias de la FDCS.

3) DEPARTAMENTO DE RED BANCARIA

Dependencia encargada de administrar y supervisar las operaciones realizadas por los estudiantes por medio de la red bancaria y el módulo del e-Alu (vía Web), para el pago de aranceles académicos y por servicios; además los pagos vía pos, en la sede Central, en coordinación con la Dirección de Giraduría y la Dirección de Contabilidad. Estas tareas incluyen a la Escuela de Ciencias Sociales y Ciencias Políticas y el Postgrado.

4) DEPARTAMENTO DE REGISTROS E INFORMES ESTADÍSTICOS ACADÉMICOS

Diseñar, coordinar, dirigir, y controlar los procesos prospección en virtud a los datos estadísticos del sector académico y administrativo. Las cargas de los datos estadísticos están vinculados al sistema integrado de programación presupuestaria (SIPP) del Ministerio de Hacienda y al Módulo de Sistema de Presupuesto por Resultados (SPR) de la Secretaría Técnica de Planificación.

5) DEPARTAMENTO DE SISTEMAS EN LAS FILIALES

Las filiales contarán con una dependencia que se encargará de las tareas relativas a la Tecnología e Información, con supervisión directa de la DTI, a través de los Departamentos de Sistemas y de Comunicaciones, Redes y Equipos (NOC). Este departamento contará con un Encargado de la Seguridad Informática, que tendrá las funciones de realizar la copia de seguridad diaria, administración de la red interna, y velar por el cumplimiento de este reglamento. El Encargado de la Seguridad Informática, no realizará las reparaciones de los equipos ni sistemas.

23. SISTEMAS UTILIZADOS POR LA INSTITUCIÓN

Los sistemas informáticos utilizados en la FDCS, son proveídos por el CNC, entidad encargada de los sistemas informáticos de la UNA, los cuales se detallan a continuación:

- ACAD5-SISTEMA ACADÉMICO: utilizado para la gestión de datos académicos de los alumnos, cargas de matrículas, inscripciones a exámenes, carga de notas finales y parciales, emisión de certificados de estudios, carga de actividades de extensión universitaria y otros datos académicos.
- SISTEMA ACADÉMICO del Departamento de Filiales: utilizado para los registros de calificaciones de las filiales y el control respectivo en la elaboración de los certificados de estudios.
- GCA-SISTEMA DE CAJA: utilizado para el cobro de aranceles académicos, derecho de examen y matrículas, conectado al sistema académico para la generación de la deuda.
- PERSON4-SISTEMA DE SUELDOS: utilizado para la liquidación de sueldos administrativos y docentes.
- EPR-SISTEMA DE EJECUCIÓN PRESUPUESTARIA: utilizado para la gestión presupuestaria, ejecución de rubros y solicitudes de transferencias de recursos.
- PATRIM4-SISTEMA DE PATRIMONIO Y ALMACÉN: utilizado para la gestión de bienes de la institución y el control de la distribución de materiales y suministros de almacén.
- RH-SISTEMA DE GESTIÓN DE RECURSOS HUMANOS: utilizado para el control de entrada/salida del personal, cálculo de horas extras, entre otros. La Sede Central cuenta con cuatro relojes marcadores distribuidos en los siguientes puntos: Administración (dos), Dirección Académica, área de Institutos y un reloj en el Edificio Histórico.
- SGB-SISTEMA DE GESTIÓN DE BIBLIOTECA: utilizado para la carga de los materiales bibliográficos disponibles en la biblioteca (sede Central y filiales) y los movimientos de los mismos.

- GDOC-SISTEMA DE GESTIÓN DE DOCUMENTOS: utilizado para el seguimiento de los documentos ingresados por Mesa de Entrada de la Institución. Los usuarios pueden realizar el seguimiento de sus documentos ingresados, vía Web.
- E-ALU: módulo de consulta Web, desde el cual, los estudiantes pueden consultar sobre sus informaciones académicas, administrativas, realizar inscripciones a exámenes y matriculaciones on line.
- Además, se cuenta con plataformas utilizadas para las clases virtuales, administradas por la CTAD: Classroom y EDUCA.

Todos los sistemas mencionados cuentan con niveles de acceso para cada usuario y registros de auditoría.

SISTEMAS INFORMÁTICOS UTILIZADOS EN FILIALES, LA ESCUELA DE CIENCIAS SOCIALES Y CIENCIAS POLÍTICAS Y POSTGRADO:

La FDCS cuenta con nueve filiales en el interior del país: Quiindy, San Juan Bautista Misiones, Caacupé, Coronel Oviedo, Caaguazú, San Estanislao, San Pedro, Pedro Juan Caballero y Benjamín Aceval. Además, la sede de la Escuela de Ciencias Sociales y Ciencias Políticas, localizada en el Edificio Histórico (Yegros y Mariscal Estigarribia), donde son utilizados los siguientes sistemas:

- ACAD5-SISTEMA ACADÉMICO
- GCA-SISTEMA DE CAJA

En cada sede y filial, se cuenta con un sistema independiente de control de entrada/salida de funcionarios, por medio de un reloj de marcación.

24. SISTEMAS EXTERNOS (DEL MINISTERIO DE HACIENDA)

La FDCS utiliza los sistemas informáticos del Ministerio de Hacienda, a los cuales se accede por medio de la red metropolitana, por conexión VPN con el CNC, los que se detallan a continuación:

- SICO (Sistema de Contabilidad).
- SIPP-PLAN FINANCIERO (Sistema de Carga del Plan Financiero y actualización de metas de productos).
- SIPP-PLURIANUAL (Sistema de Carga de Anteproyectos Anuales y Plurianuales).
- SIPP-PAC (Sistema de Plan Anual de Contrataciones).
- SINARH (Sistema de Recursos Humanos).

25. OTROS SISTEMAS Y MÓDULOS UTILIZADOS

1. SISTEMA DE CORRECCIÓN DE EXÁMENES

El sistema de corrección de exámenes, se realiza por medio de hojas de respuestas para selección múltiple, proveídos por el Departamento de Sistemas, con una capacidad para corregir hasta cien preguntas con cinco opciones de respuestas por cada una. Las hojas de respuestas de los alumnos, la matriz de respuestas correctas y otros datos del examen, son cargados en un sistema informático, para su procesamiento y la expedición de los reportes correspondientes.

Este sistema es utilizado por los docentes, tanto para las correcciones de exámenes parciales como finales, considerando la gran cantidad de alumnos matriculados en cada materia, la velocidad de corrección y, principalmente, la seguridad en los resultados (error cero).

La DTI cuenta con escáneres de alta velocidad, para la lectura de hojas de respuestas, con un promedio de cincuenta y cinco lecturas por minuto.

Además de los exámenes de grado, la FDCS también colabora con la corrección de exámenes con afluencia masiva de participantes, a pedido de las diferentes instituciones públicas.

2. SISTEMA DE CONTROL DE ASISTENCIA A CLASES

Todas las aulas de la sede Central, cuentan con relojes marcadores (con lector de huella dactilar), para el control de asistencia a clases de los alumnos. Los lectores tienen gran capacidad de almacenamiento de transacciones y registro de estudiantes, así como mini baterías para un funcionamiento de hasta dos horas en caso de corte de corriente eléctrica.

El sistema tiene la capacidad para elaborar los informes porcentuales de asistencia, para cada materia, turno y sección.

3. PAGO DE ARANCELES VÍA WEB

El módulo e-Alu, permite al alumno acceder a sus datos académicos y administrativos, así como al proceso de pago de aranceles desde Internet, utilizando una contraseña proporcionada por el Departamento de Sistemas. Igualmente, gestionar sus matriculaciones e inscripciones a exámenes finales.

La empresa para realizar los pagos es Bancard S.A., la cual cuenta con bocas de cobranza en todo el territorio nacional.

Las direcciones de acceso son las siguientes:

https://www.cnc.una.py/ealu/#/pages/login (acceso al módulo del e-Alu).

https://www.infonet.com.py (acceso al portal de pagos de aranceles vía web).

La aplicación e-Alu está disponible en el Play Store, para su utilización en dispositivos móviles.

4. SEGURIDAD (CCTV)

La sede Central de la FDCS, cuenta con cámaras de seguridad en todo el predio, con cámaras instaladas en la plata alta, con cobertura en los estacionamientos, accesos al edificio, pasillos, Aula Magna y Biblioteca. Así mismo, en la planta baja, en el área administrativa, con cobertura en las Cajas y todos los accesos.

El Edificio Histórico y todas las Filiales, también cuentan con cámaras de seguridad con cobertura en los accesos principales y áreas sensibles.

26. FORMULARIOS PARA SOLICITUDES.

1. FORMULARIO DE REGISTRO DE COPIAS DE SEGURIDAD DIARIA
2. FORMULARIO DE REGISTRO DE USUARIOS Y SISTEMAS ASIGNADOS
3. FORMULARIO DE MOVIMIENTO DE EQUIPOS INFORMÁTICOS
4. FORMULARIO PARA CONEXIÓN A LA RED INTERNA
5. FORMULARIO PARA CUENTAS INSTITUCIONALES
6. FORMULARIO PARA DESIGNACIÓN DE RESPONSABLES DEL BACKUP

FORMULARIO DE REGISTRO DE COPIAS DE SEGURIDAD DIARIA
PLANILLA DE REGISTRO DE BACKUP O COPIAS DE RESPALDO DE LA BASE DE DATOS

(1) SEDE:				
(2) N°	**(3) FECHA DE COPIA DEL BACKUP**	**(4) HORA DEL PROCESO**	**(5) ENCARGADO**	**(6) FIRMA**

OBS.: se debe remitir una copia en forma semanal a la DTI.

1) SEDE (CENTRAL/FILIAL)
2) NÚMERO SECUENCIAL.
3) FECHA DE REALIZACIÓN DEL BACKUP.
4) HORA DE REALIZACIÓN DEL BACKUP.
5) NOMBRE DEL FUNCIONARIO QUE REALIZA EL PROCESO DE COPIA DEL BACKUP.
6) FIRMA DEL FUNCIONARIO QUE REALIZA EL PROCESO DE COPIA DEL BACKUP.

FORMULARIO DE REGISTRO DE USUARIOS Y SISTEMAS ASIGNADOS
PLANILLA DE SOLICITUD DE CREACIÓN DE USUARIOS PARA SISTEMAS

(1) SEDE/DEPARTAMENTO:				
(2) N°	**(3) APELLIDOS Y NOMBRES DEL FUNCIONARIO**	**(4) CÓDIGO DE USUARIO**	**(5) SISTEMA/S UTILIZADO/S**	**(6) ACCESO (TOTAL /PARCIAL/BORRADO)**

(7) OBSERVACIONES:
(8) FIRMA SOLICITANTE:

OBS.: los cambios de accesos deberán ser remitidos a la DTI, usando este mismo formulario.

1) SEDE (CENTRAL/FILIAL)/DEPARTAMENTO
2) NÚMERO SECUENCIAL.
3) NOMBRE DEL FUNCIONARIO AL CUAL SE SOLICITA LA CREACIÓN DE USUARIO PARA UTILIZACIÓN DEL SISTEMA.
4) CÓDIGO DEL FUNCIONARIO A SER ASIGNADO (ESTE CAMPO LO LLENA LA DTI).
5) SISTEMA AL CUAL SE REQUIERE PARA EL ACCESO.
6) TIPO DE ACCESO REQUERIDO PARA EL SISTEMA (TOTAL O PARCIAL). EN CASO DE PARCIAL DETALLAR QUE MÓDULOS U OPCIONES SON LOS REQUERIDOS. SÍ ES PARA BORRADO DEL ACCESO, SE UTILIZA ESTE MISMO FORMULARIO.
7) OBSERVACIONES, EN CASO NECESARIO.
8) FIRMA DEL JEFE O ENCARGADO QUE SOLICITA EL ACCESO PARA EL FUNCIONARIO.

FORMULARIO DE MOVIMIENTO DE EQUIPOS INFORMÁTICOS

PLANILLA DE REGISTRO DE MOVIMIENTO DE EQUIPOS INFORMÁTICOS

(1) SEDE/DEPARTAMENTO:					
(2) N°	(3) DETALLE DEL EQUIPO RETIRADO	(4) CÓDIGO DE PATRIMONIO	(5) FECHA/HORA DE RETIRO	(6) FECHA/HORA DE DEVOLUCIÓN	(7) FIRMA RESPONSABLE

(7) OBSERVACIONES:

(8) RETIRADO POR:

OBS.: cualquier equipo retirado deberá ser comunicado a la DTI para realizar los reclamos correspondientes.

Por cada equipo retirado se debe llenar una planilla independiente.

1) SEDE (CENTRAL/FILIAL)/DEPARTAMENTO
2) NÚMERO SECUENCIAL.
3) DETALLE DEL EQUIPO A SER RETIRADO (PC, NOTEBOOK, MONITOR, ETC.).
4) CÓDIGO DE PATRIMONIO DEL EQUIPO A SER RETIRADO.
5) FECHA Y HORA DE RETIRO DEL EQUIPO.
6) FECHA Y HORA DE LA DEVOLUCIÓN (A SER LLENADO POR LA DTI).
7) FIRMA DEL ENCARGADO DEL EQUIPO A SER RETIRADO.
8) EN OBSERVACIONES DETALLAR EL MOTIVO DEL RETIRO Y LA PERSONA O EMPRESA QUE RETIRA EL EQUIPO.

FORMULARIO PARA CONEXIÓN A LA RED INTERNA

PLANILLA DE SOLICITUD DE CONEXIÓN A LA RED INTERNA

(1) SEDE/DEPARTAMENTO:				
(2) N°	(3) CÓDIGO DE PATRIMONIO DEL EQUIPO:	(4) CONEXIÓN PARA USO DE:	(5) FECHA/HORA DE PEDIDO	(6) FIRMA RESPONSABLE

(7) OBSERVACIONES:

1) SEDE (CENTRAL/FILIAL)/DEPARTAMENTO
2) NÚMERO SECUENCIAL.
3) CÓDIGO DE PATRIMONIO DEL EQUIPO A SER CONECTADO A LA RED INTERNA.
4) MOTIVO DEL PEDIDO (USO DE SISTEMAS, INTERNET, ACCESO A DISPOSITIVOS DE LA RED).
5) FECHA Y HORA DEL PEDIDO.
6) FIRMA DEL JEFE O ENCARGADO QUE REALIZA EL PEDIDO.
7) EN OBSERVACIONES DETALLAR EL NOMBRE DEL FUNCIONARIO QUE UTILIZARA EL EQUIPO.

FORMULARIO PARA CUENTAS INSTITUCIONALES
PLANILLA DE CREACIÓN/ELIMINACIÓN DE CUENTAS INSTITUCIONALES

(1) CREACIÓN/ELIMINACIÓN EN CASO DE ELIMINACIÓN DETALLAR LA CUENTA A SER ELIMINADA	
(2) APELLIDOS Y NOMBRES	
(3) CÉDULA DE IDENTIDAD N°	
(4) TELÉFONO	
(5) SEDE/DEPARTAMENTO	
(6) CARGO - MATERIA (SI ES DOCENTE)	
(7) TIPO DE CUENTA (ADMINISTRATIVO/DOCENTE)	
(8) FECHA/HORA DEL PEDIDO	
(9) RESPONSABLE DEL PEDIDO	
(10) FIRMA	
(11) FECHA DE PROCESO DEL PEDIDO	
(12) PROCESADO POR (DTI). FIRMA/ACLARACIÓN	

OBS.: para eliminaciones de cuentas, también se utilizará el mismo formulario.

1) DETALLAR SI ES CREACIÓN O ELIMINACIÓN DE CUENTA (DE CORREO INSTITUCIONAL).
2) NOMBRE DEL FUNCIONARIO.
3) CEDULA DEL FUNCIONARIO.
4) TELÉFONO DEL FUNCIONARIO.
5) SEDE/DEPARTAMENTO DEL FUNCIONARIO.
6) CARGO DEL FUNCIONARIO O MATERIA SI ES DOCENTE.
7) TIPO DE CUENTA A SER CREADA, ADMINISTRATIVO O DOCENTE.
8) FECHA Y HORA DEL PEDIDO.

9) JEFE O ENCARGADO QUE REALIZA EL PEDIDO.
10) FIRMA DEL JEFE O ENCARGADO QUE REALIZA EL PEDIDO.
11) FECHA DE PROCESO (A SER LLENADO POR LA DTI)
12) PROCESADO POR EL FUNCIONARIO DE LA DTI (A SER LLENADO POR LA DTI).

FORMULARIO PARA DESIGNACIÓN DE RESPONSABLES DEL BACKUP
PLANILLA DE DESIGNACIÓN A RESPONSABLE DE LAS COPIAS DE RESPALDO (BACKUP)
DE LA BASE DE DATOS

(1) FECHA/HORA:	
(2) DESIGNACIÓN/CAMBIO (SI ES CAMBIO, DETALLAR EL DATO DEL FUNCIONARIO DESIGNADO ANTERIOR)	
(3) APELLIDOS Y NOMBRES	
(4) CEDULA DE IDENTIDAD N°	
(5) TELÉFONO Y CORREO	
(6) SEDE/DEPARTAMENTO	
(7) CARGO	
(8) FIRMA FUNCIONARIO DESIGNADO	
(9) FIRMA/ACLARACIÓN DEL DIRECTOR	

OBS.: para cambio de designación utilizar el mismo formulario.
1) FECHA/HORA DEL LLENADO DE LA PLANILLA
2) COMPLETAR SI ES DESIGNACIÓN O CAMBIO DEL RESPONSABLE.
3) NOMBRE DEL FUNCIONARIO.
4) CEDULA DEL FUNCIONARIO.
5) TELÉFONO DEL FUNCIONARIO.
6) SEDE/DEPARTAMENTO DEL FUNCIONARIO.
7) CARGO DEL FUNCIONARIO.
8) FIRMA DEL FUNCIONARIO DESIGNADO.
9) FIRMA Y ACLARACIÓN DEL DIRECTOR DE LA SEDE.

Art. 2°.- COMUNICAR a quienes corresponda y cumplido, archivar. -----

JOAQUÍN RAMIRO GARCETE TORRES
SECRETARIO DE LA FACULTAD

MIRYAM PEÑA CANDIA
DECANA