

Universidad Estatal a Distancia  
Vicerrectoría de Planificación  
Centro de Planificación y Programación Institucional  
**Unidad De Procesos, Programación y Estructura**

Manual de Procedimientos  
para la Seguridad de Tecnologías de  
Información y Comunicaciones de la  
Universidad Estatal a Distancia

Aprobado por el Consejo de Rectoría en sesión No. 1950-2017, Artículo V, inciso 3),  
celebrada el 26 de junio del 2017.

**2017**

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Tabla de contenido

Aprobación .....	6
Elaboración y Revisión .....	8
Introducción .....	9
Marco Normativo .....	10
Lineamientos(Directrices) para el mantenimiento de Software e Infraestructura ..	13
Objetivo del Manual .....	15
Alcance del Manual.....	15
Servicios de TI institucionales para la gestión y apoyo a la administración .....	16
Clasificación de recursos de TI .....	18
Clasificación de la Información.....	20
Normas de Aplicación .....	22
Monitoreopreventivo y solicitud de estudios necesarios sobre el uso de la red institucional, equipos tecnológicos y las aplicaciones.....	22
Monitoreo y Diagnóstico Preventivo .....	22
Estudios Necesarios .....	23
En cuanto a la configuración base para los equipos de cómputo institucional .....	24
Perfil de Usuario .....	25
Perfil de Software.....	25
Perfil de Hardware.....	27
Nivel de acceso .....	28
Configuración Base .....	29
Usuario Estándar .....	29
Configuración base para el Perfil de Usuario de los Laboratorios: .....	29
Configuración base para el Perfil de Encargados de Cátedra/Programa .....	29
Configuración base para el Perfil de Personal Administrativo.....	29

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Configuración base para el Perfil de Investigador.....	29
Configuración base para el Perfil de Personal de TI.....	29
Configuración base para el Perfil de Diseñador Gráfico.....	30
Configuración base para el Perfil de Centro Universitario.....	30
Perfil de Autoridades Universitarias.....	30
En cuanto al Estándar de Nombres de Servidor .....	30
Localización.....	31
Numeración decimal asociada Centros de Datos y Centros Alternos de la UNED	31
Sistema Operativo del Servidor .....	31
Infraestructura del Servidor (tipo de servidor) .....	33
Servicios.....	33
Rol .....	33
Secuencia.....	34
Ejemplo del Estándar de Nombres de Servidores UNED.....	34
En cuanto al Estándar de Nombres de dispositivos Tecnológicos.....	34
Nombre de equipo: .....	34
Localización.....	35
Tipo de Dispositivo Tecnológico .....	35
Nombre de la dependencia.....	35
Número de Activo Institucional.....	36
Ejemplo del Estándar de Nombres para Dispositivos Tecnológicos UNED.....	36
En cuanto al estándar de nombres de usuario de la UNED .....	36
Nombre de usuario .....	36
Convenio de nombres.....	37
Manejo colisiones.....	38
Convenio de nombres de usuario para la UNED .....	38
Nombres de usuario para funcionarios del Directorio activo y Correo electrónico .....	38

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Nombres de usuario para Sistema Institucionales en el iSeries (AS400).....	39
Nombres de usuario para estudiantes (Directorio activo y correo electrónico) .....	40
Nombres de usuario para acceso remoto (VPN) para personal externo a la UNED .....	41
Nombres de usuario para la Unidad de Soporte Técnico.....	41
Nombres de usuarios de la Unidad de Infraestructura Tecnológica .....	42
Nombres de usuario de Aplicaciones.....	42
Nombres de usuario para Servicios de Software (Servidores).....	42
En cuanto a los derechos y deberes en el uso de equipo e internet en la UNED .....	43
Deberes de la DTIC.....	43
Deberes de los funcionarios .....	43
Deberes de los demás usuarios.....	43
Prohibiciones de los funcionarios y de los demás usuarios .....	44
Administración de Contraseñas de Usuario.....	46
Administración de Contraseñas Críticas .....	47
En cuanto al uso de contraseñas .....	48
En cuanto a las Regulaciones sobre el almacenamiento, transmisión y difusión de la información .....	49
Custodia de Medios Magnéticos de Respaldo e información de carácter institucional.....	49
En cuanto a la Notificación y Respuesta a Incidentes de Seguridad Informática.....	51
Detección de un Incidente.....	51
Incidentes de Seguridad .....	51
Dimensión de los daños .....	52
Se mide con base en el impacto del evento: .....	52
Criticidad de los recursos involucrados:.....	52

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Se mide con base en la prioridad e importancia del recurso en la universidad. La escala de que se maneja para establecer la prioridad o importancia es la siguiente:..... 52

Estado del Incidente..... 53

En cuanto al Equipo de Respuesta a Incidentes de Seguridad Informática ..... 53

En cuanto a la documentación del incidente ..... 53

En cuanto a la Autorización de Funcionarios para las labores de soporte y mantenimiento de los equipos y dispositivos..... 54

En cuanto a la instalación y configuración de hardware, software y dispositivos de red ..... 55

En cuanto a la implementación y administración del programa de antivirus ..... 57

Del Uso de Internet y Servicios en Línea..... 58

En cuanto a la autorización de acceso ..... 58

Sitios web ..... 58

Red institucional..... 58

En cuanto al Correo Electrónico Institucional ..... 59

Conceptos..... 61

Nombres y Abreviaturas ..... 69

Actores y Responsabilidades..... 70

Matriz Descriptiva de los Procedimientos ..... 71

Matriz Resumida de Procedimientos y sus Objetivos..... 72

Diagrama o Mapa del Procedimiento ..... 73

Administración, Control y Evaluación ..... 74

Información ..... 74

Comunicación ..... 75

Coordinación..... 75

Controles ..... 75

Control Antes ..... 75

Control Durante ..... 75

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Control Después.....	75
Parámetros de Seguimiento, Actualización, Rediseño o Anulación del Manual.....	77
Anexos:.....	78
Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros .....	79
Directriz sobre el Uso de Redes Privadas Virtuales (VPN) UNED.....	84
Disposiciones de la Ley de Control Interno en cuanto a la Identificación y Valoración de Riesgos de TI.....	90
Responsabilidades de las áreas usuarias de la DTIC.....	93
Instr-01 -MEGA-PEGTI.03-PR-06 -Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia del Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia.....	102

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Aprobación

En relación a la solicitud planteada por el señor Vicerrector de Planificación el Dr. Edgar Castro Monge de realizar el levantamiento de los todos los procesos de la universidad en concordancia al proyecto de la Propuesta del Macroproceso Institucional, se trabaja en la elaboración del presente ***Manual de Procedimientos de Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia***, en coordinación con el Centro de Planificación y Programación Institucional y representantes de las dependencias involucradas en cada uno de ellos.

<b>Pre-aprobación</b>	Juan Carlos Parreaguirre, Jefe del Centro de Planificación y Programación Institucional
<b>Aprobación final</b>	Consejo de Rectoría

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



**PARA:** Mag. Juan Carlos Parreaguirre, Jefe Centro de Planificación y Programación Institucional  
Mag. Francisco Durán, Director Tecnología, Información y Comunicaciones

**DE:** *Theodosia Mena Valverde*  
**CONSEJO DE RECTORIA**

**FECHA:** 28 de junio de 2017  
**REF.:** CR.2017.635

Les transcribo el acuerdo tomado por el Consejo de Rectoría, en sesión No. 1950-2017, Artículo V, inciso 3), celebrada el 26 de junio del 2017.

Se conoce nota CPPI.048.2017 (REF.1070.17) con fecha 20 de junio del 2017, suscrita por la Mag. Juan Carlos Parreaguirre, Jefe Centro de Planificación y Programación Institucional en relación con la entrega del Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia y del Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia; trabajo colaborativo, liderado por el Centro de Planificación y Programación Institucional con el apoyo de la Dirección de Tecnologías de Información y Comunicación, en busca el ordenamiento institucional.

**SE ACUERDA:**

1. Aprobar el Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia.
2. Aprobar el Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia.

Theo\*\* acuerdo 635\*28.06.2017

C: Ana Ivelth Rojas, CPPI / Gretel Schonwandt, CPPI  
Vicerrectoría de Planificación  
Archivo

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Elaboración y Revisión

El Centro de Planificación y Programación Institucional, CPPI mediante su Unidad de Programación y Procesos de conformidad con lo establecido en el Manual Organizacional UNED-2012, sobre la función: *“Coadyuvar en la formulación de los procedimientos de trabajo de las unidades administrativas, académicas y técnicas que componen la UNED, para alcanzar, de manera eficiente, los objetivos que les corresponde dentro de la actividad institucional”*.

En este sentido, se brinda el acompañamiento para la elaboración de los manuales de procedimientos que se soliciten o que se consideren necesarios para la optimización de los recursos institucionales y/o el ordenamiento de la gestión, desde los procesos del Macroproceso Institucional.

Para la elaboración del presente ***Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones de la Universidad Estatal a Distancia***, se brindó asesoría mediante sesiones de trabajo conjunto, con el funcionario de la DTIC: Johnny Saborío Álvarez, coordinador de la Unidad de Seguridad Digital; y se realizaron las consultas pertinentes y la participación de los siguientes funcionarios:

- Alejandro Sánchez Rivera, **Coordinador de la Unidad Soporte Técnico**
- Esteban Artavia Herrera, **Funcionario de la Unidad de Infraestructura Tecnológica**
- Francisco Duran Montoya, **Director de la Dirección de Tecnología, Información y Comunicaciones**
- Jose Pablo Chávez Sanchez, **Coordinador de la Unidad de Sistemas de Información**
- Rolando Rojas Coto, **Coordinador de la Unidad de Infraestructura Tecnológica**

La coordinación y asesoría estuvo a cargo de las firmantes.

Grettel Schonwandt Alvarado  
**Centro de Planificación y Programación Institucional**

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Introducción

El presente *Manual de Procedimientos de Seguridad Informática del Proceso de Tecnología, Información y Comunicación de la Universidad Estatal a Distancia* establece de forma clara y articulada de los procedimientos de Seguridad Informática de la universidad, los actores y sus responsabilidades y detalla las actividades de cada procedimiento a seguir para el alcance de un objetivo.

Como parte del objetivo de la herramienta presente y acorde a la normativa general y la específica, se pretende dar a conocer a la comunidad universitaria la secuencia lógica y articula para los tramites que se realizan a nivel financiero; mediante la descripción específica de cada actividad en los procedimientos y la asignación de responsabilidades, a modo de garantizar la transparencia de los procedimientos y el estableciendo de medidas que permitan el aprovechamiento de los recursos institucionales.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Marco <sup>1</sup>Normativo

Como resultado de la recopilación de leyes, normativa interna, acuerdos, pronunciamientos, contratos, resoluciones y directrices; entre otras, y en cumplimiento a la norma N° 1.7 del documento “Normas Técnicas para la Gestión y el Control de las Tecnologías de Información” (N-2-2007-CO-DFOE) aprobadas mediante Resolución del Despacho de la Contralora General de la República, N° R-CO- 26-2007 del 7 de junio del 2007.

Por tanto, se elabora este Marco Jurídico en Tecnologías de la Información y las Comunicaciones de la UNED, aprobada por la Comisión Estratégica de Tecnología de Información y Comunicaciones (CETIC-UNED) en sesión No.012-2016, celebrada el 30 de enero del 2017. Estatuto de Personal, aprobado por el Consejo Universitario en Sesión N° 464, Artículo VI, acuerdo N° 549 de 29 de noviembre de 1983). Se incluye las últimas modificaciones aprobadas por el Consejo Universitario en sesión 2416, Art. II, Inciso 1-A de 9 de abril del 2015, a ser utilizado para la gestión y gobernabilidad de las Tecnologías de la Información y la Comunicación (TIC) de la Universidad Estatal a Distancia (UNED).

- Estatuto Orgánico, analizado y aprobado por la Asamblea Universitaria en su sesión N° 058-2000 del 30 de mayo del 2000, publicado en la Gaceta N° 201 el viernes 20 de octubre del 2000. Incluye la última reforma realizada por la Asamblea Universitaria en sesión ordinaria N° 089-2013, celebrada el 25 de octubre del 2013, publicada en el diario oficial La Gaceta N° 249 del 26 de diciembre del 2013.
- Ley N° 6683 de Derechos de Autor y Derechos Conexos, publicada en la Gaceta N° 212 del 04 de noviembre del 1982.
- Ley N° 7202 del Sistema Nacional De Archivos, publicada en la Gaceta N° 225 del 27 de noviembre del 1990.

<sup>1</sup> Acuerdo CETIC.2017.006 tomado por la Comisión Estratégica de Tecnologías de Información y Comunicaciones, en sesión No.012-2016, Artículo IV, inciso 2) celebrada el 30 de enero del 2017.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Ley N<sup>ª</sup> 7600 de Igualdad de Oportunidades para las Personas con Discapacidad, publicada en la Gaceta N<sup>º</sup> 102, del 29 de mayo de 1996.
- Ley N<sup>ª</sup> 8292 General de Control Interno, publicada en la Gaceta N<sup>º</sup> 169, del 04 de setiembre del 2002.
- Ley N<sup>ª</sup> 8422 Contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública, publicada en la Gaceta N<sup>º</sup> 212 del 29 de octubre del 2004.
- Ley N<sup>ª</sup> 8454 de Certificados, Firmas y Documentos Electrónicos, publicada en la Gaceta N<sup>º</sup> 197, del 13 de octubre del 2005.
- Ley N<sup>ª</sup> 8642 General de Telecomunicaciones, publicada en la Gaceta N<sup>º</sup> 125, del 30 de junio del 2008.
- Ley N<sup>ª</sup> 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, publicada en la Gaceta N<sup>º</sup> 170, del 05 de setiembre del 2011.
- Ley N<sup>ª</sup> 9048 de Delitos Informáticos y Conexos, publicada en la Gaceta N<sup>º</sup> 214 del 06 de noviembre del 2012.
- Normas del Control Interno en el Sector Publico (N-2-2009-CO-DFOE), publicado en la Gaceta N<sup>º</sup> 26 del 06 de febrero del 2009.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, N-2-2007-CO-DFOE, publicado en la Gaceta N<sup>º</sup> 119 del 21 de junio del 2007.
- Políticas para el Uso y Desarrollo de Tecnologías de la Información y la Comunicación de la UNED, aprobadas por el Consejo Universitario, sesión N<sup>ª</sup> 2401-2015, Artículo III, inciso 1-a), del 05 de febrero del 2015.
- Reforma al Reglamento a la Ley N<sup>º</sup> 7494 de Contratación Administrativa, publicado en la Gaceta N<sup>º</sup> 93, del 16 de mayo del 2007, Decreto N<sup>º</sup> 33758-H.
- Reglamento a la Ley N<sup>º</sup> 6683 de Derechos de Autor y Derechos Conexos, publicado en la Gaceta N<sup>º</sup> 201, del 24 de octubre del 1995, Decreto N<sup>º</sup> 24611-J.
- Reglamento a la Ley N<sup>º</sup> 7202 del Sistema Nacional De Archivos, publicado en la Gaceta N<sup>º</sup> 47, del 7 de marzo del 1995, Decreto N<sup>º</sup> 24023-C.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Reglamento a la Ley N° 7494 de Contratación Administrativa, publicada en la Gaceta N° 210, del 02 de noviembre de 2006, Decreto N° 33411-H.
- Reglamento a la Ley N° 7600 de Igualdad de Oportunidades para las Personas con Discapacidad, publicado en la Gaceta N° 75, del 20 de abril del 1998, Decreto N° 26831-MP.
- Reglamento a la Ley N° 8422 Contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública. Publicado en la Gaceta N° 82, del 09 de abril del 2005, Decreto N° 32333-MP-J.
- Reglamento a la Ley N° 8454 de Certificados, Firmas y Documentos Electrónicos, publicado en la Gaceta N° 77, del 21 de abril del 2006, Decreto N° 33018.
- Reglamento a la Ley N° 8642 General de Telecomunicaciones, publicado en la Gaceta N° 186, del 26 de setiembre del 2008, Decreto N° 34765-MINAET.
- Reglamento a la Ley N° 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, publicado en la Gaceta N° 45, del 05 de marzo del 2013, Decreto N° 37554-JP.
- Reglamento General Estudiantil, aprobado por el Consejo Universitario en sesión N° 2145, Art. IV, I. -a) del 15 de marzo del 2012. Acuerdo analizado posteriormente en sesión N° 2151, Art. V, inciso 4) de 12 de abril del 2012.
- Reglamento para la Utilización del Sistema de Compras Gubernamentales CompraRED, publicado en la Gaceta N° 204, del 24 de noviembre del 2005, Decreto N° 32717-h.
- Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, aprobado por el Consejo Universitario en sesión N° 2336, Art. II, inciso 2-a) de 15 de mayo del 2014.
- Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, aprobado por el Consejo Universitario en sesión N° 2336, Art. II, inciso 2-a) de 15 de mayo del 2014.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Lineamientos(Directrices) para el mantenimiento de Software e Infraestructura

- Acuerdo para deshabilitar el Servicio de CHAT de manera generalizada, aprobado por el Consejo de Rectoría, en sesión N° 1253-2002, Art. V, celebrada el 26 de agosto del 2002.
- Acuerdo de Políticas para el Uso y Seguridad de internet, aprobado por el Consejo Universitario, en sesión 1604-2002, Art. VIII, inciso 2), celebrada el 24 de octubre del 2002.
- Acoger las iniciativas propuestas por la Administración en el Proyecto para el Fortalecimiento del Modelo de Educación a Distancia e Innovación de la Oferta Académica, basada en Tecnología de la Información y la Comunicación (TIC), y se ratifican los componentes de Desarrollo Profesional, Desarrollo Académico-Tecnológico e Información Institucional, incluidos en este proyecto, aprobado por el Consejo Universitario, en sesión 2092-2011, Artículo III, inciso 4), del 04 de mayo del 2011.
- Actualización de las Orientaciones Generales para la Implementación y Funcionamiento del Sistema de Valoración de Riesgo Institucional (SEVRI) en la UNED, aprobado por el Consejo de Rectoría, en sesión N° 1833-2014, Artículo V, celebrada el 22 de setiembre de 2014.
- Estructura de Riesgos UNED, Anexo N° 2 de las Orientaciones Generales para la Implementación y Funcionamiento del Sistema de Valoración de Riesgo Institucional (SEVRI) en la UNED, aprobado por el Consejo de Rectoría, en sesión N° 1833-2014, Artículo V, celebrada el 22 de setiembre de 2014.
- Políticas para el Uso y Desarrollo de Tecnologías de la Información Y la Comunicación de la UNED, aprobadas por el Consejo Universitario, sesión Nª 2401-2015, Artículo III, inciso 1-a), del 05 de Febrero del 2015.
- Lineamientos de Política Institucional 2015-2019 aprobados por la Asamblea Universitaria Representativa, aprobados en sesión N° 094-2019, artículo I, celebrada el 20 de febrero del 2015.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Acuerdo de creación de la Comisión Estratégica de Tecnología de Información y Comunicaciones (CETIC)-UNED y sus funciones, aprobado por el Consejo Universitario, en sesión 2406-2015, Art. II, inciso 1-a) celebrada el 26 de febrero del 2015.
- Acuerdo de funciones específicas de cada miembro de la Comisión Estratégica de Tecnología de Información y Comunicaciones (CETIC)-UNED, aprobado en sesión 2433-2015, celebrada el 04 de junio del 2015.
- Orientaciones y metodología para la autoevaluación del sistema de control interno de la UNED, aprobado por el Consejo de Rectoría, en sesión N° 1857-2015, Artículo IV, inciso 2), celebrada el 13 de abril de 2015.
- Plan de Desarrollo de Tecnologías de Información y Comunicación 2015-2019 (PDTIC) fue aprobado por el Consejo de Rectoría, en sesión extraordinaria N° 1860-2015, Artículo I, celebrada el 29 de abril de 2015.
- Prioridades Institucionales en Tecnologías de la Información y la Comunicación (TIC), que deberá atender la Dirección de Tecnologías de Información y Comunicación (DTIC), aprobado Consejo de Rectoría, en sesión N° 1896-2016, Artículo VI, celebrada el 29 de febrero del 2016.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Objetivo del Manual

El objetivo de este documento es establecer los procedimientos de seguridad de la UNED, con el fin de regular la gestión de la seguridad de la información al interior de la universidad.

## Alcance del Manual

Los procedimientos de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los estudiantes, funcionarios y terceros que laboren o tengan relación con la UNED, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Es de aplicación para toda la comunidad universitaria: funcionarios, docentes, no docentes, estudiantes y toda otra persona que de alguna manera esté relacionada con la UNED. En particular, debe ser conocida y cumplida por todos los funcionarios de planta de la UNED, terceros que visiten la universidad, técnicos contratados y proveedores; con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la Universidad Estatal a Distancia, en adelante UNED.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Servicios de TI institucionales para la gestión y apoyo a la administración

Para efectos de este documento se tomó como insumo los servicios descritos en el Plan de Contingencias de TI, los cuales consolidan los diferentes sistemas que brindan servicios a la Institución y los catalogan de acuerdo al tipo de usuario y de transacción. El cuadro # 1 tiene el listado de los sistemas y sus respectivas clasificaciones.

**Cuadro # 1. <sup>2</sup>Servicios de TI institucionales**

Servicio Académico	Tipo de Servicio
<b>Información y comunicación</b>	
Correo electrónico estudiantil	Servicio Académico
Portal de Recursos (Audiovisuales, Mediateca, Repositorio, Videoconferencias)	Servicio Académico
Sistema de Bibliotecas	Servicio Académico
Portal Institucional	Servicio Académico
Portal Investiga	Servicio Académico
Portal de Revistas UNED	Servicio Académico
Mensajería de Texto	Servicio Académico
Correo masivo estudiantes	Servicio Académico
<b>Transacción interna</b>	
Gestiona	Servicio Académico
LMS – Moodle	Servicio Académico
PAAD – Apoyo Didáctica a Distancia	Servicio Académico
PAL – Apertura de cursos	Servicio Académico
PAL – Consultas	Servicio Académico
PAL – Inscripción	Servicio Académico
SAE – Admisión y Matrícula	Servicio Académico
SAE – Asignación de tiempos	Servicio Académico
SAE – Notas parciales	Servicio Académico
SAE – Pase MEP	Servicio Académico
SAE – Planes de estudio	Servicio Académico
SAIE – Apelaciones	Servicio Académico

<sup>2</sup> Acuerdo CR.2016.124 tomado por el Consejo de Rectoría, en sesión No. 1896-2016, Artículo VI, celebrada el 29 de febrero del 2016.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

<b>Servicio Académico</b>	<b>Tipo de Servicio</b>
<b>Información y comunicación</b>	
SARCIE – Trasiego de instrumentos	Servicio Académico
SIBEC – Sistema de becas	Servicio Académico
SISGRA – Sistema de graduaciones	Servicio Académico
SCAM – Sistema de carreras, asignaturas y materiales.	Servicio Académico
<b>Transacción Externa Estudiante</b>	
SAE – Matriweb	Servicio Académico
SAE – Admisión y Empadronamiento	Servicio Académico
SAE – Reconocimientos	Servicio Académico
Entorno de Estudiantes	Servicio Académico
Encuestas en línea	Servicio Académico
<b>Transacción externa público</b>	
Eventos	Servicio Académico
<b>Servicio administrativo</b>	
<b>Información y comunicación</b>	
Telefonía IP	Servicio administrativo
<b>Transacción interna</b>	
AS – 400 – Activos fijos	Servicio administrativo
AS – 400 – Adelanto y liquidación de viáticos	Servicio administrativo
AS – 400 – Contabilidad general	Servicio administrativo
AS – 400 – Contratación y suministros	Servicio administrativo
AS – 400 – Control de presupuesto	Servicio administrativo
AS – 400 – Cuentas por cobrar	Servicio administrativo
AS – 400 – Cuentas por pagar	Servicio administrativo
AS – 400 – Devoluciones a estudiantes	Servicio administrativo
AS – 400 – Honorarios	Servicio administrativo
AS – 400 – Ingresos	Servicio administrativo
AS – 400 – Inventario y facturación	Servicio administrativo
AS – 400 – Liquidaciones	Servicio administrativo
AS – 400 – Movimientos bancarios	Servicio administrativo
AS – 400 – Planillas	Servicio administrativo
AS – 400 – Presupuesto	Servicio administrativo
AS – 400 – Relación de puestos	Servicio administrativo
AS – 400 – Servicio al personal	Servicio administrativo
Carrera profesional	Servicio administrativo

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Servicio Académico	Tipo de Servicio
<b>Información y comunicación</b>	
Entorno de funcionarios	Servicio administrativo
Facturación de librerías	Servicio administrativo
Librería virtual	Servicio administrativo
SGDP – Gestión y desarrollo de personal	Servicio administrativo
SGDP – Personal	Servicio administrativo
SGDP – Puestos y Plazas	Servicio administrativo
SGDP – Reclutamiento	Servicio administrativo
Sistema Servicios Médicos	Servicio administrativo

Fuente: Plan de contingencias, acuerdo tomado por la Comisión Estratégica de Tecnologías de Información y Comunicación, en sesión No.007-2016, Art. I, celebrada el 25 de enero del 2016

## Clasificación de recursos de TI

Los recursos de TI que cuenta la Universidad Estatal a Distancia son los siguientes:

1. **Aplicaciones:** son las que incluyen tanto sistemas de información automatizados como procedimientos manuales que procesan información.
2. **Información:** son los datos de la UNED en todas sus formas, tanto de entrada como salida, procesados y generados por los sistemas de información.
3. **Infraestructura:** es la tecnología (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, entre otros,) que permiten el procesamiento de las aplicaciones.
4. **Instalaciones:** son los espacios físicos (Oficinas, Cuartos de Comunicaciones, Centros de Datos) donde se sitúa la infraestructura tecnológica de la universidad y el ambiente que los soporta.
5. **Recurso humano (personas):** personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información de la UNED. Estas pueden ser internas, externas, por outsourcing o contratadas, de acuerdo a la necesidad de la universidad.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

<b>Clasificación de Recursos de TI</b>	
<b>Nombre</b>	<b>Tipificación</b>
Aplicaciones	Sistema Financiero Contable
	Sistema de Matricula
	Sistema de Transportes
	Procedimientos Manuales
	Otros
Información(datos)	Archivos
	Base de datos
	Cintas de Respaldo
	Documentos
	Manuales
	Otros
Infraestructura	Hardware
	Redes
	Sistemas de administración de base de datos
	Sistemas Operativos
	Otros
Instalaciones	Centro de Datos
	Cuarto de Comunicación
	Oficinas (dependencias)
	Otros
Recurso Humano	Administrador de Base de Datos
	Analistas
	Auditor de TI
	Líder de Proyectos
	Personal de Infraestructura
	Personal de Seguridad Informática
	Personal de Soporte Técnico
	Proveedores de TI
	Director de TI
	Otros

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Clasificación de la Información

La información se puede clasificar en términos de su valor, requerimientos legales, sensibilidad, y criticidad para la UNED.

Tipo de información institucional:

- **Información Confidencial:** Se trata de información sensible para la universidad, además, es una información que la ley no permite divulgar ya que puede afectar la intimidad personal, la imagen de la institución, la seguridad nacional, o simplemente es excluida por la ley. Su divulgación puede traer posibles conflictos legales que pudieran ocasionar eventuales perjuicios económicos y de otra naturaleza a la universidad.
- **Información Pública:** cualquier tipo de información que se puede compartir tanto fuera como dentro de la UNED. Su divulgación no traería conflictos legales ni de otra naturaleza para la institución.

Valor de la información institucional:

- **Información clave:** es la información cuya pérdida perjudicaría la continuidad de un proceso, actividad, servicio o proyecto de la universidad.
- **Información no vital:** es el tipo de información en que su no disponibilidad no afectaría las actividades, procesos, servicios o proyectos de la universidad.

Clasificación de la Información	
Nombre	Tipificación
Información Confidencial	Expediente físico del estudiante
	Los instrumentos y estrategias de evaluación y sus resultados.
	Información médica de los Funcionarios
	Informes preliminares de Auditoría Interna
	Investigaciones de Auditoría Interna
	Información de carácter personal de los Funcionarios y de los estudiantes
	Base de datos de la universidad
	Notas de estudiantes universitarios
	Otros
Información Publica	Acuerdos de Asamblea Representativa
	Acuerdos de Consejo Universitario
	Acuerdos de Consejo de Rectoría

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

<b>Clasificación de la Información</b>	
<b>Nombre</b>	<b>Tipificación</b>
	Normativa Universitaria
	Información de Carreras
	Información Científica
	Informes finales de Auditoría Interna

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Normas de Aplicación

### Monitoreo<sup>3</sup> preventivo y solicitud de estudios necesarios sobre el uso de la red institucional, equipos tecnológicos y las aplicaciones

La Dirección de Tecnología Información y Comunicaciones tiene entre sus atribuciones y deberes realizar de oficio, monitoreos preventivos y estudios necesarios por solicitud de las jefaturas o instancias competentes, cuando se cuente con elementos de juicio sobre la existencia de anomalías contrarias a este reglamento, con el fin de presentar las denuncias correspondientes o las acciones correctivas que procedan. Por tanto, deben realizar lo siguiente:

#### Monitoreo y Diagnóstico Preventivo

1. Para el caso de la red institucional se utilizará el FortiAnalyzer institucional o cualquier otro dispositivo que la DTIC considere necesario.
2. Para el caso de Dispositivos tecnológicos y aplicaciones se utilizará el firewall institucional o cualquier otro dispositivo (System Center, KALI Linux, entre otros) que la DTIC considere necesario.
3. El monitoreo y el diagnóstico se realizará cada tres meses seleccionando una o varias dependencias de la universidad.
4. Para el caso del monitoreo y diagnóstico de la red institucional se va contar con los siguientes reportes:
  - a. Uso de ancho de banda y aplicaciones
  - b. Uso de actividad web
  - c. Amenazas informáticas
5. El monitoreo y diagnóstico va tener la duración de 15 días y producto del mismo se realizará un análisis de los datos que este genere.
6. Se entregará un informe a la DTIC, la Oficina de Recursos Humanos y la jefatura correspondiente en caso de encontrarse alguna anomalía contraria al Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, con el fin de que presenten las denuncias correspondientes o las acciones correctivas que procedan

<sup>3</sup> De conformidad con lo establecido en el artículo cinco, en el inciso b, del Reglamento para uso de equipos de cómputo e internet de la Universidad Estatal a Distancia, 2014.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Estudios Necesarios

1. Se debe entregar a la DTIC por medio de correo electrónico u oficio, una solicitud de monitoreo o estudio necesario del uso de la red institucional y/o del equipo tecnológico a investigar, esta debe contener como mínimo:
  - a. El nombre del funcionario que hace la solicitud
  - b. El motivo o justificación del estudio.
  - c. El lugar donde se debe realizar.
  - d. Red institucional, Dispositivo o dispositivos tecnológicos involucrados, aplicación o aplicaciones a investigar.
  - e. Cualquier otra información que sea indispensable para poder llevar a cabo dicha actividad.
  - f. Para el caso de estudios de dispositivos tecnológicos:
    - i. Nombre del funcionario responsable del activo o del aplicativo
    - ii. Dependencia donde labora,
    - iii. Nombre del Jefe inmediato.
    - iv. Activo o nombre del dispositivo tecnológico opcional)
  - g. La solicitud debe ser lo más completa y clara posible, ya que de esto depende el tipo de software o equipo a utilizar durante el estudio.
2. Se utilizará el FortiAnalyzer institucional o cualquier otro dispositivo (System Center, KALI Linux, entre otros) que la DTIC considere necesario.
3. Se solicitará la participación y asesoramiento de la Oficina Jurídica, así como de cualquier oficina que requiera ser involucrada (Auditoría Interna, Control Interno, etc.).
4. Una vez identificado el lugar o el dispositivo tecnológico a investigar, se realizarán revisiones con el fin de recabar la mayor cantidad de información. Este estudio se va realizar inicialmente durante un mes o hasta que se considere necesario, previa coordinación con el usuario que presente la solicitud.
5. En caso de ser requerido, se coordinará una o varias visitas para revisar el dispositivo o dispositivos tecnológicos, aplicaciones, red institucional, etc., involucrados en la solicitud. Según el tipo de solicitud, en estas visitas debe estar presentes:
  - a. El funcionario o funcionarios que estén involucrados, así como sus dispositivos tecnológicos (Activo UNED).
  - b. El superior inmediato del o los funcionarios.
  - c. Un funcionario de la Oficina Jurídica, el cual levantara un acta de todo lo realizado en la visita.
  - d. Un funcionario de la DTIC, quien realizara la revisión del dispositivo tecnológico, aplicativo, entre otros, delante de las personas mencionadas anteriormente.
  - e. Como parte de la revisión del dispositivo tecnológico y según la denuncia planteada, se puede proceder a revisar:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- i. Estado físico del dispositivo
  - ii. Ubicación del dispositivo
  - iii. Usuarios con accesos al dispositivo.
  - iv. Logs
  - v. Historial de navegación web.
  - vi. Historial de archivos recientes.
  - vii. Archivos (documentos de office, cookies, temporales, etc.)
  - viii. Aplicaciones instaladas.
  - ix. Correo electrónico institucional.
  - x. Entre otros.
- f. En caso que la DTIC no cuente con las herramientas necesarias para realizar el estudio, se le informara a la instancia solicitante dicha situación.
  - g. En una segunda etapa, al igual con una solicitud planteada a la DTIC, se puede proceder a un monitoreo mensual del uso de dispositivo tecnológico o de la red institucional, esto con el fin de descartar cualquier amenaza o riesgo asociado.
6. Se entregará un informe a la DTIC, la Oficina de Recursos Humanos y la jefatura correspondiente, en caso de encontrarse anomalías contrarias al Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, se adjuntarán las evidencias correspondientes, esto con el fin que se establezcan las medidas correctivas y se aplique el régimen disciplinario correspondiente.

### **En cuanto a la <sup>4</sup>configuración base para los equipos de cómputo institucional**

Las actividades macro que se desarrollaron fueron los siguientes:

1. Identificación de los perfiles de usuario que tiene actualmente la UNED, basado en el tipo de aplicaciones que utiliza y las actividades que desarrolla.
2. Definición de una <sup>5</sup>configuración base de Hardware y software.
3. Identificación de las aplicaciones de uso institucional por perfil de funcionario, entendiéndose <sup>6</sup>como:
  - a. Perfil: la actividad que desarrolla una persona en su puesto de trabajo.

<sup>4</sup>El objetivo es dar cumplimiento al inciso d) del Artículo 5 del Reglamento Para Uso de Equipos de Cómputo e Internet de la Universidad Estatal A Distancia (UNED), el cual solicita “Establecer una configuración base que defina los derechos y deberes de los usuarios sobre los equipos de cómputo de acuerdo a sus funciones, que serán asignados bajo un código o perfil de usuario, con el fin de evitar la propagación de virus y la instalación de software no deseado por parte de los usuarios.”

<sup>5</sup> La cual contiene la lista de software que será instalada en todo equipo de cómputo con activo de la UNED.

<sup>6</sup>De esta manera se logró identificar los programas que se deben instalar en un computador dependiendo del funcionario que vaya hacer uso del mismo.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- b. De esta manera se logró identificar los programas que se deben instalar en un computador y el nivel de acceso dependiendo del funcionario que vaya hacer uso del mismo.
- c. Definición de las características de hardware tanto para computadoras de escritorio como para computadoras portátiles, definiendo dos perfiles para cada tipo de computadora.
- d. Laboratorio para definir los niveles de acceso y derechos que tienen los usuarios sobre los equipos de cómputo de acuerdo a sus funciones.
- e. Elaboración de las configuraciones base tomando como referencia:
  - Perfil de Usuario
  - Perfil de Software
  - Perfil de Hardware
  - Nivel de Acceso

### Perfil de Usuario

Los perfiles de usuario a nivel institucional se establecieron de acuerdo a:

1. Las <sup>7</sup>actividades que cumplen los funcionarios de la universidad,
2. La ubicación física que debe tener los equipos de cómputo (laboratorios y equipos de cómputo que no se encuentran físicamente en las instalaciones de la UNED)

Los perfiles de usuario son los siguientes:

1. Perfil de Usuario para Laboratorios
2. Perfil de Usuario para Encargados de Catedra/Programas
3. Perfil de Usuario para Personal Administrativo
4. Perfil de Usuario para Investigadores
5. Perfil de Usuario para Personal de TI
6. Perfil de Usuario para Diseñador Gráfico
7. Perfil de Usuario para Centros Universitarios
8. Perfil de Autoridades Universitarias

### Perfil de Software

1. El <sup>8</sup>software que se utilice en los equipos de cómputo de la Universidad deben tener licencia propietaria o GPL.

---

<sup>7</sup>Para cada uno de ellos, se efectuaron las respectivas consultas con el fin de conocer que aplicaciones utilizan y que nivel de acceso debe tener para poder desempeñar de la mejor forma sus labores cotidianas con tal de cumplir con los fines y objetivos de la UNED.

<sup>8</sup>La cual debe encontrarse al día, tal y como lo establece el Artículo 12 del Reglamento para Uso De Equipos De Cómputo E Internet. Además, cualquier software que no forme parte de los perfiles de

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 2. Los perfiles de <sup>9</sup>software a nivel institucional:

- a. **Perfil de Software para Laboratorios:** este perfil está compuesto de la configuración de software base institucional, y software que da soporte a la seguridad del equipo. Son computadoras que serán utilizadas en su mayoría por estudiantes de la UNED, y para diferentes actividades de funcionarios de la institución.
- b. **Perfil de Software para Encargados de Catedra/Programas:** esta configuración es una combinación del software base institucional más las aplicaciones de carácter administrativo y académico.
- c. **Perfil de Software para Personal Administrativo:** este perfil está compuesto de la configuración de software base institucional y los programas administrativos.
- d. **Perfil de Software para Investigadores:** este perfil está compuesto de la configuración de software base institucional, más programas para geo procesamiento, análisis y procesamiento de datos, y aplicaciones para desarrollo de software.
- e. **Perfil de Software para Personal de TI:** este perfil está compuesto de la configuración de software base institucional, más programas para desarrollo de software, así como programas de uso administrativo.
- f. **Perfil de Software para Diseñador Gráfico:** este perfil está compuesto de la configuración de software base institucional, más programas para el diseño y desarrollo de software.
- g. **Perfil de Software para Centros Universitarios:** este perfil está compuesto de la configuración de software base institucional, más programas y aplicaciones de uso administrativo y docente.

---

software aquí mencionados y que deban ser utilizados por personal de la universidad, debe ser autorizado previamente por la DTIC, tal y como lo establece el inciso C) del Artículo 7 del Reglamento antes citado.

<sup>9</sup>En caso de que exista uno o varios funcionarios que no coincidan con los perfiles antes citados, la DTIC procederá a crear un perfil nuevo, y procederá a actualizar este documento.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- h. **Perfil de Software de Autoridades Universitarias:** este perfil está compuesto de la configuración de software base institucional y los programas administrativos.

### Perfil de Hardware

1. Se realiza en los equipos de cómputo asignados a los departamentos, dependencias y usuarios de la Universidad
2. Los perfiles de hardware se deben revisar y modificados anualmente por parte de la DTIC, esto con el fin mantener actualizado la información de las características de los equipos de cómputo.

A continuación, se definen los perfiles de <sup>10</sup>hardware a nivel institucional:

1. Perfil de Hardware para computadores portátiles “PASCAL”
2. Perfil de Hardware para computadores portátiles “KELVIN”
3. Perfil de Hardware para computadores portátiles “KEPLER”
4. Perfil de Hardware para computadores portátiles MAC “CURIE”
5. Perfil de Hardware para computadores portátiles MAC “DAVINCI”
6. Perfil de Hardware para computadores escritorio “PASCAL”
7. Perfil de Hardware para computadores escritorio “KELVIN”
8. Perfil de Hardware para computadores escritorio “KEPLER”
9. Perfil de Hardware para computadores escritorio MAC “CURIE”
10. Perfil de Hardware para computadores escritorio MAC “DAVINCI”
11. Perfil de Hardware para computadores escritorio PC “DAVINCI”

---

<sup>10</sup>Para la adquisición de cualquier hardware que no esté contemplado en el respectivo perfil, debe ser solicitado a la DTIC para su correspondiente visto bueno, además, el funcionario debe cumplir con lo estipulado en el inciso k) y el inciso l) del Artículo 8 del Reglamento antes citado.

**Importante:** Se va iniciar con la aplicación del Perfil de Hardware de Gama Alta para todas las configuraciones base que se mencionan en este documento, en el momento que la UNED cuente con un plan de sustitución de equipos, se podrá realizar la asignación de un Perfil de Hardware de Gama Baja. Lo anterior obedece a que el cambio o sustitución de computadoras a nivel institucional supera los 5 años.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Nivel de acceso

1. Lo niveles de acceso de usuario que se definieron, están basados en:
  - a. Los permisos de usuario que propone Microsoft como parte de su sistema operativo, por tanto, corresponde a los derechos como usuario que tiene cada funcionario a la hora de utilizar la computadora que le asigna la UNED como activo para desempeñar sus funciones.
2. Los niveles de acceso se apegan a las buenas prácticas de seguridad informática, basándose en el principio del mínimo privilegio, así como el Reglamento para Uso de Equipos de Cómputo e Internet y las Normas técnicas para la gestión y el control de las tecnologías de información.
3. Los niveles de acceso son los siguientes:
  - a. **Nivel de Acceso de Administrador (Grupo de Usuario Administrador):** Los miembros de este grupo tienen control total del equipo y pueden asignar derechos de usuario y permisos de control de acceso a los usuarios según sea necesario. La cuenta Administrador es un miembro predeterminado de este grupo. Cuando un equipo se une a un dominio, el grupo Admins. de dominio se agrega automáticamente a este grupo. Puesto que este grupo tiene control total del equipo, es importante tener precaución al agregarle usuarios.
  - b. **Nivel de Acceso Estándar (Grupo Usuarios estándar):** Los miembros del grupo Usuarios pueden realizar las tareas más habituales, como ejecutar aplicaciones, usar impresoras locales y de red, y bloquear el equipo. Los miembros de este grupo no pueden compartir directorios ni crear impresoras locales. Los grupos Usuarios de dominio, Usuarios autenticados e Interactivo son miembros de este grupo de forma predeterminada. Por tanto, todas las cuentas de usuario que se crean en el dominio son miembros de este grupo.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Configuración Base

### Usuario Estándar

#### *Configuración base para el Perfil de Usuario de los Laboratorios:*

1. Perfil de Software
  - a. Perfil de Software para Laboratorios
2. Perfil de Hardware
  - a. Para computadores portátiles: KELVIN
  - b. Para computadores de escritorio: KELVIN
3. Nivel de Acceso: Usuario Estándar

#### *Configuración base para el Perfil de Encargados de Cátedra/Programa*

1. Perfil de Software
  - a. Perfil de Software para Encargados de Cátedra/Programa
2. Perfil de Hardware
  - a. Para computadores portátiles: PASCAL
  - b. Para computadores de escritorio: PASCAL
3. Nivel de Acceso: Usuario Estándar

#### *Configuración base para el Perfil de Personal Administrativo*

1. Perfil de Software
  - a. Perfil de Software para Personal Administrativo
2. Perfil de Hardware
  - a. Para computadores portátiles: PASCAL
  - b. Para computadores de escritorio: PASCAL
3. Nivel de Acceso: Usuario Estándar

#### *Configuración base para el Perfil de Investigador*

1. Perfil de Software
  - a. Perfil de Software para Investigadores
2. Perfil de Hardware
  - a. Para computadores portátiles: KELVIN
  - b. Para computadores de escritorio: KELVIN
3. Nivel de Acceso: Usuario Administrador

#### *Configuración base para el Perfil de Personal de TI*

1. Perfil de Software
  - a. Perfil de Software para Personal de TI
2. Perfil de Hardware
  - a. Para computadores portátiles: KEPLER
  - b. Para computadores de escritorio: KEPLER
3. Nivel de Acceso: Usuario Estándar

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. Los funcionarios de la Unidad de Infraestructura utilizarían el usuario “GS” para sus labores de Gestión del Centros de Datos y Cuartos de Comunicación. En el caso del personal de la Unidad de Soporte Técnico utilizaran el usuario “UST”, para las tareas de Soporte y Mantenimiento.

### ***Configuración base para el Perfil de Diseñador Gráfico***

1. Perfil de Software
  - a. Perfil de Software para Personal de TI
2. Perfil de Hardware
  - a. Para computadores portátiles: DAVINCI
  - b. Para computadores de escritorio MAC: DAVINCI
  - c. Para computadores de escritorio MAC: CURIE
  - d. Para computadores de escritorio PC: DAVINCI
3. Nivel de Acceso: Usuario Estándar

### ***Configuración base para el Perfil de Centro Universitario***

1. Perfil de Software
  - a. Perfil de Software para Centro Universitario
2. Perfil de Hardware
  - a. Para computadores portátiles: KELVIN
  - b. Para computadores de escritorio KELVIN
3. Nivel de Acceso: Usuario Estándar

### ***Perfil de Autoridades Universitarias***

1. Perfil de Software
  - a. Perfil de Software para Autoridades Universitarias
2. Perfil de Hardware
  - a. Para computadores portátiles: KELVIN
  - b. Para computadores de escritorio KELVIN
3. Nivel de Acceso: Usuario Administrador

### **En cuanto al Estándar de Nombres de Servidor**

La nomenclatura a utilizar contempla los siguientes elementos:

1. Localización
2. Sistema Operativo
3. Tipo de Servidor
4. Servicio
5. Rol de Servidor
6. Secuencia

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Localización

En el caso de la localización, se establece el uso de las siguientes convenciones de nombres:

Identificador	Descripción
CD	Centro de Datos
CA	Centro de Datos Alterno
CU	Centro Universitario
CC	Cuarto de Comunicaciones
CZ	Centro de Datos Windows Azure

## Numeración decimal asociada Centros de Datos y Centros Alternos de la UNED

El uso de la numeración decimal asociada a los símbolos de localización (CD, CA, CU, CC) se utilizará con el fin identificar en que ubicación de la universidad o fuera de ella se encuentra ese servidor. La convención a utilizar es la siguiente:

Ubicación	Numeración
Centro de Datos Sabanilla	CD00
Centro Alterno Cartago	CA01
Centro Alterno Liberia	CA02
Centro Alterno UCR	CA03
Centro Alterno UCR Liberia	CA04
Centro Alterno CONARE	CA05
Centro Universitario San José	CU01
Centro de Datos Windows Azure	CZ00

## Sistema Operativo del Servidor

Esta nomenclatura de nombres identifica el Sistema Operativo que tiene instalado el Servidor. La convención a emplear será la siguiente:

Sistema operativo del servidor	Convención
Windows	W
Linux	L
AS400	O
Mac	M

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

HP UX	H
-------	---

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### Infraestructura del Servidor (tipo de servidor)

La infraestructura nos indica que tipo de servidor estamos nombrando. La convención a emplear será la siguiente:

Infraestructura del Servidor	Convención
Infraestructura Física	F
Infraestructura Virtual	V

### Servicios

1. La institución brinda una gran cantidad de servicios tecnológicos, y estos residen en uno o varios equipos físicos i/o virtuales, o en una combinación de estos.
2. Estos servicios están dirigidos a estudiantes, docentes, funcionarios y público en general, o simplemente cumple una determinada función.
3. La convención a utilizar en el caso de los servicios es la siguiente:

Servicio	Convención
Servidor de Nombres	DNS
Hypervisor de Microsoft	HVI
VMware	HVM
Citrix	HXS
Workstations	WKS
Impresoras	PRT
Servidor Terminal	TES
Controladores de dominio	PDC
Servidor Web	WEB
Servidor de Correo	MLS
Servidor de SQL Server	SDB
Servidor de Mensajería SMS	SMS
Servidor de Aplicaciones	APP
Nombre de Clúster	CLN

### Rol

Se utilizan ambientes separados de Desarrollo, pruebas y Producción, donde la convención a utilizar es:

Rol	Convención
Desarrollo	D
Pruebas	T

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Producción	P
------------	---

### Secuencia

Secuencia de números de dos dígitos que se utilizara para llevar la cantidad de equipos servidor por Servicio.

Secuencia	Servicio
01	DNS
02	DNS
01	SQL
02	SQL

Ejemplo del Estándar de Nombres de Servidores UNED

Nombre de Servidor	Descripción
CD00WFHVIP01	Servidor físico del Centro Datos Sabanilla que brinda el servicio de Hypervisor
CA01WVTFSD01	Servidor virtual del Centro Datos Alterno de Cartago que brinda el servicio de Team Foundation Service
CD00WVDNST01	Servidor virtual del Centro Datos Sabanilla que brinda el servicio de Team Foundation Service

### En cuanto al Estándar de Nombres de dispositivos Tecnológicos

Las siguientes son las especificaciones necesarias para la estandarización de los nombres de dispositivos tecnológicos:

#### Nombre de equipo:

1. NetBIOS: mínimo 1 carácter y máximo 15.
2. DNS: mínimo 2 caracteres y máximo 24.

La nomenclatura a utilizar contempla los siguientes elementos:

1. Localización
2. Tipo de Dispositivo Tecnológico
3. Nombre e iniciales de las dependencias de la UNED
4. Activo Institucional

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Localización

En el caso de la localización de los dispositivos tecnológicos, se establece el uso de las siguientes convenciones de nombres:

Identificador	Descripción
SC	Sede Central
CU	Centro Universitario
EU	Fuera de la UNED

## Tipo de Dispositivo Tecnológico

Esta nomenclatura de nombres identifica el tipo de dispositivo tecnológico. La convención a emplear será la siguiente:

Tipo de Dispositivo Tecnológico	Convención
Computadora de Escritorio	E
Computadora Portátil	P
Tablet	T
Otro	O

## Nombre de la dependencia

La convención a utilizar en el caso del nombre de la dependencia donde labora el funcionario es la siguiente:

Nombre de la dependencia	Convención
Rectoría	REC
Vicerrectoría Académica	VAC
Vicerrectoría Investigación	VIN
Vicerrectoría Ejecutiva	VEJ
Vicerrectoría Planificación	VPL
Escuela de Ciencias de la Administración	ECA
Escuela de Ciencias de la Educación	ECE

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Nombre de la dependencia	Convención
Escuela de Ciencias Exactas y Naturales	ECEN
Escuela de Ciencias Sociales y Humanidades	ECSH

### Número de Activo Institucional

El número de activo es el consecutivo utilizado por la UNED para llevar el control de los bienes de la universidad. La convención a emplear será la siguiente:

Bien Institucional	Convención (Numeración)
Computadora Portátil	35220

Ejemplo del Estándar de Nombres para Dispositivos Tecnológicos UNED

Nombre de Servidor	Descripción
SCPDTIC35220	Computadora Portátil ubicada en la DTIC, Sede Central
SCEECEN12534	Computadora de Escritorio ubicada en la ECEN, Sede Central
CUEALA62881	Computadora de Escritorio ubicada en el Centro Universitario de Alajuela

### En cuanto al estándar de nombres de usuario de la UNED

Las siguientes son las especificaciones necesarias para la estandarización de los nombres de usuarios:

#### Nombre de usuario

1. Como requerimiento imprescindible, los nombres de usuario deben ser únicos, por tanto, cada funcionario, estudiante y personal externo de la institución debe tener un nombre de usuario que sea diferente y lo identifique del resto de la población de la UNED.
2. Los nombres de usuario se deben crear tomando en cuenta otros elementos para el desarrollo de la convención de nombres, por ejemplo:
  - a. Cuentas de Correo Electrónico

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- b. Usuarios para Sistemas Legados
- c. Usuarios para Aplicaciones Web
- d. Entre otros.

### **11 Convenio de nombres**

El convenio de nombres va tomar en cuenta los siguientes factores:

1. **El tamaño de la UNED:** este factor se relaciona con la cantidad de usuarios que puede soportar la convención de nombres de la universidad. En una institución pequeña, se permite que cada funcionario utilice su primer nombre como cuenta de usuario, para el caso de la UNED esta opción no es viable.
2. **La estructura de la UNED:** este factor puede tener influencia sobre el convenio de nombres más adecuado para una universidad. Para una institución con una estructura bien definida, puede ser adecuado incluir elementos de esa estructura en la convención de nombres, sin embargo, si existe mucho movimiento de personal a lo interno de la institución, esta opción deja de ser la mejor opción. Por ejemplo, se puede incluir los códigos de las dependencias como parte del nombre de usuario.
  - a. **La naturaleza de la UNED:** este factor indica que la naturaleza completa de la institución también puede significar que algunas convenciones de nombres son más apropiadas que otras. Una institución que maneja datos confidenciales puede decidirse por una convención que no indica ningún tipo de información personal que pueda vincular al funcionario con su nombre. Por ejemplo: una institución de este tipo, el nombre de usuario John Doe podría tener una cuenta de usuario: LUH3417.

He aquí algunas convenciones de nombres que otras instituciones han utilizado:

- a. Primer nombre (jorge, carlos, pedro)
- b. Primer apellido (perez, obregon, ramirez)
- c. Primera inicial del nombre, seguida del primer apellido (jperez, cobregon, pramirez)
- d. Primer apellido, seguido del código del departamento (perez029, obregon454, ramirez191, etc.)

---

<sup>11</sup>Un aspecto importante a tomar en cuenta en la convención de nombres descrita en este documento es lo siguiente: es posible que existan dos funcionarios que, de acuerdo a la convención, obtendrían el mismo nombre de usuario. Esto se conoce como una colisión.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### Manejo colisiones

1. Indistintamente del convenio de nombres que se utilice y de los factores que se seleccionen, siempre van a existir colisiones.
2. Se debe establecer las reglas para el manejo de choques de nombres. Algunos métodos de manejo de colisiones son:
  - a. Añadiendo números en secuencia al nombre de usuario en colisión (perez, perez1, perez2, etc.)
  - b. Añadiendo datos específicos (primera y segunda letra del nombre) al usuario al nombre de usuario en colisión (perez, eperez, ekperez, etc.)
  - c. Añadiendo información adicional de la organización al nombre de usuario (perez, perez029, perez454, etc.). Agregando el código del departamento.

### Convenio de nombres de usuario para la UNED

#### *Nombres de usuario para funcionarios del Directorio activo y Correo electrónico*

A continuación, se detalla el convenio de nombres para los funcionarios de la UNED.

En el caso de los usuarios creados a nivel de Active Directory, destinados para el uso del correo electrónico institucional y la validación en los diferentes dispositivos y aplicaciones de la universidad, se utilizará la siguiente nomenclatura:

Opciones	Nombre	Nombre de Usuario	Descripción
1.	Ericka Moya Hidalgo	emoya	Letra inicial del Primer Nombre + Primer Apellido.

En el caso de que se produzca una colisión, el manejo de la misma es el siguiente:

Manejo de Colisiones			
Opciones	Nombre	Nombre de Usuario	Descripción
1.	Ericka Moya Hidalgo	emoya	Colisión
	Ericka María Moya Hidalgo	emoyah	Diferenciarlo con la inicial del segundo apellido.
2.	Ericka María Moya Hidalgo	emoyah	Colisión

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Manejo de Colisiones			
Opciones	Nombre	Nombre de Usuario	Descripción
	Ericka María Moya Hidalgo	ermoyah	Diferenciarlo con la segunda letra del nombre.
3.	Ericka Moya Hidalgo	ermoyah	Colisión
	Ericka Moya Hidalgo	erimoyah	Solución: Diferenciarlo con la tercera letra del nombre.

Si existen muchas colisiones, la solución es incorporar letras de forma consecutiva del primer nombre del usuario.

#### *Nombres de usuario para Sistema Institucionales en el iSeries (AS400)*

A continuación, se detalla el convenio de nombres para los funcionarios de la UNED que hacen uso del AS400 e iSeries:

Opciones	Nombre	Nombre de Usuario	Descripción
1.	Johnny Francisco Saborío Álvarez	DTICJFSA	Iniciales de la Dependencia + iniciales del nombre

En este caso si se pueden generar colisiones y la asignación del usuario quedaría registrada y almacenada en una base de datos.

En el caso de que se produzca una colisión, el manejo de la misma es el siguiente:

Manejo de Colisiones			
Opciones	Nombre	Nombre de Usuario	Descripción
1.	Johnny Francisco Saborío Álvarez	DTICJFSA	Colisión
	Johnny Gerardo Saborío Álvarez	DTICJGSA	Solución: Diferenciarlo utilizando el segundo nombre del funcionario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Manejo de Colisiones			
Opciones	Nombre	Nombre de Usuario	Descripción
2	Johnny Gabriel Saborío Álvarez	DTICJMSA	Colisión
	Johnny Saborío Álvarez	DTICJSA	Solución: se elimina la inicial del segundo nombre
3	José Saborío Álvarez	DTICJSA	Colisión
	Jorge Saborío Álvarez	DTICJSA1	En caso de que no exista un segundo nombre, o este se repite, se agrega un consecutivo.

### *Nombres de usuario para estudiantes (Directorio activo y correo electrónico)*

A continuación se detalla el convenio de nombres para los estudiantes de la UNED, y que forman parte del dominio \*.UNED.CR.

En el caso de los usuarios creados a nivel de Active Directory, destinados para el uso del correo electrónico institucional y la validación en los diferentes dispositivos y aplicaciones de la universidad, se utilizará la siguiente nomenclatura:

Opciones	Nombre de Usuario	Descripción
1.	Ericka.Moya.Hidalgo	Primer nombre + punto + primer apellido + punto + segundo apellido

En el caso de que se produzca una colisión, el manejo de la misma es el siguiente:

Manejo de Colisiones		
Opciones	Nombre de Usuario	Descripción
1.	Ericka.Moya.Hidalgo	Colisión
	Ericka.C.Moya.Hidalgo	Solución: Diferenciarlo con la inicial del segundo nombre.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

2.	Ericka.C.Moya.Hidalgo	Colisión
	Ericka.Moya.H	Solución: Diferenciarlo con la primera inicial del segundo nombre.
3.	Ericka.C.Moya.Hidalgo	Colisión
	Ericka.Moya.H	Solución: Diferenciarlo con la primera inicial del segundo nombre.

### ***Nombres de usuario para acceso remoto (VPN) para personal externo a la UNED***

A continuación, se detalla el convenio de nombres para los usuarios que requieran un acceso VPN de la UNED que sean externos:

Opciones	Nombre	Nombre de Usuario	Descripción
1.	Empresa Babel	uext_babel	Iniciales del acceso + nombre de la empresa + consecutivo

La creación del usuario quedaría registrado y almacenado en una base de datos para llevar su control.

### ***Nombres de usuario para la Unidad de Soporte Técnico***

A continuación, se detalla el convenio de nombres para los usuarios de la unidad de Soporte Técnico (UST):

Opciones	Iniciales de unidad	Unidad	Nombre de usuario	Descripción
1.	ust_	soporte+	ust_soporte1	Iniciales de la unidad + parte del nombre de la unidad + consecutivo

La creación del usuario quedaría registrado y almacenado en una base de datos para llevar su control.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### *Nombres de usuarios de la Unidad de Infraestructura Tecnológica*

A continuación, se detalla el convenio de nombres para los usuarios de la unidad de infraestructura tecnológica (UIT):

Opciones	Iniciales de unidad	Unidad	Nombre de usuario	Descripción
1.	uit_	infraestructura+	uit_infraestructura1	Iniciales de la unidad + parte del nombre de la unidad + consecutivo

La creación del usuario quedaría registrado y almacenado en una base de datos para llevar su control.

### *Nombres de usuario de Aplicaciones*

A continuación, se detalla el convenio de nombres para los usuarios de las diferentes aplicaciones desarrolladas e implementadas en la UNED:

Opciones	Iniciales del Servidor	Nombre de la aplicación	Nombre de usuario	Descripción
1.	Sis_	nombredelaaplicacion	sis_apelaciones	Iniciales del servidor + nombre aplicación

La creación del usuario quedaría registrado y almacenado en una base de datos para llevar su control.

### *Nombres de usuario para Servicios de Software (Servidores)*

A continuación, se detalla el convenio de nombres para los diferentes servicios de Software que se utilizan en los servidores de la UNED:

Opciones	Iniciales del Servidor	Nombre de la aplicación utilizada	Nombre de usuario	Descripción
1.	Serv_	SSCM	Serv_SSCM	Iniciales del servicio + nombre de aplicación + consecutivo.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

La creación del usuario quedaría registrado y almacenado en una base de datos para llevar su control.

## En cuanto a los derechos y deberes en el uso de equipo e internet en la UNED

### Deberes de la DTIC

1. Contar con el equipo de cómputo y los dispositivos móviles necesarios para cumplir con los fines y objetivos de sus funciones.
2. Contar con información personal en los equipos de cómputo sin que se considere propiedad de la UNED y siempre y cuando no este entre las prohibiciones citadas en el Reglamento para Uso de equipos de Cómputo e Internet.
3. Asignación de un código de usuario y sus respectivas claves de acceso tanto para el equipo de cómputo como para sus aplicaciones.

### Deberes de los funcionarios

1. Es responsable de la adecuada conservación uso y acceso de los dispositivos tecnológicos que la institución le provea para el desempeño de sus labores.
2. Utilizar el equipo de cómputo y sus componentes únicamente en funciones propias de su cargo en la UNED.
3. Verificar que la información almacenada en el computador esté libre de virus y otras amenazas informáticas, para lo cual deberá velar porque el antivirus institucional esté instalado y debidamente actualizado.
4. Mantener un respaldo de la información que resida en el disco duro de la computadora que se le haya asignado para ejecutar sus labores, mediante los procedimientos o dispositivos que defina la DTIC.
5. Notificar a la DTIC cualquier anomalía en el funcionamiento de los equipos de cómputo, para que se proceda a su revisión y eventual corrección.
6. Informar oportunamente sobre la tenencia en su lugar de trabajo equipo de cómputo personal a fin de que no sea tomado en cuenta en caso de inventario de activos de la UNED.
7. Los demás que determinen otros Reglamentos o lineamientos institucionales al respecto.

### Deberes de los demás usuarios

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

1. Procurar que el equipo de cómputo de la Universidad y sus componentes se mantengan en condiciones adecuadas de limpieza en su exterior.
2. Hacer un uso adecuado y responsable de las claves de acceso al equipo de cómputo, red institucional y demás aplicaciones institucionales.
3. Utilizar en los equipos de cómputo de la Universidad únicamente software bajo licencia o autorizado previamente por la DTIC.
4. Acatar las instrucciones divulgadas por la DTIC en cuanto al uso de los distintos recursos tecnológicos.

### Prohibiciones de los funcionarios y de los demás usuarios

1. Colocar en la misma mesa donde se encuentra ubicado el equipo de cómputo, líquidos (plantas acuáticas, alcohol, aceite, etc.) y alimentos que pongan en riesgo el uso del mismo.
2. Ingerir alimentos mientras trabajan o permanecen frente a los equipos de cómputo.
3. Distribuir por vía electrónica archivos e información comercial y, en general, toda aquella ajena al quehacer de la UNED.
4. Conectar aparatos eléctricos tales como cafeteras, máquinas de escribir, microondas, celulares, ipods, radios y reproductores de música en el mismo tomacorriente donde está instalado su equipo de cómputo.
5. Colocar aparatos o extensiones eléctricas encima del equipo de cómputo.
6. Descargar y almacenar música, fotos y videos en sus diferentes formatos que no sean de uso para las funciones propias de su quehacer laboral.
7. La reproducción o grabación ilegal de software, música y películas, entre otros.
8. Hacer uso de los medios electrónicos de comunicación institucionales para acceder, enviar, conservar o reproducir material restringido.
9. Vulnerar o evadir los esquemas de protección y de seguridad de los equipos de cómputo sus componentes.
10. Compartir o reproducir el software adquirido o producido por la UNED sin previa autorización o lucrar indebidamente con el mismo.
11. Llevar actos de conductas dolosas de orden informático tales como introducir virus u otros elementos físicos o electrónicos que puedan dañar o impedir el normal funcionamiento de la red, del sistema o de equipos informáticos (hardware y software) de terceros o de la UNED.
12. Instalar hardware, software y dispositivos de red no autorizado por la DTIC, tales como protectores de pantalla, juegos y aplicaciones protegidas por la Ley de Derechos de Autor o cualquier otro software y hardware que pueda poner en riesgo la red de datos.
13. Difundir con fines maliciosos información que induzca, incite o promueva actos discriminatorios, delictivos, terroristas, denigrantes, difamatorios, coercitivos,

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

ofensivos, violentos o en general, contrarios a la ley, a la moral y las buenas costumbres o el orden público.

14. Abrir sin la autorización de la DTIC los equipos de cómputo y sus componentes.
15. Trasladar los equipos de cómputo y sus componentes hacia otras dependencias o fuera de las instalaciones de la UNED, salvo que por razones de trabajo así se requiera y se cuente con la debida autorización del jefe inmediato.
16. Suprimir, modificar, borrar o alterar los medios de identificación de los equipos, o entorpecer de cualquier otra forma los controles que para fines de inventario se establezcan.
17. Enviar, copiar o facilitar por cualquier medio, información propiedad de la UNED y que por su naturaleza no debe divulgarse a terceros ajenos a la Institución, excepto que se cuente con la debida autorización de las autoridades superiores.
18. Modificar la configuración base definida por la DTIC, así como la configuración general del equipo de cómputo.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Administración de Contraseñas de Usuario

La asignación de contraseñas se administran siguiendo los siguientes criterios:

1. Los usuarios completan y firman el respectivo<sup>12</sup>formulario de solicitud de usuarios que los compromete a mantener sus contraseñas personales en secreto y estén informados sobre la normativa interna con respecto a este tema.
2. Los usuarios deben cambiar las contraseñas iniciales que les han sido asignadas la primera vez que la utilicen.
3. Las contraseñas iniciales y provisionales, que se asignan cuando los usuarios olvidan su contraseña, se suministran por medio del sitio web de Autoservicio de Contraseñas o en forma personal con la identificación del usuario.
4. Generar contraseñas iniciales y provisionales seguras para el otorgamiento a los usuarios, estas deben cumplir con las especificaciones de complejidad definidas por la USD. Se debe evitar la participación de externos a la UNED (terceros), y el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña.
5. Almacenar las contraseñas sólo en bases de datos cifradas.
6. Promover la utilización de otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo, verificación de huellas dactilares), firma digital, verificación de firma, uso de medios de autenticación de hardware (como las tarjetas de circuito integrado o tarjetas de proximidad), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad Informática conjuntamente con el Responsable del Área Informática y el Propietario de la Información lo determine necesario (o lo justifique).
7. El Responsable de Seguridad Informática establecerá los procedimientos de manejo de contraseñas apropiados para cada sistema.
8. Los Propietarios de la Información son los responsables del proceso de asignación de contraseñas.

<sup>12</sup>El formulario puede estar acompañado de un Compromiso de Confidencialidad en el caso de personal externo a la UNED que deba realizar actividades contratadas con información institucional.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Administración de Contraseñas Críticas

1. En los diferentes ambientes de procesamiento existen <sup>13</sup>cuentas de usuarios con las cuales es posible efectuar actividades críticas como:
  - a. instalación de plataformas o sistemas,
  - b. habilitación de servicios,
  - c. actualización de software,
  - d. configuración de componentes informáticos, etc.
  
2. El Propietario de la Información, el Administrador del Servicio y el Responsable de Seguridad Informática definen los criterios y acciones necesarias, para la administración de dichas contraseñas críticas contemplando lo siguiente:
  - a. Definición de las causas que justificarán el uso de contraseñas críticas, así como el nivel de autorización requerido.
  - b. Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
  - c. Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas en un documento impreso y este será custodiado por el Director de la DTIC.
  - d. Para la utilización de las contraseñas críticas se debe:
    - a. Registrar,
    - b. Documentar las causas que determinaron su uso,
    - c. Documentar el responsable de las actividades que se efectúen con la misma.
  - e. Cada contraseña crítica se renovará una vez sea utilizada y se renovará una vez al año en caso de que no se la haya utilizado.
  - f. Registrar todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas.

---

<sup>13</sup>Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- g. La revisión del registro posterior de actividad será revisado por el Responsable de Seguridad Informática.

### En cuanto al uso de contraseñas

La conformación de contraseñas a utilizar en Ambiente Windows es la siguiente:

1. Las contraseñas establecidas, deben cumplir con los parámetros mínimos contemplados para contraseñas fuertes o de alto nivel las cuales son como mínimo:
  - a. Incluir caracteres al menos de tres de las cuatro siguientes categorías
    - Mínimo ocho caracteres de longitud.
    - Mayúsculas (de la “A” a la “Z”)
    - Minúsculas (de la “a” a la “z”)
    - Dígitos de base 10 (del 0 al 9)
    - Caracteres no alfanuméricos (por ejemplo: ! . @ \$ # % )
    - No debe contener vocales tildadas, ni eñes, ni espacios.
    - No permitir repetir los últimos 6 claves utilizados.
2. Las contraseñas deben ser cambiados en forma obligatoria cada 4 meses, forzados desde la administración de las aplicaciones, o cuando lo considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

La conformación de contraseñas a utilizar en Ambiente AS/400 es el siguiente:

1. Las contraseñas establecidas, deben cumplir con los siguientes parámetros mínimos:
  - a) Entre ocho y diez caracteres alfanuméricos de longitud.
  - b) Letras
  - c) Números.
  - d) No debe contener caracteres especiales (+-\*/@#%&).
  - e) No debe contener vocales tildadas, ni eñes, ni espacios.
  - f) No permitir repetir la última clave utilizada.
2. Las contraseñas deben ser cambiados en forma obligatoria cada 4 meses, forzados desde la administración de las aplicaciones, o cuando lo considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## En cuanto a las Regulaciones sobre el almacenamiento, transmisión y difusión de la información

1. El usuario podrá almacenar en los servidores de red de la UNED únicamente información proveniente de las bases de datos y aplicaciones institucionales.
2. En los servidores de red institucional, no se almacenarán archivos de texto, hojas electrónicas y otros, sino que será en espacios idóneos destinados al efecto.
3. La DTIC no contrala el contenido de la información que transite por la red o internet que utilice un usuario.
4. La DTIC no ejerce control sobre el contenido de los documentos electrónicos que se almacenen en las computadoras o dispositivos electrónicos de la universidad.
5. Se almacena durante un periodo de 6 meses la bitácora y sus respectivos respaldos, sobre las actividades en internet de todos los usuarios de la red, de manera confidencial y sin perjuicio de las potestades de la Auditoría Interna.
6. Las autoridades competentes (CONRE, Consejo Universitario, Auditoría Interna, Oficina Jurídica, el jefe inmediato) tendrán acceso a las bitácoras en caso de incidente y de un procedimiento administrativo.

## Custodia de Medios Magnéticos de Respaldo e información de carácter institucional

1. Los Medios Magnéticos de respaldo e información de carácter institucional que haya sido generada o procesada en los Centros de Procesamiento de Información (Centros de Datos, cuartos de comunicación, la DTIC, entre otros) de la UNED, debe ser resguardada por un tercero externo a la UNED, para ello deben cumplir con lo siguiente:
  - a. La contratación del Servicio de Custodia de Medios Magnéticos y de información institucional se encuentra a cargo de la Oficina de Contratación y Suministros con la asesoría de la DTIC.
  - b. El proveedor seleccionado debe suministrar cajas antimagnéticas para la custodia y transporte de los medios electrónicos entre la UNED y el lugar de resguardo. Dichas cajas magnéticas deben contar con las siguientes características:
    - i. Anti golpes y reducción de Fuerza G.
    - ii. Separadores moldeados al tamaño exacto de tapes, CD/DVD, Discos Duros y otros medios extraíbles.
    - iii. Sistema al vacío.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- iv. Protección contra altas y temperaturas y humedad.
- v. Garantía de por vida
- vi. A prueba de Agua.
- c. El servicio de contar con un Sistema de Trazabilidad, como mínimo con código de barras y las siguientes características:
  - i. Un Sistema de trazabilidad con RFID
  - ii. Etiqueta Imprimible RFID/Código de Barras.
  - iii. De sólo lectura.
  - iv. Programable una sola vez.
  - v. Que ayude a conocer exactamente qué elementos han sido sustraídos y, si es necesario, dónde localizarlos.
  - vi. Con lecturas rápidas y precisas (eliminando la necesidad de tener una línea de visión directa)
- d. El servicio debe brindar acceso a la información custodiada las 24 horas del día, los 7 días de la semana. Además, se deben proporcionar un sitio web para consultar el inventario de medios con las siguientes características:
  - i. Que el sitio web utilice protocolo https, utilizando una conexión bajo SSL (Secure Socket Layer).
  - ii. De ser posible, que este sitio web este alojado en un servidor dedicado únicamente para este servicio (y que el mismo no resida en un servidor en hosting)
  - iii. Suministrar un usuario para la institución, con el cual va poder gestionar los medios custodiados.
  - iv. Que el sitio web sea compatible con múltiples sistemas operativos (Windows, Mac OS, Linux, Solaris) y sea soportado por múltiples navegadores (IE, Firefox, Chrome).
- e. El servicio debe suministrar un Software para Record Management con sistemas de auditoría y sistemas de retención, con las siguientes características:
  - i. Compatibilidad con Códigos de Barras y RFID.
  - ii. Creación de campos personalizables (mínimo Título, código Alternativo, código de Barras y RFID).
  - iii. Que el sistema permite la búsqueda mediante los metadatos y campos personalizables, lectores de códigos de barras y lectores RFID.
  - iv. Auditoría sobre la actualización de datos.
  - v. Que la Auditoria de los datos tenga la capacidad de mostrar el dato actual y el dato histórico.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## En cuanto a la Notificación y Respuesta a Incidentes de Seguridad Informática

Un incidente de seguridad informática es la violación o amenaza a la política de seguridad de la información de la UNED, tal y como lo establece la Norma 1.4 “Gestión de la Seguridad de la Información”. También es considerado un incidente de seguridad un evento que compromete la confidencialidad, integridad y disponibilidad de los sistemas, servicios o red de la universidad.

### Detección de un Incidente

Un incidente puede ser denunciado por los usuarios de la institución, o indicado por un único o una serie de eventos de seguridad informática.

### Incidentes de Seguridad

Se cataloga como incidente de seguridad lo siguiente:

1. Uno o varios eventos adversos en un sistema, aplicación o servicio que pueda comprometer o compromete la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
2. Una violación o amenaza contraría a la política de seguridad de la información de la Institución, Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia y cualquier otra normativa aplicable a las TICS.

Los eventos que generan los incidentes de seguridad son:

1. Escaneo
2. Denegación de Servicios
3. Uso prohibido de un recurso informático o de red de la Universidad.
4. Uso indebido de información crítica.
5. Divulgación no autorizada de información personal.
6. Intrusión física.
7. Destrucción no autorizada de información.
8. Robo o pérdida de información.
9. Interrupción prolongada en un sistema o servicio de red.
10. Modificación, instalación o eliminación no autorizada de software.
11. Acceso o intento de acceso no autorizado a un sistema informático.
12. Ingeniería social, fraude o Phishing.
13. Modificación no autorizada de un sitio o página web de la Universidad.
14. Eliminación insegura de información.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

15. Modificación o eliminación no autorizada de datos.
16. Anomalía o vulnerabilidad técnica de software.
17. Amenaza o acoso por medio electrónico.
18. Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.)
19. Robo o pérdida de un recurso informático de la Universidad.
20. Otro no contemplado.

### Dimensión de los daños

Se mide con base en el impacto del evento:

1. Grave, la afectación puede representar:
  - Pérdidas muy significativas
  - Impide el logro de los objetivos de la UNED
  - Pérdidas económicas importantes
  - Pérdida de capacidad de brindar el servicio
  - Pérdida de información e implicaciones legales,
  - Interrupciones que producen incertidumbre acerca de cuándo se restablecerán los servicios
  - Afecta la misión o reputación de la Universidad.
  - Daños mayores a los sistemas y significativos a la propiedad
2. Moderado, la afectación puede representar:
  - Puede causar pérdidas menores.
  - Deshabilita temporal o parcialmente los sistemas.
  - Fallas que causan demoras en varias áreas, no afectan otras actividades
3. Leve, la afectación puede representar:
  - Puede causar inconvenientes o ineficiencias.
  - Pérdidas o daños muy bajos de activos o recursos tangibles que no afecta considerablemente los intereses de la Universidad.
  - No presentan perjuicio económico.

### Criticidad de los recursos involucrados:

Se mide con base en la prioridad e importancia del recurso en la universidad. La escala de que se maneja para establecer la prioridad o importancia es la siguiente:

1. **Alta:** Los servicios de prioridad alta, deben ser considerados como servicios de misión crítica por lo que no pueden detenerse y requieren un alto grado de redundancia y alta disponibilidad. Asimismo, al presentar fallos o incidentes de seguridad, deben ser atendidos inmediatamente.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

2. **Media:** Estos servicios deben tener cierto grado de redundancia y disponibilidad, deben ser considerados servicios de atención preferente. Asimismo, al presentar fallos o incidentes de seguridad informática, deben ser atendidos lo más pronto posible, siempre que no haya incidentes de misión crítica.
3. **Baja:** Estos servicios no requieren redundancia o alta disponibilidad. Asimismo, al presentar fallos o incidentes de seguridad informática, deben ser atendidos de acuerdo a la capacidad de atención, y siempre que no haya incidentes de misión crítica o de atención preferente, por lo que se pueden tratar como de mejor esfuerzo

### Estado del Incidente

El incidente puede ser categorizado de la siguiente manera:

1. **Pendiente:** El incidente ha sido reportado, pero aún no se lo ha comunicado al Equipo de Respuesta a Incidentes de Seguridad Informática.
2. **Informado:** El incidente ha sido reportado al Equipo de Respuesta a Incidentes de Seguridad Informática
3. **En curso:** El incidente ha sido reportado al Equipo de Respuesta a Incidentes de Seguridad Informática y está siendo atendido.
4. **Resuelto:** El incidente ha sido resuelto.
5. **Demorado:** La atención al incidente ha sido interrumpida por motivos de fuerza mayor.

### En cuanto al Equipo de Respuesta a Incidentes de Seguridad Informática

1. La atención al incidente de seguridad informática se realizará de acuerdo a la naturaleza o tipo de incidente que se presente por el Equipo de Respuesta a Incidentes de Seguridad Informática.
2. El Equipo de Respuesta a Incidentes de Seguridad Informática, se conforma por uno o más representantes de las siguientes unidades de la DTIC:
  - a. Unidad de Sistemas de Información.
  - b. Unidad de Infraestructura Tecnológica.
  - c. Unidad de Soporte Técnico.
  - d. Unidad de Seguridad Digital.
3. Los representantes, del Equipo de Respuesta a Incidentes, serán nombrados por el Director(a) de la DTIC.

### En cuanto a la documentación del incidente

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

1. Se documenta el Estado actual, entendido como la condición en que se encuentra el dispositivo o servicio afectado una vez suscitado el incidente.
2. Se debe realizar un Resumen, que contempla la descripción de lo sucedido.
3. Se debe registrar todas las acciones que se realizaron antes, durante y después del incidente.
4. Las Dependencias involucradas son:
  - a. Direcciones,
  - b. Oficinas y demás departamentos de la institución relacionados con el incidente.
  - c. También puede haber instancias o personas externas a la UNED involucradas con el incidente.
5. Se debe contar con un listado de evidencias, donde se reúnen las pruebas y demás elementos relacionados con el incidente.
6. En relación a los comentarios, deberán anotarse cualquier observación sobre el incidente, que no se ha registrado como parte de los puntos anteriores.
7. Se deben establecer los próximos pasos y acciones de mejora, como pautas a seguir y correcciones a realizar producto del incidente.

### **En cuanto a la Autorización de Funcionarios para las labores de soporte y mantenimiento de los equipos y dispositivos**

En cumplimiento al artículo 5, inciso K) del Reglamento para uso de equipos de cómputo e Internet, donde se le atribuye a la DTIC “Autorizar a funcionarios de otras dependencias para que realicen labores de soporte y mantenimiento de los equipos y dispositivos en coordinación y supervisión de la DTIC”.

1. El funcionario o dependencia interesada debe enviar una solicitud a la DTIC por medio de correo electrónico u oficio, solicitando la autorización.
2. En la solicitud se debe adjuntar el perfil del funcionario o funcionarios que necesitan ser autorizados para realizar labores de soporte y mantenimiento de los equipos y dispositivos. Además, se debe indicar si estos funcionarios cuentan con conocimientos en soporte y mantenimiento de dispositivos tecnológicos.
3. Algunas de las funciones que se pueden realizar son las siguientes:
  - a. Tareas básicas de soporte como: instalación de impresoras y computadoras, creación de estaciones de trabajo del AS-400, configuración de cuentas de correo en Outlook y afines.
  - b. Mantenimiento de equipos de laboratorio de cómputo.
  - c. Labores de monitoreo de equipos de comunicaciones de la red de datos y soporte previa coordinación con los funcionarios de la Unidad de Infraestructura Tecnológica

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. El Director de la DTIC en conjunto con el coordinar de la Unidad respectiva, evalúa el perfil de funcionario.
5. El Director de la DTIC envía un oficio al funcionario solicitante, aprobando o rechazando la solicitud. En caso de contar con la autorización del Director de la DTIC, se le indica lo siguiente:
  - a. Funciones autorizadas. El detalle de las funciones autorizadas es definido por el coordinador de la Unidad y el Director de la DTIC.
  - b. El nombre de la persona que va coordinar sus actividades.
  - c. El nombre de la persona con quien debe coordinar los temas de capacitación y actualización.
  - d. Debe entregar un informe trimestral de las actividades llevadas a cabo en cumplimiento de sus funciones.
6. El coordinar de cada unidad de la DTIC debe revisar de forma anual las autorizaciones de funcionarios que tenga a cargo, con el fin de velar si las condiciones se mantienen y si no existe algún cambio que pueda dejar sin efecto dicha autorización.
7. El funcionario que deje de realizar labores de soporte y mantenimiento de los equipos y dispositivos, debe coordinar previamente con la DTIC para la entrega de activos, Discos, documentación, información de usuarios y demás materiales utilizados para dicho fin. La DTIC debe coordinar con las unidades respectivas para la revisión de la información entregada, hacer los cambios de usuario y deshabilitar las cuentas de usuario que ya no se deban utilizar.

### **En cuanto a la instalación y configuración de hardware, software y dispositivos de red**

1. Se prohíbe a los funcionarios y usuarios que utilizan los diferentes medios electrónicos institucionales “Instalar hardware, software y dispositivos de red no autorizado por la DTIC, tales como protectores de pantalla, juegos y aplicaciones protegidas por la Ley de Derechos de Autor o cualquier otro software y hardware que pueda poner en riesgo la red de datos”, tal y como lo establece al inciso I) Artículo 8 Capítulo II del Reglamento para Uso De Equipos De Cómputo E Internet.
2. Cualquier hardware, software y dispositivos de red debe ser instalado y configurado por funcionarios de la DTIC o personal autorizado por esta dirección.
  - a. **En cuanto al software**

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- i. Es definido y proporcionado por la UNED, tal y como lo establece en la Configuración base para los equipos de cómputo institucional, el cual es un documento en respuesta al inciso d) Artículo 5 Capítulo II del Reglamento para Uso De Equipos De Cómputo E Internet.
- ii. El software que se utilice en los equipos de cómputo de la Universidad deben tener licencia propietaria o GPL, la cual debe encontrarse al día, tal y como lo establece el Artículo 12 del Reglamento antes citado.
- iii. Cualquier software que no forme parte de los perfiles de software mencionados en la configuración base para los equipos de cómputo institucional y que deban ser utilizados por personal de la universidad, debe ser autorizado previamente por la DTIC, tal y como lo establece el inciso C) del Artículo 7 del Reglamento antes citado.
- iv. La DTIC es quien gestiona la renovación de las licencias del software, en coordinación con la Oficina de contratación y suministros o quien corresponda.
- v. La compra de software debe contar con la aprobación de la DTIC.
- vi. Única y exclusivamente la DTIC, puede administrar, custodiar y controlar las licencias de software en la UNED.

**b. En cuanto al hardware:**

- i. La configuración de hardware que se destine para los equipos de cómputo asignados a los diferentes departamentos, dependencias y usuarios de la Universidad, serán para cumplir con los fines y objetivos de la UNED, en relación al perfil de software del funcionario responsable del activo, tal y como lo establece el Artículo 9 del Reglamento antes citado. Los perfiles de hardware deben ser revisados de forma anual por parte de la DTIC, esto con el fin mantener actualizado la información de las características de los equipos de cómputo.
- ii. Para la adquisición de cualquier hardware que no esté contemplado en el perfil de hardware establecido en la configuración base para los equipos de cómputo institucional, debe ser solicitado a la DTIC para su correspondiente visto bueno, además, el funcionario debe cumplir con lo estipulado

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

en el inciso k) y el inciso l) del Artículo 8 del Reglamento antes citado.

**c. En cuanto a dispositivos de red**

- i. La DTIC es el único órgano facultado para autorizar la conexión de dispositivos en la red institucional, por lo que queda prohibido a los usuarios conectar o interconectar otros equipos sin su autorización, tal y como lo establece el Artículo 16 del Reglamento antes citado.

**En cuanto a la implementación y administración del programa de antivirus**

1. Es competencia de la DTIC:
  - a. Implementar y administrar el programa antivirus institucional que será el único y oficial de la UNED.
  - b. Establecer una configuración base que defina los derechos y deberes de los usuarios sobre los equipos de cómputo de acuerdo a sus funciones, que serán asignados bajo un código o perfil de usuario, con el fin de evitar la propagación de virus y la instalación de software no deseado por parte de los usuarios
2. En el caso de los funcionarios deben verificar que la información almacenada en el computador esté libre de virus y otras amenazas informáticas, para lo cual deberá velar porque el antivirus institucional esté instalado y debidamente actualizado.
3. La implementación de la solución antivirus institucional estará a cargo de la Unidad de Infraestructura Tecnológica en coordinación con la Unidad de Seguridad Digital y la Unidad de Soporte, de la DTIC.
4. Se inicia en la sede central y luego los centros universitarios, hasta lograr un cien por ciento de cobertura.
5. El antivirus institucional se instala en los servidores, laboratorios de cómputo, las estaciones de trabajo de las y los funcionarios y los equipos portátiles de la UNED.
6. Cualquier instalación que se realice por parte de un funcionario(a) externo a las unidades de Operaciones, Soporte y Seguridad de la DTIC, deberá ser autorizada con antelación por los responsables de las mismas; lo anterior con el propósito de mantener un control por parte de la DTIC.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

7. En caso de anomalías o fallos relacionados con el <sup>14</sup>antivirus institucional, se deberá reportar a las unidades de Operaciones, Soporte y Seguridad de la DTIC, para que estos determinen las medidas de mejora y solución según sea el caso.
8. Para la instalación, utilización, actualización y prácticas para la detección de amenazas informáticas del antivirus institucional, la instalación del antivirus institucional se puede realizar de dos maneras:
  - a. La instalación local o en sitio, por parte de algún funcionario de la DTIC o autorizado; esta es preferible realizarla en la instalación a estaciones de trabajo de los centros universitarios y equipo portátil.
  - b. La instalación remota desde el servidor de administración, la cual es preferible para los equipos ubicados en la sede central y su periferia.

## Del Uso de Internet y Servicios en Línea

### En cuanto a la autorización de acceso

- La DTIC es quién garantiza el ancho de banda que satisfaga las necesidades institucionales de acceso a internet de la UNED
- Debe monitorear los consumos de internet para optimizar los permisos de acceso.
- La DTIC puede denegar el acceso a sitios o protocolos que, por su naturaleza:
  - ponen en riesgo la seguridad de la plataforma tecnológica,
  - conllevan a un desaprovechamiento de la tecnología o afecten el cumplimiento de las funciones y responsabilidades de los usuarios.
- La DTIC debe informar las denegaciones que realice.
- Las jefaturas, deben velar por el uso correcto de la Red institucional y solicitar a la DTIC el estudio respectivo en caso de incidentes.

### Sitios web

- El acceso a cualquier Red social está restringido a asuntos de tipo:
  - Académico
  - Estudiantil
  - Propios de la administración

### Red institucional

- Es de uso exclusivo para asuntos institucionales
- La DTIC asignará la respectiva cuenta de usuario.

<sup>14</sup> Una vez instalado en las estaciones de trabajo o máquinas portátiles.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Solo la DTIC, puede autorizar la conexión de dispositivos a la red institucional.
- Ningún usuario puede conectar o interconectar otros equipos sin autorización de la DTIC.

### En cuanto al Correo Electrónico Institucional

1. Es el medio oficial de envío y recepción de información y comunicación.
2. El funcionario debe mantener actualizado el correo electrónico institucional.
3. Por los principios de libertad de expresión, privacidad y confidencialidad de la información, no se realizan monitoreos o inspección en los buzones de correo de los usuarios.
4. La DTIC limita el tipo de archivos que pueden ser trasegados a través del correo electrónico institucional, así como el tamaño de los buzones y las capacidades de envío o recepción de información.
5. Si por razones de que el funcionario toma vacaciones, incapacidades prolongadas, renuncia, traslada o es despedido, deberá definir con el superior previamente, los datos del buzón de su correo que son de importancia para la oficina y solicitar a la DTIC el traslado de esa información.
6. Si por razones de que el funcionario toma vacaciones, incapacidades prolongadas, renuncia, traslada o es despedido, no se podrá habilitar a otro funcionario para que accedan a ese buzón, solo si se cuenta con la autorización expresa del usuario titular, casos de fuerza mayor o interés institucional.
7. Los casos de fuerza mayor o interés institucional los define la CETIC.
8. Los correos masivos son restringidos por la DTIC.
9. Las razones para restringir correos masivos son:
  - a. Técnicas: cuando existe una amenaza o riesgo de TI hacia el propio servicio, dispositivos tecnológicos y red de la institución.
  - b. Capacidad: el tamaño de los envíos es muy alto, y la capacidad de los buzones se ve comprometida.
  - c. Saturación: el envío de correos atenta contra el límite de destinatarios diarios permitido por Office 365
10. Solo se pueden enviar correos masivos en casos de interés institucional y con autorización del superior jerárquico respectivo.
11. Ante incidentes por el contenido de un correo o por daño a la herramienta por uso indebido, el responsable es el usuario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

12. La DTIC mantiene informada a la comunidad universitaria sobre los tipos de archivos que no pueden enviarse por el correo electrónico institucional, dentro los cuales se puede mencionar:
- Los tipos de archivo que se especifican más abajo, incluso si están comprimidos (en archivos .gz o .bz2, por ejemplo) o almacenados dentro de otros (.zip o .tgz, por ejemplo).
  - Los documentos que contienen macros maliciosas.
  - Los archivos cuyo contenido está protegido con una contraseña.
  - Los archivos protegidos por contraseña que contengan un archivo.
  - Tipos de archivo que no se pueden adjuntar a mensajes: .ADE, .ADP, .BAT, .CHM, .CMD, .COM, .CPL, .EXE, .HTA, .INS, .ISP, .JAR, .JS (NUEVO), .JSE, .LIB, .LNK, .MDE, .MSC, .MSI, .MSP, .MST, .NSH, .PIF, .SCR, .SCT, .SHB, .SYS, .VB, .VBE, .VBS, .VXD, .WSC, .WSF, .WSH
13. El usuario debe acatar las medidas<sup>15</sup> de seguridad, integridad, funcionalidad y calidad en el servicio que defina la DTIC.
14. La DTIC define las capacidades de almacenamiento de los buzones, incluyendo:
- Almacenamiento total de los correos (Bandeja de entrada, Bandeja de salida, Elementos enviados, Borradores y Elementos Eliminados).
  - Tamaño máximo de los correos de envío y recepción cuando contengan archivos adjuntos.
15. La capacidad óptima de los correos para el funcionamiento eficaz y eficiente, es definida por la DTIC.
16. En caso de que un usuario entorpezca el uso adecuado del correo electrónico institucional, la DTIC podrá suspenderle de manera preventiva o permanente el servicio.

<sup>15</sup> Estas medidas son dadas a conocer a la institución y a sus funcionarios mediante comunicados de correo electrónicos, videoconferencias, afiches y las herramientas administrativas como manuales, instructivos, protocolos, entre otros en temas de TIC.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Conceptos

A los efectos de una correcta interpretación del presente Manual de Seguridad de la Información, se realizan las siguientes definiciones:

- **Activos de Información:** Son los bienes relacionados a un sistema de información en cualquiera de sus etapas. Ejemplos de activos son:
  - ✓ Información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, resultados de proyectos de investigación, etc.
  - ✓ Software: Software de aplicaciones, software de sistemas, herramientas de desarrollo, etc.
  - ✓ Activos físicos: Computadoras, equipamiento de redes y comunicaciones, medios de almacenamiento, mobiliario, lugares de emplazamiento.
  - ✓ Servicios: Servicios informáticos y de comunicaciones.
- **Acceso no autorizado:** es la explotación de una vulnerabilidad en un equipo, aplicación o sistema, con el fin de poder obtener accesos y privilegios que no le corresponden.
- **Administración de Riesgos:** Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.
- **Administrador de aplicación:** funcionario responsable de la gestión de una aplicación informática.
- **Almacenamiento secundario magnético:** es una unidad de disco duro, flexible, cinta, medio óptico o de cualquier otro tipo.
- **Antivirus Institucional:** Programa o herramienta encargado de eliminar los virus a nivel institucional.
- **Aplicación:** es un programa de computadora que se utiliza como herramienta para una operación o tarea específica.
- **Aplicación:** Se refiere a un sistema informático, tanto desarrollado por la UNED como por terceros, o al sistema operativo o software de base, que integren los sistemas de información o donde estos estén alojados.
- **Archivo:** Acumulación de datos con nombre almacenados en un medio de
- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Clave de acceso o contraseña:** Secuencia de dígitos que permite el acceso a un
- **Código de usuario:** Código de acceso a la red y sistemas institucionales definido por la DTIC.
- **Código malicioso:** es código informático que provoca vulnerabilidades de seguridad para dañar un sistema o aplicación.
- **Comité de Seguridad de la Información:** El Comité de Seguridad de la Información, es un grupo interdisciplinario de profesionales en TI con funcionarios claves en la UNED, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.
- computador, servicio, sistema, programa, entre otros. Forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso informático.
- **Concientización del usuario:** El proceso de capacitación en temas específicos de la seguridad para reducir los problemas relacionados con la seguridad, ya que los usuarios generalmente constituyen el eslabón más débil en la cadena de la seguridad.
- **Confiability de la Información:** que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y objetivos institucionales.
- **Confidencialidad:** aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.
- **Configuración base equipos de cómputo institucional:** software que es necesario para el funcionamiento del computador, el cual debe ser suministrado por la institución e instalado por la instancia autorizada para estos fines. Por ejemplo, el sistema operativo, paquetería ofimática, antivirus institucional, y demás aplicaciones institucionales desarrolladas para el desempeño de las funciones de los funcionarios y funcionarias.
- **Contrato o Compromiso de confidencialidad:** aquel acuerdo entre dos partes, donde una se compromete tratar uno o varios temas de forma discrecional y se intenta evitar que las partes implicadas puedan utilizar información para sus propios fines.
- **Datos:** es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Es un valor que puede recibir un dispositivo tecnológico por diferentes medios.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- **Denegación de Servicios:** es un tipo de ataque que se realiza a un sistema, computadoras, servidores o una red en específico, que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **Disponibilidad:** aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- **DTIC:** Dirección de Tecnología, Información y Comunicaciones de la UNED.
- **Equipo de respuesta a incidentes:** grupo de funcionarios de la universidad que tiene la responsabilidad de actuar frente a cualquier incidente de seguridad informática.
- **Equipos o dispositivos tecnológicos:** Todo dispositivo tecnológico con funciones similares a un computador, como Tablet, Smartphone (teléfonos inteligentes), entre otros, que puede establecer conexión a una red de datos o Internet.
- **Escaneo:** técnica que se utiliza para obtener información de un sistema, servicio o equipo que posteriormente será utilizada para atacarlo.
- **Estudios (uso de red y equipo):** investigación que permitirá determinar posibles anomalías en contra del Reglamento de Uso de Equipo de Cómputo y acceso a Internet de la UNED, así como de las buenas prácticas de seguridad informática.
- **Evaluación de Riesgos:** Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la UNED.
- **Exportación:** es transferir datos desde un programa hacia otro.
- **Incidente de Seguridad de la Información:** se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información y Reglamento de Uso de Equipo de Cómputo y acceso a Internet de la UNED.
- **Incidente de Seguridad:** Un incidente de seguridad es un evento adverso en un sistema de Información, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.
- **Información:** es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento de la persona o sistema que recibe dicho mensaje.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- **Información:** Se refiere a 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, en papel, en pantallas de computadoras, audiovisual u otro.
- **Integridad:** garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
- **Impacto del evento:** es la escala de impacto funcional de acuerdo a la afectación de los sistemas, servicios o red de la universidad.
- **Legalidad:** referido al cumplimiento de las leyes, lineamientos, normas, acuerdos, pronunciamientos, reglamentos o disposiciones a las que está sujeta la UNED.
- **Licencia GPL:** licencia orientada principalmente a proteger la distribución, modificación y uso de software libre.
- **Licencia propietaria:** también conocidas como licencia de software de código cerrado o software privativo. En este tipo de licencia regula la cantidad de copias que pueden ser instaladas y el propietario indica que el software no puede ser modificado, desarticulado, copiado o distribuido.
- **Marco de Seguridad de la Información de la UNED:** es el marco metodológico que incluye la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
- **Marco Jurídico en Tecnologías de la Información y las Comunicaciones:** es la recopilación de leyes, normativa interna, acuerdos, pronunciamientos, contratos, resoluciones y directrices; entre otras, a ser utilizado para la gestión y gobernabilidad de las Tecnologías de la Información y la Comunicación (TIC) de la Universidad Estatal a Distancia (UNED)
- **Material restringido:** Se refiere a las listas de direcciones, sitios o archivos que por su naturaleza son contrarios a la moral, las buenas costumbres y el orden público.
- **Monitoreo:** es el proceso de recolectar, analizar y utilizar información para hacer seguimiento a un programa, computadora, funcionario o actividad determinada.
  - ✓ **Monitoreo de la Red Institucional:** es una revisión periódica del uso de la red de datos institucional, sus protocolos, tipos de aplicaciones, consumo de ancho de banda, entre otros.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- ✓ Monitoreo preventivo de dispositivos tecnológicos: es una revisión periódica que permite detectar posibles puntos de falla, amenazas y un mal uso de cualquier equipo tecnológico.
- **No repudio**: se refiere a evitar que una entidad (persona) que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Norma**: Regla de comportamiento dictada por una autoridad competente que se debe seguir o a la que se deben ajustar las conductas, tareas, actividades, etc.
- **Outsourcing**: término del inglés que podemos traducir al español como 'subcontratación', 'externalización' o 'tercerización'.
- **Perfil de usuario**: serie de características que definen los privilegios de acceso de un usuario, el cual puede ser Invitado, restringido, avanzado, administrador, entre otros.
- **Procedimiento**: Acciones que se realizan, con una serie común de pasos claramente definidos, que permiten realizar correctamente una tarea o alcanzar un objetivo. Se distinguen dos clases de procedimientos: obligatorios y recomendados. Estos últimos representan “buenas prácticas”, que son aconsejables, pero no requeridas. Si en un procedimiento no se utiliza la palabra “recomendado” se asume que es obligatorio.
- **Proceso de Información**: Conjunto de tareas relacionadas lógicamente que se realizan para lograr un resultado determinado en un Sistema de Información.
- **Programas o software base**: Conjunto de instrucciones expresadas mediante palabras, códigos, lenguajes, gráficos, diseño o en cualquier otra forma que, al ser incorporados en un dispositivo de lectura automatizada, es capaz de hacer que una computadora un aparato electrónico o similar sea capaz de ejecutar determinada tarea, elaborar informaciones u obtenga determinado resultado. También forma parte del programa su documentación técnica y sus manuales de uso.
- **Propietario de la información**: es la unidad organizacional o proceso donde se crean los activos de información.
- **Propietario de un Activo Físico**: Es el responsable patrimonial del bien.
- **Propietario de un Proceso de Información**: Es el responsable por la creación, puesta en funcionamiento y mantenimiento de un Proceso de Información.
- **Propietarios de la Información**: Son los funcionarios, unidades académicas o dependencias responsables de la generación o recopilación de la información, con competencia jurídica para administrar y disponer de su contenido.
- **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **Recurso de TI:** son elementos que permiten a las dependencias tecnológicas de la UNED hacer la entrega de servicios para que la universidad pueda cumplir con sus objetivos.
- **Registro:** Conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos, informatizada o no. A los efectos de este Manual se clasifican en:
  - ✓ **Registros Académicos:** Son los relacionados al desempeño académico de un estudiante en el marco de un programa organizado en alguna de las Unidades Organizativas de la UNED sobre los que se prevé emitir algún tipo de certificación.
  - ✓ **Registros de Funcionamiento:** Son los asociados con las actividades de soporte a las actividades principales (docencia, investigación y extensión) de la UNED.
  - ✓ **Registros Personales:** Son los relacionados con las personas físicas o jurídicas tal como se establece en la Ley de Protección de los Datos Personales.
  - ✓ **Registros de Producción:** Son los asociados a las actividades de investigación y extensión de la UNED o de alguno de sus miembros.
- **Registros de Auditoría:** son archivos donde son registrados los eventos que se han identificado en los sistemas de información, dispositivos tecnológicos y redes de datos de la universidad. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
- **Reporte de Incidentes de Seguridad de Información:** es la notificación de un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad de la Información y Reglamento de Uso de Equipo de Cómputo y acceso a Internet de la UNED.
- **Reporte del Monitoreo:** es el resultado del control y seguimiento de las actividades de la red de datos, como de los equipos tecnológicos.
- **Respaldos:** es una copia de seguridad de los datos de la UNED. Son aquellos documentos, base de datos, archivos, entre otros, que son considerados importantes para la universidad. Estos respaldos se realizan de forma periódica, si por algún

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

motivo se pierde o daña el archivo original, la DTIC puede restaurar una copia del respaldo.

- **Responsable de la Unidad de Auditoría Interna:** Auditor Interno Titular.
- **Responsable de la Unidad Organizativa:** Administrador de un Centro Universitario, Vicerrectores, Jefes o Director responsable del funcionamiento de la Unidad Organizativa.
- **Responsable de un Sistema de Información:** Encargado de velar por la puesta en marcha y el correcto funcionamiento del Sistema de Información o en su defecto el Responsable de la Unidad Organizativa.
- **Responsable por el activo de información:** es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.
- **Restaurar:** devolver al estado inicial los documentos, base de datos, archivos de un respaldo o copia de seguridad.
- **Riesgo:** el potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.
- **Seguridad de la Información:** La seguridad de la información se entiende como la preservación de las siguientes características:
  - ✓ Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
  - ✓ Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
  - ✓ Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Seguridad física y ambiental:** Impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información de la universidad.
- **Seguridad Informática:** se encarga de la identificación de las vulnerabilidades de un sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten estas debilidades.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento,

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Sistema de Información:** sistema, automatizado o manual, que abarca personas, máquinas, y/o métodos organizados de recolección de datos, procesamiento, transmisión y diseminación de datos que representa información para el usuario.
- **Software (o programas):** equipamiento lógico o soporte lógico de un computador digital. Conjunto de componentes lógicos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).
- **Tecnología de la Información:** Se refiere al hardware y software operados por la UNED o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la UNED, sin tener en cuenta la tecnología utilizada, ya se trate de procesamiento de datos, telecomunicaciones u otro tipo.
- **Terceros:** todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la universidad.
- **UNED:** Universidad Estatal a Distancia.
- **Unidad de Seguridad Digital:** Es la persona o personas que cumple la función de supervisar el cumplimiento del Manual de Seguridad de la Información, la Política de Seguridad de la Información y de asesorar en materia de seguridad de la información a los funcionarios de la UNED que así lo requieran.
- **Unidades Académicas:** Son las Escuelas y demás dependencias de la UNED que son propietarias de la información almacenada en registros académicos.
- **Unidades Organizativas:** Las Unidades Organizativas de la UNED son los Centros Universitarios, Subsedes, Escuelas, Direcciones, Oficinas y demás áreas administrativas.
- **Uso inapropiado de los recursos o Incidente múltiple:** cualquier acción que vaya en contra de lo estipulado en el Reglamento para Usos de Equipos de Cómputo e Internet de la UNED.
- **Usuario:** Son usuarios, los estudiantes, visitantes y demás personas que asuman la condición de usuarios de los equipos de la UNED o que hagan uso del internet o de la red institucional.
- **Virus:** Programa que se inserta en computador y que realiza una serie de funciones, en algunos casos dañinos, no deseados o innecesarios para el equipo de cómputo. Para los efectos de este reglamento comprenderá, sin dejar de lado lo anterior, los caballos de Troya, las bombas lógicas y los gusanos.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- **Vulnerabilidades:** son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la UNED, las cuales se constituyen en fuentes de riesgo.

## Nombres y Abreviaturas

Abreviatura	Nombre de la dependencia
Dep./Func.	Dependencias y/o funcionario(a)s respectivas
C.USD.DTIC	Coordinación de la Unidad de Seguridad Digital
D.DTIC	Director (a) de la Dirección de Tecnología de Información y Comunicaciones
Solic.	Solicitante

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Actores y Responsabilidades

ACTOR	RESPONSABILIDADES
Coordinación de la Unidad de Seguridad Digital de la Dirección de Tecnología de Información y Comunicaciones	<ul style="list-style-type: none"> <li>• Elaborar el Estudio de incidentes y/o anomalías de Seguridad en TI.</li> <li>• Coordinar con las instancias y/o funcionarios que se considere necesario para elaborar el estudio de incidentes y/o anomalías de Seguridad en TI.</li> <li>• Implementar las acciones que se consideren necesarias para eliminar el riesgo o mitigar los daños en la seguridad en TI.</li> <li>• Elaborar el informe en Seguridad en TIC, para ser trasladado a la Oficina de Recursos Humanos y a la jefatura correspondiente.</li> </ul>
Director (a) de la Dirección de Tecnología de Información y Comunicaciones	<ul style="list-style-type: none"> <li>• Analizar y tramitar ante la Coordinación de la Unidad de Seguridad Digital, para la elaboración del Estudio de incidentes y/o anomalías de Seguridad en TI.</li> </ul>
Solicitante	<ul style="list-style-type: none"> <li>• Solicitar ante la Dirección de Tecnología de Información y Comunicaciones, la elaboración del Estudio de incidentes y/o anomalías de Seguridad en TI.</li> <li>• Implementar las medidas o acciones necesarias de conformidad con los hallazgos del Estudio de incidentes y/o anomalías de Seguridad en TI.</li> </ul>
Dependencia (s) y/o Funcionario (a) (s)	<ul style="list-style-type: none"> <li>• Colaborar y facilitar lo que sea necesario para la elaboración del Estudio de incidentes y/o anomalías de Seguridad en TI.</li> </ul>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Matriz Descriptiva de los Procedimientos

<b>PR-06-01 Procedimiento para la atención de estudios, incidentes y/o anomalías de Seguridad Informática.</b>			
<b>Orden</b>	<b>Descripción actividades</b>	<b>Responsable</b>	<b>Paso</b>
<b>01.01</b>	Presenta la necesidad de realizar un estudio sobre el uso de equipo de cómputo e internet. En caso de ser derivado del <sup>16</sup> monitoreo, <b>Pasa al orden 1.3</b> En caso de que la necesidad sea presentada por Jefaturas/D.DTIC/Autoridades envía la solicitud de estudio mediante a la dirección de la DTIC	Solic.	<b>01.02</b>
<b>01.02</b>	Recibe analiza y tramita la solicitud de estudio. Traslada la coordinación de la Unidad de Seguridad Digital de la DTIC el estudio a realizar En caso de ser rechazada finaliza el procedimiento.	D.DTIC	<b>01.03</b>
<b>01.03</b>	Recibe analiza y coordina con las instancias y/o funcionario(a)s respectivas lo necesario para realizar el estudio	C.USD.DTIC	<b>01.04</b>
<b>01.04</b>	Recibe y facilita los respectivo para la realización del estudio	Dep./Func.	<b>01.05</b>
<b>01.05</b>	Realiza estudio. En caso de no detectar incidentes o anomalías <b><u>pasa al orden 1.7</u></b> En caso de detectar anomalías <b><u>pasa al orden 1.7</u></b> En caso de detectar incidentes	C.USD.DTIC	<b>01.06</b>
<b>01.06</b>	Ejecuta las acciones necesarias para eliminar el riesgo o mitigar los daños, en coordinación con las unidades de la DTIC que correspondan y/o la instancias y/o funcionario(a)s respectivas.	C.USD.DTIC	<b>01.07</b>
<b>01.07</b>	Elabora el Informe sobre seguridad en TIC de la UNED y se envía a la D.DTIC, la Oficina de Recursos Humanos y la jefatura correspondiente.	C.USD.DTIC	<b>01.08</b>
<b>01.08</b>	Recibe, analiza y tramita lo <sup>17</sup> correspondiente de conformidad con los hallazgos del Informe sobre la seguridad en TIC.	<sup>18</sup> Solic.	<b>FIN</b>

<sup>16</sup> El monitoreo es acción exclusiva de la Unidad de seguridad digital de la DTIC.

<sup>17</sup> En caso de que se detectara una anomalía o incidente, deberá el/la solicitante aplicar los correspondiente establecido en el Estatuto de personal y el Estatuto orgánico.

<sup>18</sup> En caso de la aplicación de sanciones, la C.USD.DTIC, únicamente suministra los hallazgos en el Informe sobre seguridad en TIC.

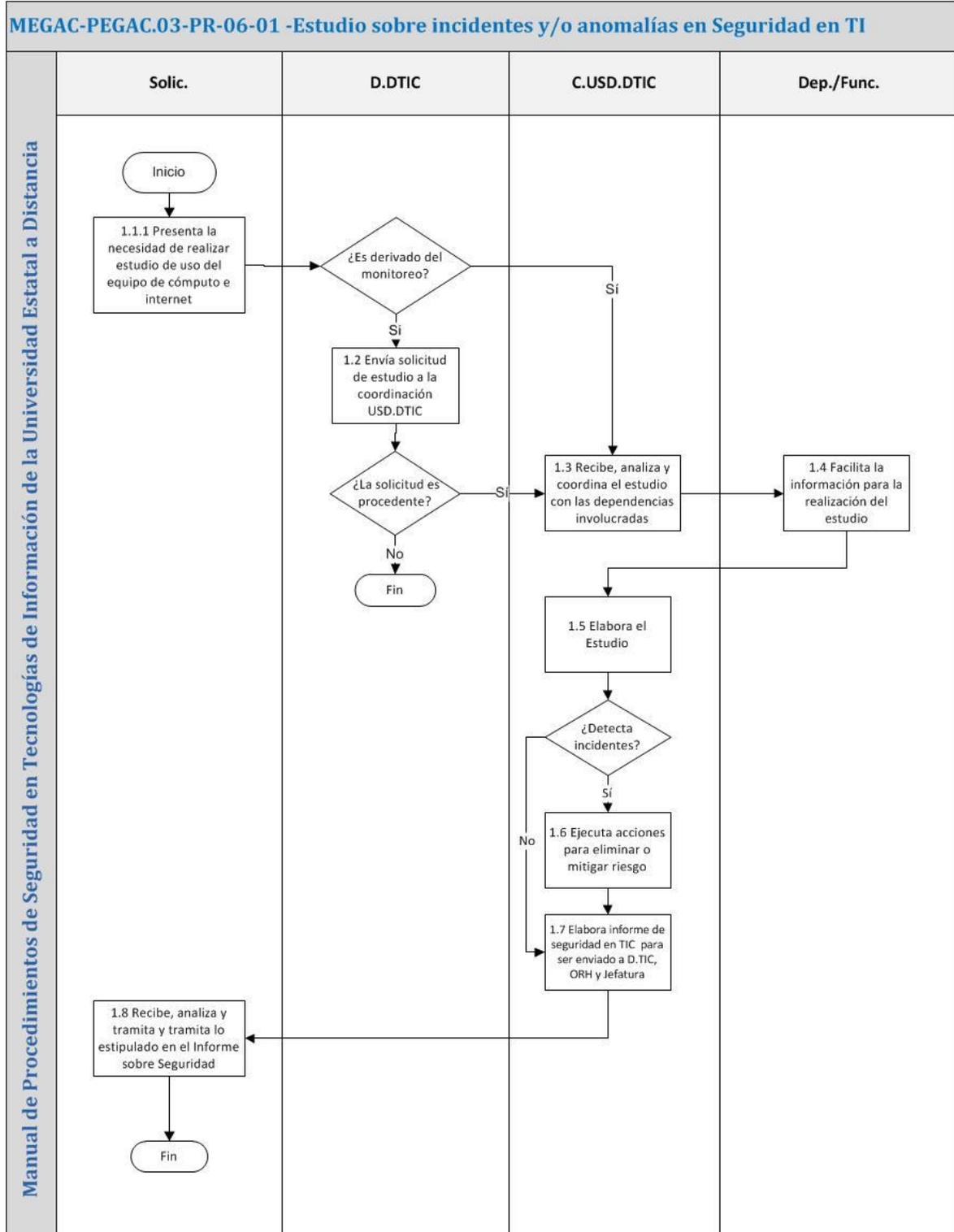
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Matriz Resumida de Procedimientos y sus Objetivos

MEGAC-PEGAC.03 - Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia		
Nº	Procedimiento del Proceso	Objetivo
PR-06-01	Procedimiento para la atención de estudios, incidentes y/o anomalías de Seguridad Informática.	Velar por la seguridad informática y el uso correcto del equipo de cómputo e internet de la Universidad.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Diagrama o Mapa del Procedimiento



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Administración, Control y Evaluación

### Información

1. La documentación de los trabajos se realiza mediante formularios de la siguiente manera:
  - a. Formulario de Autorizaciones.
  - b. Reporte de Incidentes de Seguridad Informática.
  - c. Registro de ingreso al centro de datos
  - d. Solicitud de Códigos de Usuarios.
  - e. Oficios de Cese de Funciones
2. Además, se toma de referencia los siguientes documentos:
  - a. Reglamento para uso de equipo de cómputo e internet
  - b. Convenio de nombres para dispositivos tecnológicos.
  - c. Configuración Base para los equipos de cómputo institucional
  - d. Acuerdos de Niveles de Servicio.
  - e. Divulgación de normativa institucional,
  - f. Nomenclatura de Dispositivos Tecnológicos
  - g. Nomenclatura de Servidores
  - h. Plan de Contingencias Tecnológicas de la UNED
  - i. Marco Jurídico de TI de la UNED
3. Los criterios técnicos, emitidos mediante oficio de la DTIC, a las instancias o funcionarios solicitantes.
4. Correos electrónicos<sup>19</sup> institucionales usados instrumento de comunicación oficial para toda la comunidad universitaria, en relación a la gestiones de la DTIC y de afectación a todas o algunas instancias.
5. Los tiquetes de solicitudes de órdenes de trabajo, emitidos por el sistema de tiquetes.

---

<sup>19</sup>Declarado el Correo Electrónico Institucional como medio oficial para el tránsito y comunicación de información, en la referencia: CR/2003-548 del 08 de julio, 2003; del acuerdo tomado por el Consejo de Rectoría, sesión ordinaria No. 1297-2003, Art. II celebrada el 30 de junio, del 2003.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Comunicación

Los mecanismos de comunicación y/o divulgación serán:

1. <sup>20</sup>Correo electrónico.
2. Videoconferencia
3. Talleres
4. Charlas
5. Entrega de documentos en papel.
6. Sitio Web Institucional

## Coordinación

1. De acuerdo a las actividades de la Matriz descriptiva de los Procedimientos y las responsabilidades establecidas para cada actor (ver Matriz de Actores y Responsabilidades).
2. Los instrumentos de información citados en el punto uno de Información.

## Controles

### Control Antes

1. Los criterios técnicos emitidos mediante oficio de la DTIC.
2. Monitores y estudios necesarios.
3. Todas las normas de aplicación citadas en el presente manual.
4. Plan de contingencias.

### Control Durante

1. Correos institucionales para la comunicación de situaciones particulares, y el abordaje por parte de la DTIC.
2. Oficios recibidos
3. Consecutivos de formularios
4. Mediante el seguimiento a las solicitudes por medio de tiquetes.

### Control Después

1. Implementación de controles de seguridad

---

<sup>20</sup>Declarado el Correo Electrónico Institucional como medio oficial para el tránsito y comunicación de información, en la referencia: CR/2003-548 del 08 de julio, 2003; del acuerdo tomado por el Consejo de Rectoría, sesión ordinaria No. 1297-2003, Art. II celebrada el 30 de junio, del 2003.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

2. Compra de equipo o software para mitigar amenazas
3. Auditorias de Seguridad informática (En coordinación con la Auditoria Interna de la UNED)
4. Gestión de Riesgos informáticos

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Parámetros de Seguimiento, Actualización, Rediseño o Anulación del Manual

Dependencia	Parámetro
Director (ra) de la Dirección de Tecnología de Información y Comunicaciones  Unidad de Seguridad Digital de la DTIC	<ul style="list-style-type: none"> <li>• Debe velar por el seguimiento de los procedimientos aquí establecidos, de modo que controle la necesidad de realizar un análisis sobre los mismos.</li> <li>• Debe realizar la/las actualizaciones a este manual y solicitar de ser necesario el acompañamiento al CPPI.</li> <li>• Debe enviar cualquier cambio para valoración al CPPI, si son de forma puede enviarse de forma digital sin necesidad de oficio y si son de fondo (Actores, responsabilidad o modificaciones al procedimiento, así como la anulación-eliminación- del manual o su rediseño) debe ser enviado mediante oficio.</li> <li>• Cumplir con las demás responsabilidades establecidas en este manual.</li> <li>• Deberá velar por la divulgación del documento y la publicación en la página web de la UNED.</li> </ul>
Centro de Panificación y Programación Institucional	<ul style="list-style-type: none"> <li>• Brindará el acompañamiento necesario de ser solicitado.</li> <li>• Como dependencia competente de considerarlo necesario comunicará cualquier cambio para ser implementado previo consenso con las partes.</li> <li>• Realiza por medio de la jefatura la pre-aprobación según criterio técnico correspondiente.</li> </ul>
Otras Dependencias de los Procedimientos de este manual	<ul style="list-style-type: none"> <li>• Deberán de acatar el cumplimiento de las responsabilidades asignadas en el procedimiento.</li> <li>• De considerar necesario una modificación de la/las actividades asignadas en el procedimiento, deberá coordinar previamente con la Dirección de Tecnología de Información y Comunicaciones .</li> </ul>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Anexos:

1. Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros
2. Directriz sobre el Uso de Redes Privadas Virtuales (VPN) UNED
3. Acuerdo de Rectoría CR.2016.1
4. Disposiciones de la Ley de Control Interno en cuanto a la Identificación y Valoración de Riesgos de TI
5. Instr-01 -MEGA-PEGTI.03-PR-06 -Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia del Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros

La directriz emitida por la Dirección de Tecnología Información y Comunicaciones (en adelante DTIC) para el control de acceso físico de funcionarios y terceros a los Centros de Datos de la universidad, tiene como objetivo principal, ofrecer a la comunidad universitaria una guía sobre las características y requerimientos mínimos que deben ser cumplidos respecto al acceso a estas áreas restringidas que tiene actualmente la Universidad Estatal a Distancia (UNED), como también las implicaciones por los daños que puedan ocasionar.

### Alcance

De cumplimiento obligatorio para todos los funcionarios de la UNED, en relación al acceso a estas áreas restringidas con las que se cuenta actualmente, así como las implicaciones por los daños que puedan ocasionar. Es aplicable al control de acceso físico de los siguientes Centros de Datos de la UNED:

- Centro de Datos ubicado en el Edificio B, Tercer Piso de la Sede Central
- Centro de Datos ubicado en el Edificio de Investigación y Desarrollo I+D, Segundo Piso de la Sede Central.
- Centro de Datos ubicado en el Centro Universitario de Cartago.

### Responsabilidades

1. Coordinador de la Unidad de Infraestructura Tecnológica (en adelante UIT): es responsable de coordinar las visitas a los Centros de Datos, asignar los accesos permanentes y temporales, junto con gestionar los posibles eventos de seguridad de información.
2. Funcionario de la Unidad de Infraestructura Tecnológica: es responsable del registro de las personas que ingresan al Centro de Datos, acompañarlos y revisar las actividades que se realizan, junto con identificar e informar cualquier evento de seguridad que pudiera presentarse. En el caso de Centros de Datos donde personal de la UIT no pueda realizar esta función, el Director de la DTIC en coordinación con el coordinador de la UIT pueden autorizar a otros funcionarios para que realicen estas labores. Esta autorización debe quedar debidamente documentada.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

3. Funcionario de recepción a los Centros de Datos: es responsable de registrar el ingreso y salida de las personas externas a la DTIC y a la UNED que visitan el Centro de Datos. El Director de la DTIC en coordinación con el coordinador de la UIT deben designar al funcionario responsable de esta labor.
4. Visitantes: las responsabilidades de los visitantes están descritas en el punto 5.6 de este procedimiento.

#### **Documentos Aplicables relacionados:**

- Manual de Seguridad de la Información
- Procedimiento de Gestión de Incidentes de Seguridad de la Información.

#### **Condiciones para el Acceso físico a los Centros de datos**

1. El acceso principal al Centro de Datos estará controlado mediante:
  - a. Control de acceso con tarjeta de proximidad.
  - b. Control de acceso con llave a la sala de servidores
  - c. Cámara de seguridad
2. No podrán ser almacenados dentro de los Centros de Datos ninguna especie de materiales inflables o peligrosos (por ejemplo: cartón, cajas, papel o cualquier otro material combustible similar.)
3. El Centros de Datos debe mantenerse limpio y ordenado en todo momento.

#### **Permisos de acceso al Centro de Datos**

1. La gestión de los permisos de acceso se encontrará a cargo de la Unidad de Infraestructura Tecnológica de la DTIC.
2. Todo ingreso al Centro de Datos debe ser registrado en el registro de ingreso al Centro de Datos (Ver **Anexo 1**).
3. Los permisos de acceso pueden ser permanentes o temporales según lo indicado a continuación:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### Acceso permanente

- Los accesos permanentes son asignados por el coordinador de la Unidad de Infraestructura Tecnológica a aquellos funcionarios de la DTIC que por la naturaleza de sus funciones lo requiera.
- Los accesos permanentes otorgados a funcionarios externos a la DTIC, deben contar con la debida solicitud de acceso ([Formulario de Autorizaciones](#)) y contar con el visto bueno del Director de la DTIC y el coordinador de la UIT.
- Todo funcionario externo a la DTIC que ingrese al Centro de Datos, debe hacerlo acompañado al menos al inicio y fin de sus labores, por un funcionario de la DTIC con permisos de acceso permanente o por personal de Seguridad en los casos de acceso fuera del horario laboral.

### Acceso Temporal

- Aquellos terceros tales como funcionarios de la UNED sin autorización de acceso permanente, contratistas y proveedores de servicios externos, que requieran ingresar al Centro de Datos, deben solicitar la autorización de acceso a la Unidad de Infraestructura Tecnológica. Ver [formulario de Autorizaciones](#).
- Solo la Unidad de Infraestructura Tecnológica podrá entregar autorizaciones de acceso al Centro de Datos.
- Los terceros autorizados a ingresar al Centro de Datos que no pertenezcan a la UNED deben previamente registrarse en la entrada del Edificio donde se encuentre el Centro de Datos al momento de ingreso y salida de las instalaciones de la universidad.
- Todo tercero que ingrese al Centro de Datos, debe hacerlo acompañado al menos al inicio y fin de sus labores, por un funcionario de la DTIC con permisos de acceso permanente o por personal de Seguridad en los casos de acceso fuera del horario laboral.

### Gestión de tarjetas de proximidad

- Las tarjetas de proximidad solo se entregarán a funcionarios de la DTIC con autorización de acceso permanente aprobado por la UIT.
- La habilitación, deshabilitación y entrega de la tarjeta de acceso la realizara la Unidad de Seguridad Digital a solicitud (vía correo electrónico) del coordinador de la Unidad de Infraestructura Tecnológica.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- c. Los funcionarios autorizados deberán firmar de recibido el oficio de entrega de la respectiva tarjeta de proximidad.

## Obligaciones

Toda persona que ingrese al Centro de Datos tiene las siguientes obligaciones, las que serán informadas previo al ingreso del Centro de Datos.

1. No podrá ingresar
  - a. Bajo los efectos del alcohol/drogas o cualquier sustancia alucinógena.
  - b. Portando armas de fuego, cuchillos o similares
  - c. Con vestimenta inapropiada (pantalones cortos, camisas sin mangas.)
  - d. Fumando
2. No podrá introducir ninguno de los siguientes materiales
  - e. Productos derivados del tabaco
  - f. Explosivos, elementos inflamables o corrosivos
  - g. Armas
  - h. Químicos
  - i. Drogas ilegales / alcohol
  - j. Artículos electromagnéticos
  - k. Materiales radioactivos
  - l. Cámaras fotográficas o de video
  - m. Se encuentra prohibido tomar fotografías dentro del Centro de Datos.
  - n. Cualquier otro artículo similar a los antes mencionados.
3. Al finalizar cualquier trabajo en el Centro de Datos, deberá asegurarse que los cables estén bien instalados y ordenados, dentro de sus gabinetes, así como asegurarse que todas las puertas están cerradas.
4. Remover desechos y cajas vacías antes de salir del edificio.
5. No se permiten comidas ni bebidas dentro del Centro de Datos.
6. No se permite tomar fotos ni el uso de cámaras fotográficas o cámaras de video.
7. No se permite el uso de aspiradoras, taladros o similares en el área de la sala de equipos (cuando se cuenta con piso falso).

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

8. No podrá instalar equipos inalámbricos o antenas en las dependencias del Centro de Datos.
9. Solo podrá conectar sus equipos a las salidas asignadas a sus respectivos gabinetes.

### **Excepciones**

Toda persona que ingrese al Centro de Datos puede solicitar la excepción de alguna regla establecida o no en este documento y la autorización de la misma debe ser aprobada por el Coordinador de la UIT. Por ejemplo, el ingreso de Cámaras fotográficas o Video de parte de personal del Instituto Nacional de Seguros, cuando realizan inspecciones.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Directriz sobre el Uso de Redes Privadas Virtuales (VPN) UNED

La directriz de uso de las Redes Privadas Virtuales (VPN por sus siglas en inglés), tiene como objetivo principal, ofrecer a la comunidad universitaria una guía sobre las características y requerimientos mínimos que deben ser cumplidos respecto del uso del servicio VPN que provee la Universidad Estatal a Distancia (UNED), como también las implicaciones por el mal uso.

Es importante mencionar que el uso inapropiado de los recursos dispuestos para los funcionarios, expone a la universidad a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus servicios, como también problemas judiciales tanto nacionales como internacionales

### Alcance

Las normas mencionadas en el presente documento, cubren el uso apropiado del sistema de Red Privada Virtual, tanto para acceso VPN IPSec como para VPN SSL de la universidad y aplica a todos los funcionarios, proveedores, empresas y en general cualquier persona que haga uso del servicio de forma autorizada.

### Formulario para el trámite de solicitud de autorizaciones VPN

Una de las gestiones que debe llevar acabo la Dirección de Tecnología Información y Comunicaciones en la UNED, es la gestión entorno a los usuarios de cada uno de los colaboradores de la institución, tanto en la sede central como en los centros universitarios. Parte de esta gestión se basa en la atención de solicitudes de creación, modificación y deshabilitación de cuentas de acceso remoto (VPN).

Para esto, la DTIC confeccionó el Formulario de Autorizaciones USD-FA-001, con el fin de facilitar al usuario la solicitud de autorización del acceso remoto VPN y a la vez permita gestionar de una manera ordenada estos accesos, cumpliendo con el registro de este tipo de trámites.

### Lineamientos del uso del Servicio

Sólo los usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, los que, además, serán los responsables del correcto uso del servicio de acceso remoto. Adicionalmente:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Es de responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
- Para el caso de usuarios externos: el uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte, manteniéndola siempre en secreto.
- Para el caso de usuarios internos (funcionarios): el uso del sistema VPN debe ser controlado utilizando la contraseña de acceso al correo electrónico institucional, manteniéndola siempre en secreto.
- Cuando esté conectado activamente a la red de la universidad, el sistema VPN permitirá el tráfico de acuerdo con el perfil del usuario hacia y desde el dispositivo tecnológico a través del túnel VPN, el resto del tráfico pasará por la conexión respectiva.
- Multiplicación paralela de túneles NO ESTÁ permitida, sólo una conexión está permitida por usuario.
- Las puertas de enlace VPN serán configuradas y administradas por la Unidad de Infraestructura Tecnológica (UIT).
- Todos los dispositivos tecnológicos conectados a las redes internas de la universidad mediante VPN o cualquier otra tecnología deberán utilizar el software antivirus más actualizado, provisto por la Unidad de Soporte Técnico (UST). En el caso de dispositivos tecnológicos personales conectados al sistema, el usuario debe proporcionar el antivirus respectivo.
- Los usuarios del sistema VPN serán automáticamente desconectados de la sesión, una vez que hayan transcurrido 30 minutos de inactividad. El usuario deberá validarse nuevamente para volver a conectarse a la red universitaria. Procesos artificiales informáticos como el "PING" no deben ser utilizados para mantener la sesión abierta.
- El concentrador VPN está limitado para un tiempo de conexión absoluta de 24 horas.
- Los usuarios externos a la universidad, deberán cumplir todas las disposiciones establecidas en el presente documento, así como lo establecido en el Reglamento

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

para uso de equipos de cómputo e internet y además firmar un acuerdo de confidencialidad de la información.

- Mediante el uso de la tecnología VPN, los usuarios declaran conocer que sus dispositivos tecnológicos, ya sea institucionales o personales son una extensión de las redes de la Universidad Estatal a Distancia y como tales, están sujetos a las mismas normas y reglamentos que se aplican a los equipos dentro de las dependencias de la universidad.

### **Inhabilitación de cuentas**

Las cuentas de acceso VPN se deshabilitarán con base en los siguientes criterios:

1. Por actividades anormales detectadas por la DTIC producto de monitoreos preventivos y estudios necesarios.
2. Después de dos meses de inactividad.
3. Finalizado la fecha de vigencia de la autorización indicado en el formulario de autorización.
4. A solicitud del usuario cuando éste ya no utilice el acceso.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Acuerdo de Rectoría CR.2016.124

# CONSEJO DE RECTORÍA

TELS: 2 2 2 4 1 6 8 9 • 2 5 2 7 - 2 5 0 3 • FAX 2 2 5 3 4 9 9 0  
CORREO: tmera@uned.ac.cr



**PARA:** Licda. Grace Madrigal Castro, Gerente Área de Seguimiento de Disposiciones, División de Fiscalización Operativa y Evaluativa, Contraloría General de la República

**DE:** *Theodosia Mena Valverde*  
**CONSEJO DE RECTORIA**

**FECHA:** 2 de marzo de 2016  
**REF.:** CR.2016.124

Le transcribo el acuerdo tomado por el Consejo de Rectoría, en sesión No. 1896-2016, Artículo VI, celebrada el 29 de febrero del 2016;

### CONSIDERANDO:

1. El acuerdo de prioridades TIC, aprobado en la sesión del Consejo de Rectoría No. 1724-2012, Artículo III, inciso 1), celebrada el 21 de mayo de 2012.
1. La aprobación del Plan de Desarrollo de Tecnologías de Información y Comunicación.
2. La importancia de dar cumplimiento a “Normas Técnicas para la gestión y el control de las tecnologías de información” emitidas por la Contraloría General de la República.
3. Las prioridades definidas en el Plan de Contingencia de TI aprobado por la Comisión Estratégica en Tecnología de Información y Comunicación.
4. El cumplimiento de la disposición 4.3 del informe N° DFOE-SOC-IF-08-2015 con fecha 15 de julio del 2015, emitido por la Contraloría General de la República que textualmente indica:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## CONSEJO DE RECTORÍA

TELEFONO: 2224 1689 • 2527-2503 • FAX 2253 4990  
CORREO: fme@uned.ac.cr



*4.3. Analizar, discutir y acordar, sobre la funcionalidad del acuerdo de ese Consejo, tomado en la Sesión No. 1724-2012 Art. III, inciso 1) del 21 de mayo de 2012, relacionado con las prioridades institucionales en tecnologías de información y comunicación (TIC) que debe atender la Dirección de Tecnologías de Información y Comunicación (DTIC) en coordinación con las unidades académicas y administrativas de la UNED, lo anterior de cara al nuevo Plan de Desarrollo de Tecnologías de Información y Comunicación de la UNED 2015-2019. Para el cumplimiento de esta disposición se deberá remitir a esta Contraloría General copia del acuerdo donde se haga constar el análisis realizado en torno al acuerdo del 21 de mayo antes citado, a más tardar el 29 de febrero de 2016. Ver comentarios de los párrafos 2.20 a 2.26.*

5. La importancia de una gestión orientada a prioridades, en materia de tecnologías de información y comunicación (TIC).

**SE ACUERDA:**

Aprobar las siguientes prioridades institucionales en tecnologías de información y comunicación (TIC), que deberá atender la Dirección de Tecnologías de Información y Comunicación (DTIC):

- a. **Sistemas de prioridad alta:**
  - i. Sistema de Administración Estudiantil (S.A.E.) y sus módulos, así como la implementación del Reglamento General Estudiantil
  - ii. Plataforma LMS (Moodle)
  - iii. Entorno Estudiantil
  - iv. Portal Web
  - v. Entorno de Funcionarios
  - vi. Sistema de Gestión y Desarrollo de Personal (SGDP)
  
- b. **Sistemas de prioridad media:**
  - i. SARCIE
  - ii. Sistema de Asignación de Tiempos Académicos
  - iii. Sistema Financiero Contable

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

CONSEJO DE RECTORÍA

---

TELEF: 2224 1689 • 2527-2503 • FAX 2253 4990  
 CORREO: [tmeng@uned.ac.cr](mailto:tmeng@uned.ac.cr)



**c. Sistemas de prioridad baja:**

- i. Todos aquellos sistemas que no se hayan incluido en las listas anteriores.**

Theo\*\* acuerdo 124\*02.03.2016

C: Dirección de Tecnología, Información y Comunicaciones  
 Auditoría  
 Consejo de Rectoría  
 archivo

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Disposiciones de la Ley de Control Interno en cuanto a la Identificación y Valoración de Riesgos de TI

Como parte del cumplimiento de la Ley General de Control Interno, Ley 8292, las Normas del Control Interno en el Sector Público (N-2-2009-CO-DFOE), publicado en la Gaceta N° 26 del 06 de febrero del 2009, las Directrices generales para el establecimiento y funcionamiento del sistema específico de valoración del riesgo (SEVRI) (D-3-2005-CO-DFOE), y con el fin de dar seguimiento a la adecuada implementación de la norma 1.3 de Gestión del riesgo, de las Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO.DFOE), la cual indica:

*“La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable”.*

*2. Cualquier consulta sobre la aplicación de la herramienta puede ser realizada a PROVAGARI<sup>21</sup>.”*

La DTIC debe contemplar los siguientes elementos para la identificación y valoración de Riesgos de TI:

1. Las Orientaciones generales para la implementación del sistema específico de valoración de riesgo institucional (SEVRI) en la UNED” (aprobadas por el Consejo de Rectoría en sesión 1833-2014, Artículo V, celebrada el 22 de setiembre del 2014), en las cuales se define:
  - a. Política de Riesgos para la universidad
  - b. Metodología para la gestión de riesgos en la UNED
  - c. Entre otros aspectos.
2. La metodología aplicada para la valoración del riesgo permite la identificación y gestión de todo tipo de riesgo, por lo que los riesgos relacionados con la seguridad de la información, procesos y proyectos de TI son tenidos en cuenta al realizar este proceso. Al ser identificados riesgos de TI estos son analizados en cuanto a su

<sup>21</sup>Actualmente PROCI.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

probabilidad e impacto y de no ser aceptados son administrados con el fin de lograr su mitigación.

3. El Consejo de Rectoría emitió en la sesión No. 1891-2015, Artículo IV, inciso 1), celebrada el 25 de enero del 2016, el siguiente acuerdo:

*“1. Solicitar a las dependencias que desarrollan e implementan proyectos de TI la aplicación obligatoria de la valoración de riesgos de acuerdo a las “Orientaciones generales para la implementación del sistema de valoración de riesgo institucional (SEVRI) en la UNED” las cuales se encuentran ubicadas en el sitio web de PROVAGARI<sup>22</sup>.*

4. Adicionalmente, la actualización de las “Orientaciones generales para la implementación del sistema de valoración de riesgo institucional (SEVRI) en la UNED”, incluyen un apartado denominado alcance, en el cual se define, en relación con el área de Tecnologías de Información que la valoración del riesgo se aplicará a:
  - a. Procesos de la DTIC que incluyen las operaciones continuas.
  - b. Proyectos tecnológicos de trascendencia institucional<sup>23</sup> los cuales influyen en los procesos de docencia, investigación, extensión, producción de materiales y gestión y que afecten la imagen que se proyecta a la ciudadanía.
5. Los responsables de proyectos en TIC deben aplicar de forma oportuna la valoración del riesgo en los proyectos en TIC que lo requieran y al menos 2 veces al año (al inicio de cada semestre) enviar por medio de oficio o correo electrónico la información referente al proyecto, lo cual ayudará a mantener actualizado el portafolio de proyectos TIC, cuya responsabilidad de ejecución recae sobre el Coordinador de Proyectos TIC de la Vicerrectora de Planificación.
6. La información de proyectos en TIC requerida es la siguiente:
  - a. Nombre del proyecto
  - b. Descripción del proyecto

<sup>22</sup>Actualmente PROCI.

<sup>23</sup>Entendiéndose proyectos tecnológicos de trascendencia institucional, todos aquellos proyectos que sean aprobados por la Comisión Estratégica de Tecnologías de Información y Comunicaciones.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- c. Recursos (internos, externos o mixtos)
  - d. Quién provee los recursos (UNED u otros)
  - e. Patrocinador (quién promueve el proyecto)
  - f. Fecha de inicio
  - g. Responsable del proyecto
  - h. Enlace en la DTIC
  - i. Fecha objeto de finalización
  - j. Área de vinculación (administrativo, académico, transaccional, etc.)
  - k. Estado actual
  - l. Fase actual (en producción o desarrollo)
  - m. Valoración de Riesgo
  - n. Prioridad (alta, baja, media, etc.)
7. Los documentos actualizados pueden ser consultados y descargados de la página del Programa de Control Interno.
- a. Acuerdos
  - b. Orientaciones
  - c. Estructura de Riesgos UNED.
  - d. Herramienta para la Identificación y Valoración de Riesgos.
8. Se cuenta con la asesoría permanente del Programa de Control Interno.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Responsabilidades de las áreas usuarias de la DTIC



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



# Responsabilidades de las áreas usuarias de la DTIC

### Autores:

Alejandro Sánchez Rivera, Coordinador Unidad de Soporte Técnico  
José Pablo Chaves Sánchez, Coordinador Unidad de Sistemas de Información  
Rolando Rojas Coto, Coordinador Unidad de Infraestructura Tecnológica

21-2-2017

Responsabilidades de las áreas usuarias de la DTIC v1.0

No. páginas 1 de 9

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



## Contenido

Presentación .....	3
Unidad de Sistemas de Información .....	4
Categoría de usuarios para los Sistemas de Información Transaccionales .....	4
Lider de servicio: .....	4
Usuario operativo .....	5
Usuario indirecto .....	5
Categoría de usuarios del SIADTGE .....	5
Usuario administrador .....	5
Usuario editor .....	6
Usuario visor .....	6
Unidad de Infraestructura Tecnológica .....	6
Unidad de Soporte Técnico .....	6
Glosario .....	8

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



## Presentación

El objetivo del presente documento es identificar los usuarios y especificar las responsabilidades de los mismos, acorde a los servicios ofrecidos por tres de las unidades que integran la Dirección de Tecnologías de Información y Comunicaciones (DTIC), específicamente la unidad de sistemas de información (USI), la unidad de infraestructura tecnológica (UIT) y la unidad de soporte técnico (UST).

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



## Unidad de Sistemas de Información

La Unidad de Sistemas de Información (USI), es la encargada de los Sistemas de Información que apoyan la Gestión Académica y Administrativa de la Universidad, la categorización de los usuarios de la unidad es acorde a la relación que tienen con los sistemas.

### Categoría de usuarios para los Sistemas de Información Transaccionales

**Líder de servicio:** persona experta que conoce los procesos automatizados por el sistema de información y sus implicaciones, por ello, tiene el máximo privilegio dentro del área que administre.

Sus responsabilidades son:

- Definición de los requerimientos del sistema, acorde a los procesos que se automatizan y las necesidades de los usuarios operativos, velando por la calidad de la información con la que se alimenta el sistema y porque cumpla con las políticas de la UNED
- Reporte de errores y las solicitudes de implementación o mantenimiento sugiriendo su prioridad, valiéndose del apoyo del usuario operativo y cumpliendo con el procedimiento interno de trabajo la DTIC.
- Participación de manera activa en el desarrollo de las aplicaciones, establecimiento de los criterios mínimos de aceptación, aprobación de la etapa de pruebas y autorización de los pases a producción indicando el mejor momento para realizarlos.
- Manejo de la comunicación de lo relacionado al sistema con todos los interesados del mismo.
- Definición del rol de cada usuario operativo
- Recepción de solicitudes de parte de los usuarios indirectos cuando estos necesiten acceder a información específica del sistema que no puede ser proporcionada por medio del SIATDGI, otorgando acceso, siempre que no se incumpla con alguna norma de aplicación. La forma en que dará acceso será a través de opciones ya existentes o mediante la creación de un reporte con una estructura particular, en dicho caso, realizando la respectiva solicitud de emisión o implementación del reporte a la DTIC. En cualquiera de las formas en que le dé acceso, deberá emitir además un aviso de distribución restringida y si el tipo de restricción de divulgación de la información lo amerita, deberá proceder a firmar un contrato de confidencialidad con el usuario indirecto.

† Esto contempla Acuerdos Internacionales o Leyes Nacionales que resguardan la información, algún reglamento o norma de aplicación en la UNED, o la información goce de algún tipo de restricción en su divulgación según la clasificación interna de la UNED. En caso de que el líder de servicio deba negar el acceso por incumplirse alguno de estos aspectos, deberá justificar el motivo al usuario indirecto.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



Si la información requerida por el usuario indirecto no se encuentre en el sistema, el líder de servicio realizará la propuesta de inclusión en los casos que corresponda, de lo contrario, deberá justificar al usuario indirecto el motivo de la negativa.

**Usuario operativo:** persona que posee una interacción directa con el sistema de información. Mediante el rol que le fue asignado, hace uso de las opciones respectivas del sistema para acceder a la información existente, modificarla de ser el caso, ingresar la nueva cuando se requiera y ejecutar procesos, todo acorde a las labores que realiza en su puesto o para cumplir con directrices específicas de interés institucional.

Sus responsabilidades son:

- Propuesta al líder de servicio de mejoras a la implementación de los sistemas existentes o nuevos desarrollos,
- Reporte al líder de servicio de cualquier error que detecte en la operación del sistema.

**Usuario indirecto:** persona que necesita consultar información de un sistema que implementa procesos que no se relacionan directamente con las labores de su puesto, pero que requiere acceder a la misma para realizar las tareas que se le encomiendan.

Sus responsabilidades son:

- Solicitud de permiso de consulta de información al líder de servicio del Sistema de Información Transaccional quién definirá las vías en que tendrá acceso, en caso de proceder la solicitud.

Si es un software el que necesita acceder a la base de datos de un Sistema de Información Transaccional, la DTIC permitirá el acceso directo sin mediar ninguna autorización cuando se trate de un catálogo. Para cualquier otro tipo de datos, le corresponderá al líder de servicio del software en rol de usuario indirecto, tramitar la respectiva solicitud de acceso con el líder de servicio del Sistema de información Transaccional.

#### Categoría de usuarios del SIADTGI

**Usuario administrador:** goza de máximo privilegio en el SIADTGI, tanto de permisos como de control sobre la estructura de la información. Es el responsable de otorgar los permisos de acceso a indicadores para el usuario editor y el usuario visor.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología,  
Información y Comunicaciones



**Usuario editor:** usuario con permisos de acceso a un grupo definido de indicadores del sistema, para los cual tiene además la potestad de modificar la forma en que se presenta la información y los filtros que estarán disponibles para la misma.

**Usuario visor:** usuario con permisos de acceso a un grupo definido de indicadores del sistema, para los cuales solo puede consultar la información utilizando los filtros que tenga a su disposición.

### Unidad de Infraestructura Tecnológica

La principal función de la Unidad de Infraestructura es la administración del centro de datos y brindar servicios de tecnologías de información basados en los siguientes modelos:

- a) *Infraestructura como servicio:* proporcionar infraestructura como electricidad, red de datos, servidores y virtualización.
- b) *Plataforma como servicio:* además de los elementos de infraestructura como servicio, sistemas operativos, almacenamiento de datos y ejecución de programas. \*
- c) *Software como servicio:* además de los elementos de infraestructura y plataforma de servicios, se incorpora el software administrado por la DTIC. \*

Para todos los modelos anteriores, se distingue un único usuario, el *usuario directo*, que tiene como responsabilidades:

- Generación de las solicitudes necesarias para la implementación del servicio en el centro de datos.
- Reporte de averías relacionadas al servicio brindado.
- Coordinación con la DTIC la realización de respaldos involucrados con el servicio brindado.
- Coordinación de visitas y revisiones con los funcionarios de la UIT.
- Mantenimiento de todas las plataformas que alberga el centro de datos ligadas al servicio brindado.

### Unidad de Soporte Técnico

Es la unidad encargada de brindar apoyo a las demás instancias de la UNED con el fin de facilitar el acceso a los recursos y servicios TIC institucionales, razón por la cual tiene como usuarios todas las personas funcionarias y dependencias que integran la universidad, quienes se encargan de reportar los incidentes en materia de TI que se les presenten para que se les dé su correspondiente atención.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



Dada la cantidad de usuarios tanto en sede central como en centros universitarios, se implantó una dinámica de trabajo que busca dar una respuesta más expedita a los incidentes reportados, dicha dinámica se basa en la figura de un *usuario soportista delegado*, persona funcionaria que se encuentra en algunos centros universitarios y brinda colaboración en materia de hardware y software en las diferentes regiones del país, sus responsabilidades específicas son:

- Soporte técnico de hardware.
- Soporte técnico de software.
- Instalación de programas y equipos.
- Limpieza de equipos.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



## Glosario

**Aviso de distribución restringida:** detalle de cualquier acuerdo internacional, ley nacional, reglamento o norma de aplicación en la UNED que resguarde la información y deba ser acatado.

**Base de datos:** repositorio digital de datos estructurados y relacionados de alguna manera, con posibilidades de almacenamiento y recuperación.

**Catálogo:** lista de elementos que pertenecen a una misma categoría.

**Centro de datos:** espacio físico donde se albergan todos los recursos necesarios para el procesamiento de la información de la organización y que cuenta con las medidas de seguridad óptimas para su funcionamiento.

**Contrato de confidencialidad:** documento mediante el cual, las partes involucradas se obligan a respetar no solo el secreto y la confidencialidad de la información que se está compartiendo, sino también a utilizarla solo para un fin determinado.

**Dato:** representación simbólica de algún conocimiento (mediante números o letras), que carece de valor semántico y por ello no transmite un mensaje.

**Hardware:** conjunto de componentes físicos que integran una computadora.

**Incidente:** situación inesperada que afecta el aprovechamiento que se puede hacer de las tecnologías de información, limitándolo o impidiéndolo del todo.

**Información:** conjunto de datos adecuadamente organizados y procesados para que adquieran significado, transmitan conocimiento y permitan la toma de decisiones.

**Red de datos:** infraestructura diseñada específicamente para transmitir información mediante el intercambio de datos.

**Rol:** es la especificación detallada de las opciones a las que un usuario tiene permiso de utilizar en un sistema.

**Perfil:** nombre que se le confiere al conjunto de roles que le son asignados a un usuario para el cumplimiento de sus funciones.

**Plataforma:** sistema que sirve como base para el funcionamiento de determinado hardware o de software con los que es compatible.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
Rectoría  
Dirección de Tecnología  
Información y Comunicaciones



**SIATDGI:** Sistema de Información de apoyo para la toma de decisiones y gestión institucional.

**Sistema de información transaccional:** sistema que permite, según corresponda, recolectar, almacenar, modificar y recuperar la información ligada a los procesos que automatiza, garantizando la seguridad y la fiabilidad de los datos involucrados.

**Software:** conjunto de programas, instrucciones y reglas informáticas, que hacen posible la realización de tareas específicas dentro de una computadora.

**Usuario:** persona que utiliza determinado hardware y software para obtener un servicio específico. Para ello, debe contar con una serie de permisos que permiten establecer perfiles y roles.

También puede tratarse de un software que necesita acceder total o parcialmente la base de datos de un Sistema de Información Transaccional.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

**Instr-01 -MEGA-PEGTI.03-PR-06 -Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia del Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia**

Universidad Estatal  
a Distancia

Dirección de Tecnología,  
Información y  
Comunicación

## Instructivo de de la UNED

Asesoría por el Centro de Planificación y  
Programación Institucional

Junio 2017

---

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Tabla de contenidos

Aprobación .....	108
Elaboración y Revisión .....	109
Instructivo para el trámite de solicitud de códigos de usuarios de Producción en la DTIC (Cuenta de Correo electrónico Office 365, AS/400, accesos, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional).....	112
¿En qué consisten las solicitudes de usuarios? .....	112
Conceptos.....	112
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	112
Actividades para realizar el trámite de solicitudes de códigos de usuarios .....	112
1- Datos del solicitante.....	114
2- Detalle de la solicitud .....	114
3- Visto bueno del Jefe Inmediato .....	117
4- Recepción de solicitud .....	117
5- Datos de recibido .....	118
6- Solicitud de Creación de Usuarios para Centros Universitarios.....	118
7- Inhabilitar cuentas de usuario .....	119
(Cuenta de correo electrónico Office 365, código de usuario para los equipos de cómputo, dispositivos tecnológicos y acceso a la red institucional) .....	119
Instructivo para el trámite de solicitud de códigos de usuarios Institucional (Cuenta de Correo electrónico Office 365, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional) .....	135
¿En qué consisten las solicitudes de usuarios? .....	135
Conceptos.....	135
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	135
Actividades para realizar el trámite de solicitudes de códigos de usuarios .....	135
1- Datos del solicitante.....	137
2- Autorización del Director de la Escuela o Jefe Inmediato .....	138

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

3- Recepción de solicitud .....	138
4- Datos de recibido .....	139
5- Solicitud de Creación de Usuarios para Centros Universitarios.....	139
6- Inhabilitar cuentas de usuario (Cuenta de correo electrónico Office 365, código de usuario para los equipos de cómputo, dispositivos tecnológicos y acceso a la red institucional).....	140
Instructivo para el trámite de Autorizaciones (Aplicación, VPN, Puerto, Red Social y Otros).....	153
¿En qué consiste el trámite de Autorizaciones?.....	153
Conceptos.....	153
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	153
Actividades para realizar el trámite de Autorizaciones.....	154
1- Datos del Solicitante .....	156
2- Detalle de la solicitud .....	157
3- Visto Bueno del Jefe Inmediato.....	158
4- Datos del trámite realizado.....	159
5- Inhabilitar cuentas de usuario de VPN .....	160
Instructiva creación de cuentas de usuarios de VPN.....	165
¿En qué consiste la creación de cuentas de usuarios de VPN? .....	165
Conceptos .....	165
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	165
Actividades para realizar la Creación de Usuarios de VPN.....	165
1. Creación de Usuarios .....	165
2. Entrega del Usuario .....	169
3. Inhabilitar cuenta de usuario .....	171
Instructivo para el trámite del código de usuarios de desarrollo.....	175
¿En qué consiste el trámite del código de usuarios de desarrollo? .....	175
Conceptos.....	175
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	175

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Actividades para realizar el trámite de Código de usuarios.....	175
1- Datos del Solicitante .....	177
2- Visto Bueno del Coordinador de Proyectos .....	178
3- Datos del trámite realizado .....	178
Instructivo para la Creación e inhabilitación de usuarios de la plataforma AS400180	
¿En qué consiste la creación de usuarios e inhabilitación de AS-400? .....	180
Conceptos.....	180
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	180
Actividades para creación de usuarios e inhabilitación de AS-400.....	181
Entrega del usuario .....	187
Inhabilitar usuario AS400 .....	187
Instructivo para la creación de cuentas de usuarios en Active Directory .....	190
¿En qué consisten las solicitudes de usuarios? .....	190
Conceptos.....	190
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	190
Actividades paracreación de cuentas de usuarios en Active Directory .....	190
1. Cuentas usuario Active Directory - Creación de Usuarios sin correo electrónico	190
2. Creación de Cuentas de Usuario con Correo Electrónico.....	196
8. Creación de Cuentas de Correo para Usuarios ya Existentes.....	221
1. Creación del Grupo de Distribución .....	226
5. Entrega del Usuario .....	228
6. Inhabilitar cuentas de usuario .....	229
Instructivo para la Administración de Usuarios, roles y privilegios en ORACLE...	243
¿En qué consisten los roles y privilegios de ORACLE? .....	243
Conceptos.....	243
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	243
Actividades para realizar el trámite de Usuarios, roles y privilegios .....	245

 <p><b>UNED</b> UNIVERSIDAD ESTADAL A DISTANCIA Instituto Venezolano de la Educación y la Cultura</p>	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

(1) Creación de usuarios en Oracle .....	245
(2) Para crear Roles de base de datos en ORACLE .....	248
(3) Asignación de privilegios a roles de base de datos en ORACLE .....	250
Instructivo para la Administración de Usuarios, roles y privilegios de SQL Server	253
¿En qué consisten el Inicio de Sesión, los roles y privilegios de SQL Server? .....	253
Conceptos .....	253
Para la ejecución de las actividades se debe tener en cuenta lo siguiente .....	253
Actividades para realizar el trámite de Configuración del Inicio de Sesión de los Usuarios .....	254
(1) Pasos para crear un Inicio de sesión en SQL Server .....	254
(2) Pasos para crear un Roles de base de datos en SQL Server .....	261
(3) Pasos para otorgar privilegios a roles de base de datos en SQL Server	264

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Aprobación

En relación a la solicitud planteada por el señor Vicerrector de Planificación el Dr. Edgar Castro Monge, de realizar el levantamiento los procesos de la universidad, en concordancia al proyecto de la Propuesta del Macroproceso Institucional, se trabaja en la elaboración del presente ***Instructivo para la Gestión de Usuarios de la Universidad Estatal a Distancia***, en coordinación con el Centro de Planificación y Programación Institucional y representantes de las dependencias involucradas.

<b>Pre-aprobación</b>	Juan Carlos Parreaguirre, Jefe del Centro de Planificación y Programación Institucional
<b>Aprobación final</b>	Consejo de Rectoría

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



**PARA:** Mag. Juan Carlos Parreaguirre, Jefe Centro de Planificación y Programación Institucional  
Mag. Francisco Durán, Director Tecnología, Información y Comunicaciones

**DE:** *Theodosia Mena Valverde*  
**CONSEJO DE RECTORIA**

**FECHA:** 28 de junio de 2017  
**REF.:** CR.2017.635

Les transcribo el acuerdo tomado por el Consejo de Rectoría, en sesión No. 1950-2017, Artículo V, inciso 3), celebrada el 26 de junio del 2017.

Se conoce nota CPPI.048.2017 (REF.1070.17) con fecha 20 de junio del 2017, suscrita por la Mag. Juan Carlos Parreaguirre, Jefe Centro de Planificación y Programación Institucional en relación con la entrega del Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia y del Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia; trabajo colaborativo, liderado por el Centro de Planificación y Programación Institucional con el apoyo de la Dirección de Tecnologías de Información y Comunicación, en busca el ordenamiento institucional.

**SE ACUERDA:**

1. Aprobar el Manual Específico de Seguridad en TI de la Universidad Estatal a Distancia.
2. Aprobar el Instructivo para Gestión de usuarios de la Universidad Estatal a Distancia.

Theo\*\* acuerdo 635\*28.06.2017

C: Ana Iveth Rojas, CPPI / Grettel Schonwandt, CPPI  
Vicerrectoría de Planificación  
Archivo

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Elaboración y Revisión

El Centro de Planificación y Programación Institucional, CPPI mediante su Unidad de Programación y Procesos y de conformidad al acuerdo al Manual Organizacional UNED-2012 tiene dentro de sus funciones *“Coadyuvar en la formulación de los procedimientos de trabajo de las unidades administrativas, académicas y técnicas que componen la UNED, para alcanzar, de manera eficiente, los objetivos que les corresponde dentro de la actividad institucional “.*

Para la elaboración del ***Instructivo para la Gestión de Usuarios de la Universidad Estatal a Distancia***, se brindó asesoría mediante sesiones de trabajo conjunto, con el funcionario de la DTIC: Johnny Saborío Álvarez, coordinador de la Unidad de Seguridad Digital; y se realizaron las consultas pertinentes y la participación de los siguientes funcionarios:

Alejandro Sánchez Rivera, **Coordinador de la Unidad Soporte Técnico.**

Andrés Céspedes Monge, **Funcionario de la Unidad de Infraestructura Tecnológica.**

Erick López Agüero, **Funcionario de la Unidad de soporte técnico.**

Gonzalo Rodríguez Benavidez, **Coordinador de la Unidad de Sistemas de Información.**

Rolando Rojas Coto, **Coordinador de la Unidad de Infraestructura Tecnológica.**

La coordinación y asesoría estuvo a cargo del firmante.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Grettel Schonwandt Alvarado  
**Centro de Planificación y Programación Institucional**

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para el trámite de solicitud de códigos de usuarios de Producción en la DTIC (Cuenta de Correo electrónico Office 365, AS/400, accesos, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional)

### ¿En qué consisten las solicitudes de usuarios?

Es la gestión entorno a los usuarios de cada uno de los colaboradores de la institución, tanto en la sede central como en los centros universitarios. Se basa en la atención de solicitudes de creación de cuentas de usuarios para el sistema de correo electrónico en la nube Office 365, cuentas de usuario AS/400, y sus respectivos accesos, para ingresar a los equipos de cómputo, así como para los dispositivos tecnológicos y acceso a la red institucional.

### Conceptos

- **Boleta UIT-PL-002-Formulario -Solicitudes códigos de usuarios:** Instrumento para solicitar el correo electrónico en la nube Office 365, cuentas de usuario para AS/400 y sus respectivos accesos, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

1. En el caso que la solicitud es de un usuario del AS/400 y el funcionario que lo solicita cuenta con correo electrónico institucional, recibirá las credenciales por medio de correo, la DTIC tendrá un plazo de 4 días para crear y autorizar dicho usuario.

### Actividades para realizar el trámite de solicitudes de códigos de usuarios

1. Completar el Formulario Solicitudes para producción, de conformidad con lo establecido en este instructivo.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



**Formulario  
Solicitudes para  
PRODUCCIÓN**



Fecha de Solicitud:    /    /	Consecutivo Asignado: _____
Nombre solicitante: _____	Cédula: _____
Dependencia: _____	Puesto: _____
Solicitante es: <input type="radio"/> Administrativo <input type="radio"/> Profesional <input type="radio"/> Docente <input type="radio"/> Investigación	
<b>DETALLE DE LA SOLICITUD</b>	
<b>WINDOWS: Complete si es Correo Electrónico</b>	
Condición: <input type="checkbox"/> Propiedad <input type="checkbox"/> A Plazo    Hasta:    /    /	Teléfono Oficina: _____
<b>AS/400: Complete si es Usuario o Acceso</b>	
Tiene Usuario: <input type="radio"/> Si <input type="radio"/> No	Conserva acceso: <input type="radio"/> Si <input type="radio"/> No
Código Usuario: _____	
Detalle del usuario: _____	
Utilización: <input type="checkbox"/> Tiempo indefinido <input type="checkbox"/> Tiempo definido	
Desde:    dd/mm/aaaa	Hasta:    dd/mm/aaaa
<b>VISTO BUENO JEFE INMEDIATO</b>	
Nombre Completo: _____	Cédula: _____
Firma: _____	Sello: <table border="1" style="width: 50px; height: 30px; display: inline-table;"></table>
<b>PARA USO DE LA DTIC</b>	
<input type="radio"/> WINDOWS <input type="radio"/> Usuario <input type="radio"/> Grupo	<input type="radio"/> Correo Elect. <input type="radio"/> Lista Distribuc.
<input type="radio"/> AS/400 <input type="radio"/> Usuario <input type="radio"/> Grupo	<input type="radio"/> Lista Autoriz. <input type="radio"/> Acceso a Sistema
<input type="radio"/> LINUX <input type="radio"/> Usuario <input type="radio"/> Grupo	<input type="radio"/> SFTP
<input type="radio"/> VPN <input type="radio"/> Usuario	
<b>VISTO BUENO (PARA USO DE LA DTIC)</b>	
Mag. Francisco Durán Montoya VoBo Director DTIC	Lider de Proyectos DTIC VoBo
Realizado Por: _____	Fecha Realizado:    /    /
Código Asignado: _____	Contraseña Inicial: _____
Descripción : _____	
<b>DATOS DE RECIBIDO</b>	
Nombre Completo: _____	Firma: _____
<p><small>El funcionario de la UNED al firmar esta solicitud se hace responsable por los daños que se ocasionen a la UNED, personal o entidad externa, por el mal uso de este código. Este código es de uso personal y el funcionario debe cumplir con el Reglamento para Uso de Equipos de Cómputo e Internet de la UNED, aprobado por el Consejo Universitario en sesión N°2336, Art. II, (inciso 2-a) del 15 de mayo del 2014 y cualquier otra normativa que le resulte aplicable. Este reglamento lo debe consultar en: <a href="http://www.uned.ac.cr/reglamento/">http://www.uned.ac.cr/reglamento/</a></small></p>	

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 1- Datos del solicitante

(1) Fecha de Solicitud:    /    /	(2) Consecutivo Asignado: _____
(3) Nombre solicitante: _____	(4) Cédula: _____
(5) Dependencia: _____	(6) Puesto: _____
(7) Solicitante es: <input type="radio"/> Administrativo <input type="radio"/> Profesional <input type="radio"/> Docente <input type="radio"/> Investigación	

(1) <i>Fecha de Solicitud:</i>	Debe indicarla fecha en la que se solicita la creación del usuario.
(2) <i>Consecutivo Asignado:</i>	Este número es asignado por la DTIC al momento de recibir la solicitud.
(3) <i>Nombre solicitante:</i>	Indicar el nombre completo del solicitante, que requiere la creación del usuario.
(4) <b>Cédula:</b>	Anotar el número de cédula en formato 00-000-000.
(5) <b>Dependencia:</b>	Indicar la dependencia a la cual pertenece el solicitante
(6) <b>Puesto:</b>	Especificar el nombre del puesto que desempeña
(7) <b>Es solicitante es:</b>	Se debe seleccionar el tipo de puesto que desempeña el solicitante. (Administrativo, Profesional, Docente, Investigador)

## 2- Detalle de la solicitud

DETALLE DE LA SOLICITUD	
(8) WINDOWS: Complete si es Correo Electrónico	(10) Teléfono Oficina: _____
(9) Condición: <input type="checkbox"/> Propiedad	_____
<input type="checkbox"/> A Plazo    Hasta:    /    /	
(11) AS/400: Complete si es Usuario o Acceso	(12) Tiene Usuario:    (13) Conserva acceso    (14) Código Usuario
	<input type="radio"/> Sí <input type="radio"/> No <input type="radio"/> Sí <input type="radio"/> No    _____
(15) Detalle del usuario: _____	
(16) Utilización: <input type="checkbox"/> Tiempo indefinido	
<input type="checkbox"/> Tiempo definido	Desde:    dd/mm/aaaa    Hasta:    dd/mm/aaaa

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

(8) <i>WINDOWS:</i>	<i>Si el solicitante requiere el correo electrónico debe completar la información que se solicita</i>
(9) <i>Condición:</i>	<i>Se refiere a el tipo de nombramiento en que se encuentre: en propiedad o a plazo fijo, si el nombramiento es a plazo se debe indicar en "Hasta" la fecha en que se termina el nombramiento en el formato dd/mm/aaaa.</i>
(10) <i>Teléfono</i>	<i>Brindar el número teléfono de la oficina donde se pueda contactar.</i>
(11) <i>AS/400</i>	<i>Si el solicitante requiere usuario de AS/400o modificar uno existente, debe completar la información que correspondiente.</i>
(12) <i>Tiene usuario</i>	<i>El solicitante marca con una "X" en el espacio SI cuando ya tiene código de usuario en el AS/400 y necesita que el acceso sea reemplazado por otras opciones. En caso contrario marca la opción NO.</i>
(13) <i>Conserva acceso</i>	<i>Marcar con una "X" la casilla SI en el caso que el usuario ya tiene acceso al AS/400 pero necesita que el acceso se mantenga y se agreguen nuevas opciones Marcar con una "X" al opción NO para indicar que el usuario no necesita los accesos actuales y modificarán según esta solicitud</i>
(14) <i>Código de usuario</i>	<i>Indicar el código de usuario del AS/400 actual que tiene asignado. Si el solicitante no tiene acceso al AS/400, debe marcar con una "X" la opción <b>No</b></i>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

<i>(15) Detalle de usuario</i>	<i>Indicar el acceso que necesita el nuevo usuario o un perfil de usuario del que se pueda tomar referencia los accesos que solicita</i>
<i>(16) Utilización</i>	<i>Debe indicar con una "X", si la utilización del usuario de AS/400 es por tiempo indefinido o tiempo definido con el nombramiento a plazo fijo, donde debe indicar en "Desde", la fecha en que el usuario debe estar activo y en "Hasta", la fecha en que se deberá deshabilitar, utilizando el siguiente formato para la fecha dd/mm/aaaa.</i>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 3- Visto bueno del Jefe Inmediato

VISTO BUENO JEFE INMEDIATO	
(17) Nombre Completo: _____	(18) Cédula: _____
(19) Firma _____	(20) Sello: <div style="border: 1px solid black; width: 80px; height: 30px; display: inline-block;"></div>

(17) Nombre Completo	<i>Indicar el nombre completo de la jefatura inmediata</i>
(18) Cédula	<i>Indicar el número de cédula de la jefatura inmediata; en formato 00-0000-0000.</i>
(19) Firma	<p><i>La firma de la jefatura inmediata constituye la aprobación de la solicitud y es un elemento indispensable para tramitar la misma.</i></p> <p>En caso que los accesos solicitados correspondan a un Sistema cuyo dueño o propietario no sea el Jefe inmediato del solicitante, el Jefe del solicitante deberá adjuntar ésta solicitud un oficio emitido por el dueño del sistema autorizando la solicitud y que detalle claramente los tipos de permiso y sistemas a los que está otorgando el visto bueno.</p>
(20) Sello	<i>Estampar el sello de la dependencia.</i>

### 4- Recepción de solicitud

- a. Entrega Formulario para Solicitudes para producción en la Unidad de Soporte Técnico de la DTIC; serán verificados los datos consignados por el usuario; para corroborar que el formulario esté completo y los datos correspondan a la información solicitada.
- b. El encargado le asigna un consecutivo para que el usuario pueda dar seguimiento si así lo desea y le indica al solicitante los plazos máximos de entrega:
  - Cuenta de correo electrónico: 2 días hábiles
  - Usuario AS/400: 4 días hábiles
- c. El solicitante debe presentarse a la Unidad de Soporte Técnico con la cédula de identidad para <sup>24</sup>retirar el usuario de correo electrónico y de AS/400.

<sup>24</sup>Si la solicitud es de AS/400 y el funcionario ya cuenta con correo institucional, recibirá las credenciales por medio de correo electrónico.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 5- Datos de recibido

DATOS DE RECIBIDO	
(21) Nombre Completo: _____	(22) Firma: _____

(21) *Nombre completo* El solicitante retira el documento donde se indica el usuario y contraseña deberá escribir su nombre como comprobante de recibido.

(22) *Firma* El solicitante debe firmar la boleta como comprobante de recibido.

## 6- Solicitud de Creación de Usuarios para Centros Universitarios

En caso que el solicitante sea de Centros Universitarios, para solicitar creación de una cuenta de correo electrónico o la creación de usuario AS/400, deberá solicitar la boleta de creación de usuarios al correo electrónico [solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr) o descargarla de la página de la DTIC en la siguiente dirección:

<http://www.uned.ac.cr/dtic/documentos#formularios>

Igualmente, para la entrega del formulario se deberá enviar la boleta debidamente llena y escaneada a la dirección de correo electrónico de Soporte Técnico

([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)).

Cuando la solicitud sea atendida por parte de la DTIC (UST), se le notificará por medio de correo electrónico al encargado o asistente del CeU, el usuario y la contraseña para que le sea entregada la información al solicitante; el destinatario deberá responder por medio de correo electrónico ([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)) que recibió satisfactoriamente la información.

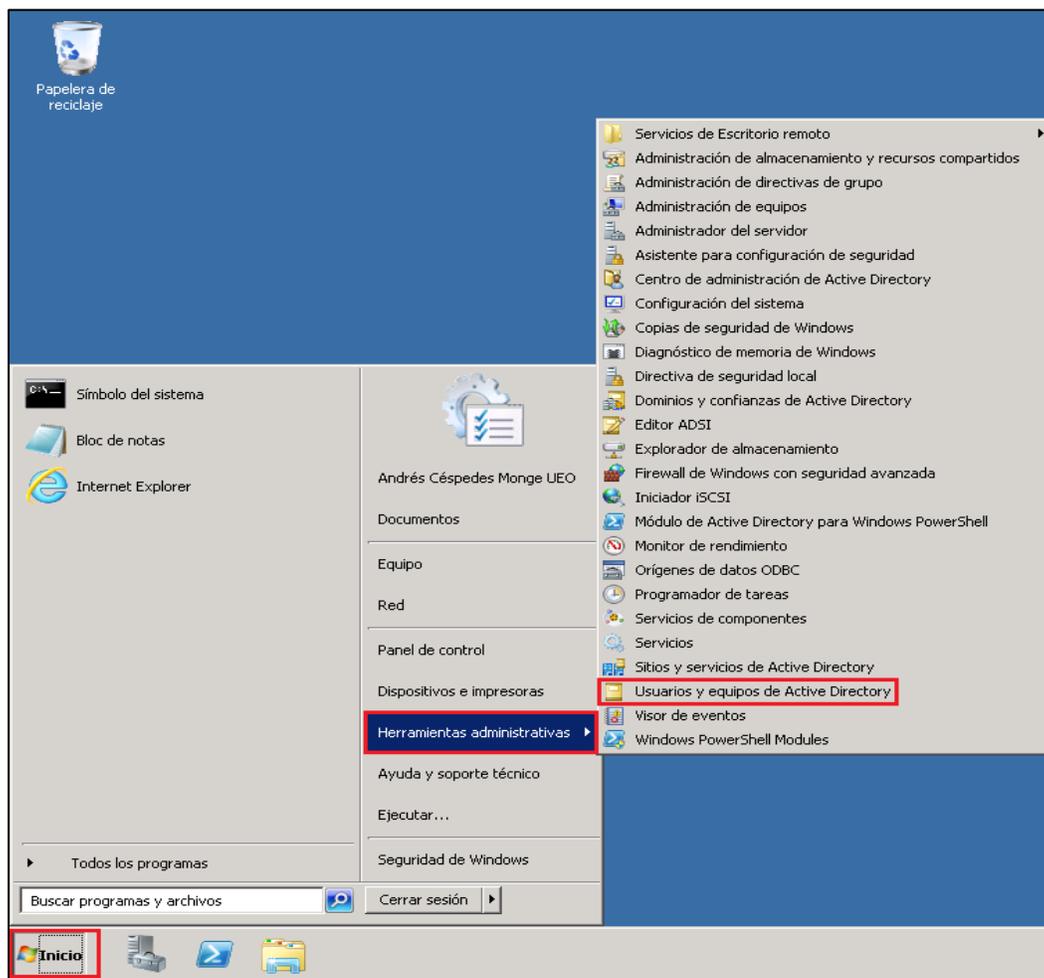
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 7- Inhabilitar cuentas de usuario

*(Cuenta de correo electrónico Office 365, código de usuario para los equipos de cómputo, dispositivos tecnológicos y acceso a la red institucional)*

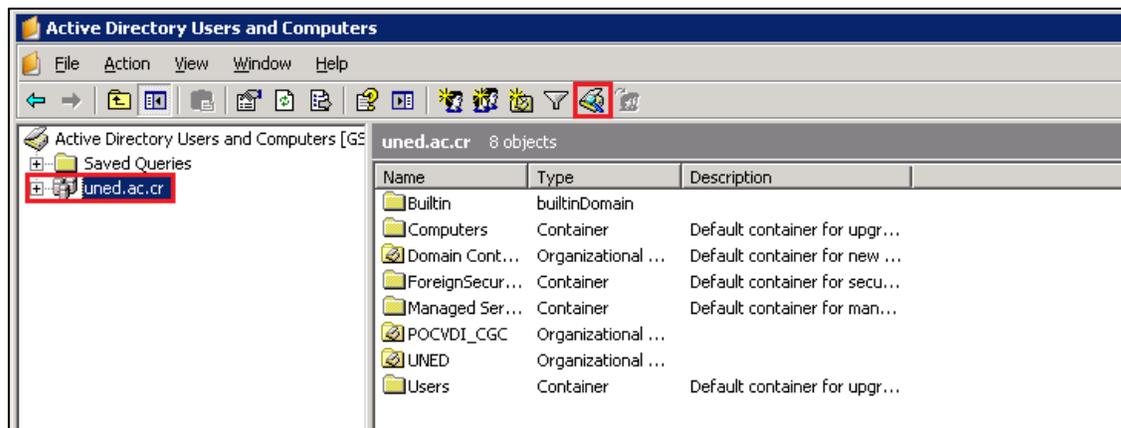
Para proceder a deshabilitar cuentas de usuarios se debe contar con un documento oficial (cese de funciones, defunción, jubilación, entre otros) de Recursos Humanos o un comunicado por correo electrónico del jefe o director dela dependencia que solicite.

1. Una vez recibida la solicitud con su respectivo visto bueno, se deberá ingresar al servidor que tenga el rol de Active Directory. Una vez en el equipo se debe presionar el botón de **Inicio**. buscar la opción **Herramientas Administrativas** y en **Usuarios y Equipos de Active Directory**, dar **Clic**.

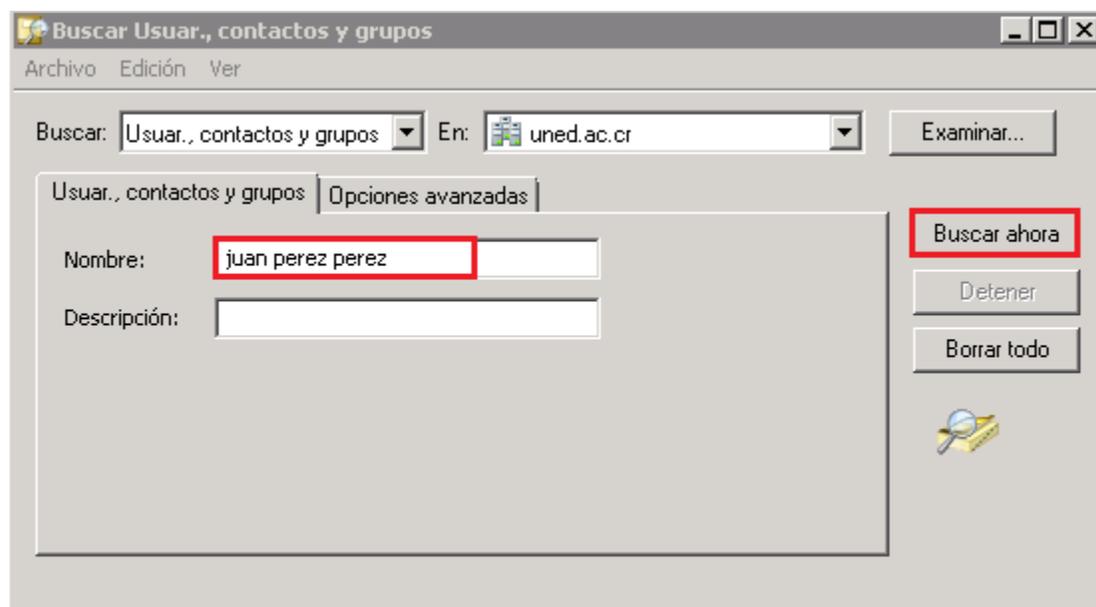


 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

- Se abre la pantalla **Active Directory Users and Computers** donde se selecciona el dominio “**uned.ac.cr**”, luego presionamos la opción de buscar usuarios.

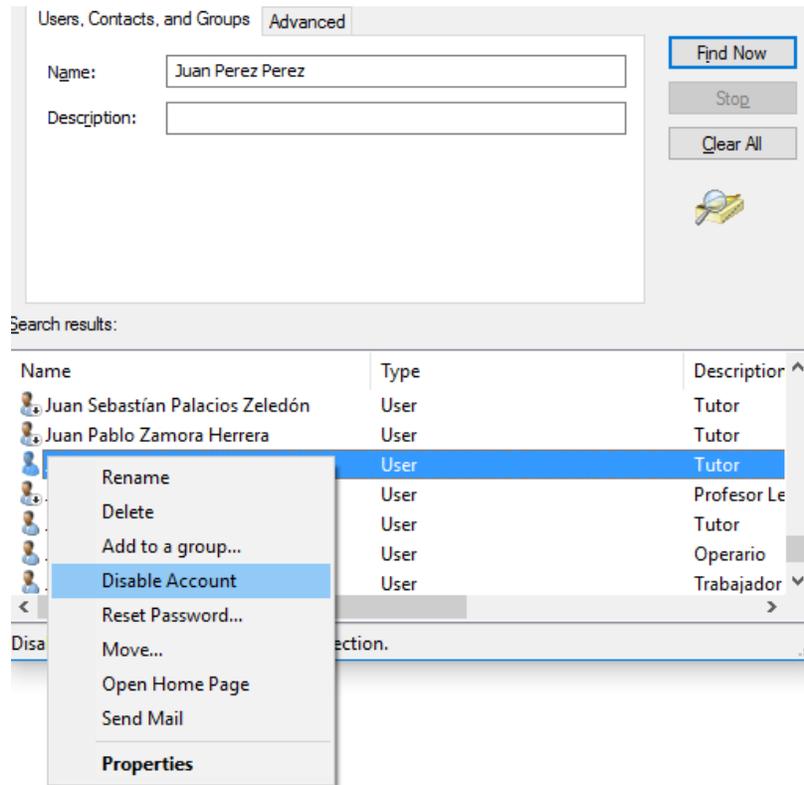


- En la ventana **Buscar Usuar, contactos y grupos**, en el campo llamado **Nombres** e ingresa el nombre del funcionario o persona al cual se le va a deshabilitar el usuario y se presiona la opción de **buscar ahora**.

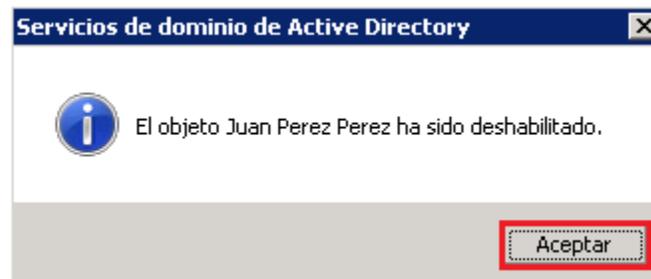


	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. Sobre esa pantalla aparecerá el usuario que se está buscando y sobre el usuario se presiona clic derecho para que aparezcan las opciones de usuario, se selecciona **“Deshabilitar Cuenta (Disable Account)”**.

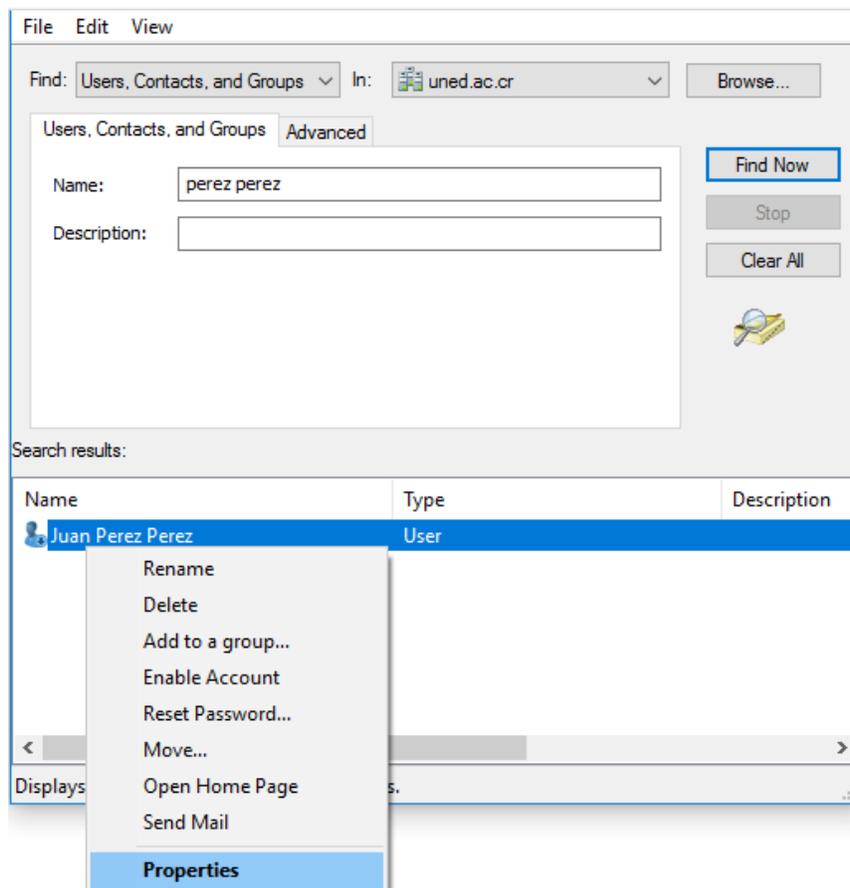


5. Luego de esto saldrá un mensaje comunicando que la cuenta se desactivo y se presiona Aceptar.



 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

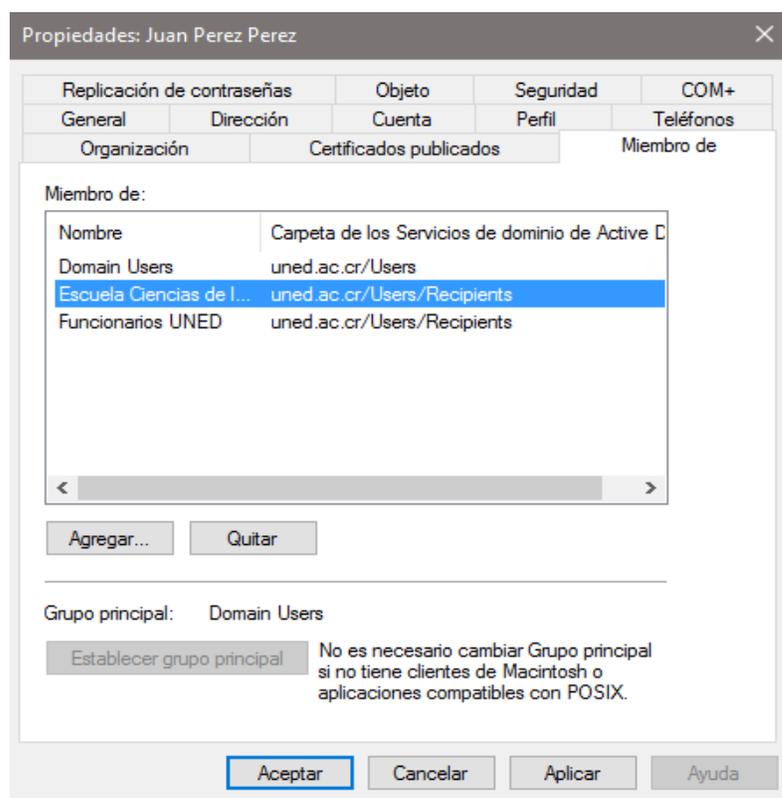
6. Una vez deshabilitada la cuenta, debe dar clic derecho nuevamente sobre el usuario y seleccionar “Propiedades (Properties)”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

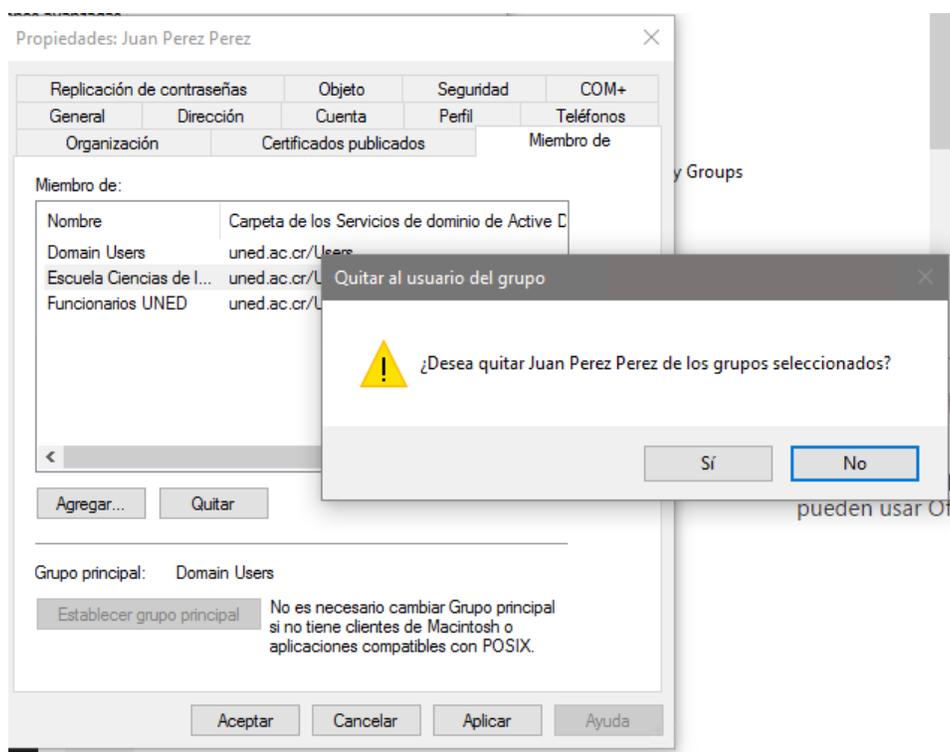
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

7. Sobre esa pantalla aparecerá las propiedades del usuario y debe dar clic sobre la pestaña “**Miembro de**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

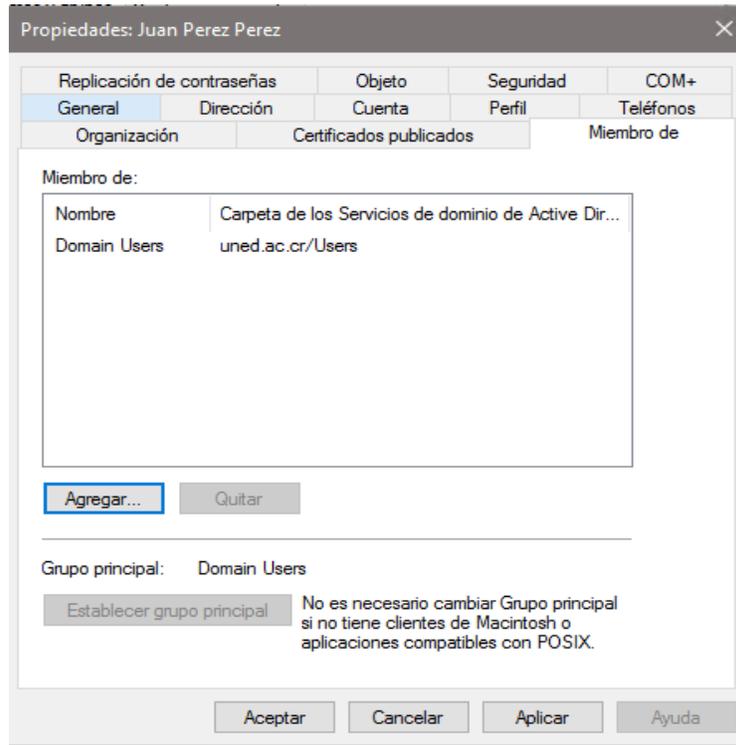
8. Ubicado en la pestaña “**Miembro de**” debe seleccionar cada uno de los grupos y dar clic al botón “**Quitar**”, el sistema le consultará si desea quitar al usuario de los grupos seleccionados, para lo cual debe dar clic al botón “**Sí**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

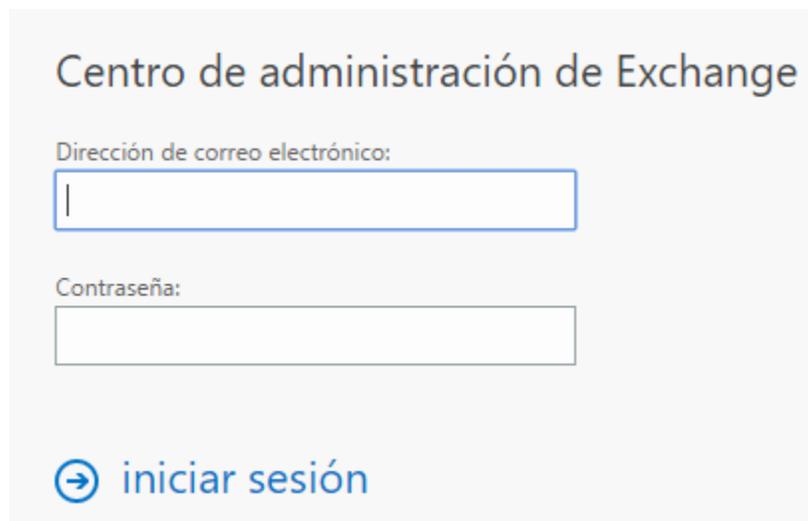
9. En la pestaña “Miembro de” debe asegurarse que el usuario deshabilitado solo quede incluido en el grupo de “**Domain Users**”. Posteriormente se da clic al botón **Aceptar**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

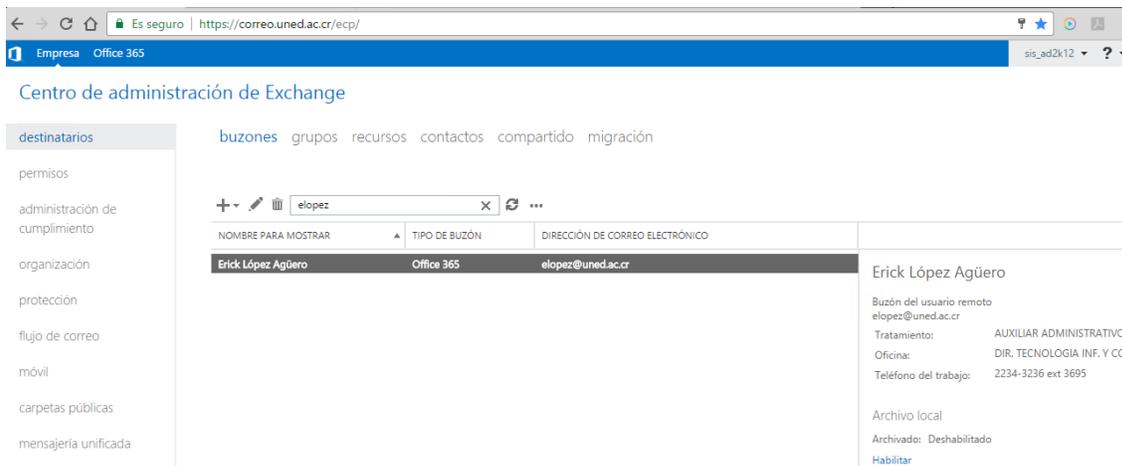


	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

10. Una vez deshabilitado el usuario y excluido de los grupos al cual pertenecía, se procede a quitar el usuario de la **lista de direcciones**. Se debe ingresar al Centro de Administración de Exchange: <https://correo.uned.ac.cr/ecp/>.



11. En la opción del Menú **“destinatarios”** debe digitar el usuario deshabilitado, y presionar el botón de **“Enter”**, esto con el fin de filtrar la lista de destinatarios. Debe dar doble clic sobre el nombre del funcionario deshabilitado.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

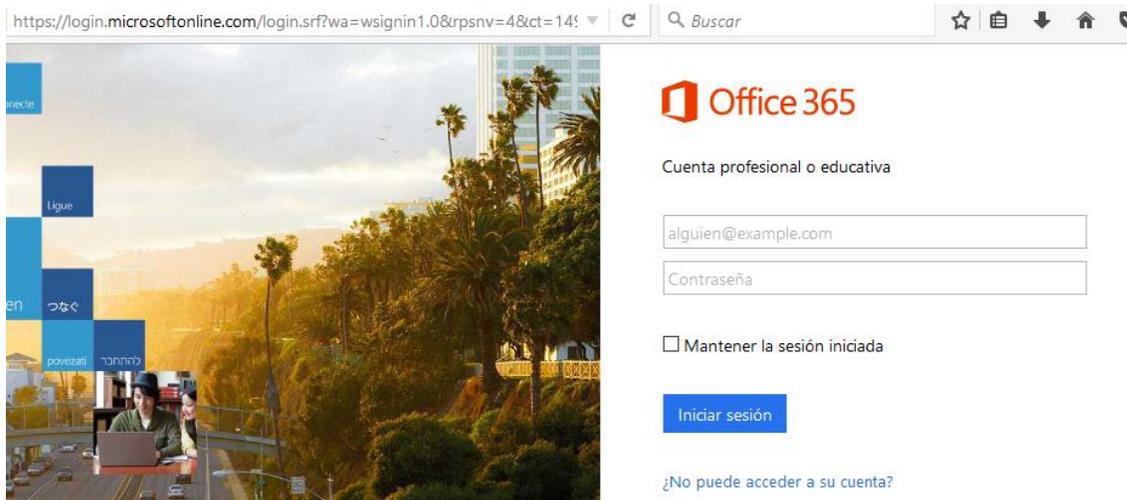
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

12. Al dar doble clic sobre el nombre del funcionario deshabilitado, se abre una pantalla con propiedades del usuario, debe deseleccionar la opción “**Ocultar de las listas de direcciones**”. Después debe presionar el botón “guardar”.

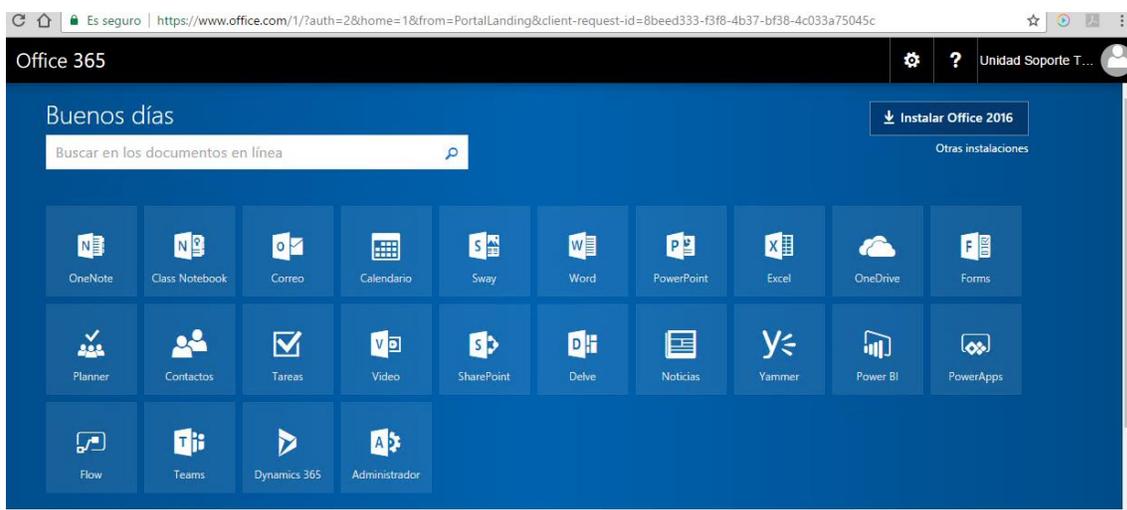
The screenshot shows the 'EditRemoteMailbox' page in Google Chrome. The user's name is Erick López Agüero. The 'General' tab is active, showing contact information fields: Nombre (Erick), Iniciales, Apellidos (López Agüero), \*Nombre (Erick López Agüero), and \*Nombre para mostrar (Erick López Agüero). The login name is elopez@uned.ac.cr. There are two checkboxes: 'Pedir el cambio de contraseña en el siguiente inicio de sesión' (unchecked) and 'Ocultar de las listas de direcciones' (checked). A tooltip points to the checked checkbox with the text: 'Si seleccionas esta opción, el usuario no aparecerá en la libreta de direcciones de tu organización ni en otras listas de direcciones, pero seguirá recibiendo el correo enviado a él.' At the bottom, there are 'guardar' and 'cancelar' buttons.

13. Como último paso se debe desactivar la licencia de Office 365, para lo cual se debe ingresar al área de “**Administración de Office 365 de la UNED**”. Una vez ingresado las credenciales debe dar clic al botón de “**Iniciar sesión**”.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



14. En la pantalla de “**Administración de Office 365 de la UNED**”, debe dar clic en la opción de “**Administrador**”.



15. En la pantalla de Administrador “**Admin center**”, debe seleccionar la opción “**Usuarios**” del menú vertical y posicionarse en la opción “**Usuarios activos**”. Ubicado en esta pantalla debe digitar el usuario deshabilitado y presionar el botón de “**Enter**” con el fin de filtrar la lista de usuarios. Una vez ubicado, debe dar doble clic sobre el nombre del usuario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Office 365 Admin center

Inicio > Usuarios activos

Universidad Estatal a Distancia

+ Agregar un... Más Vistas Todos los usuarios elopez Exportar

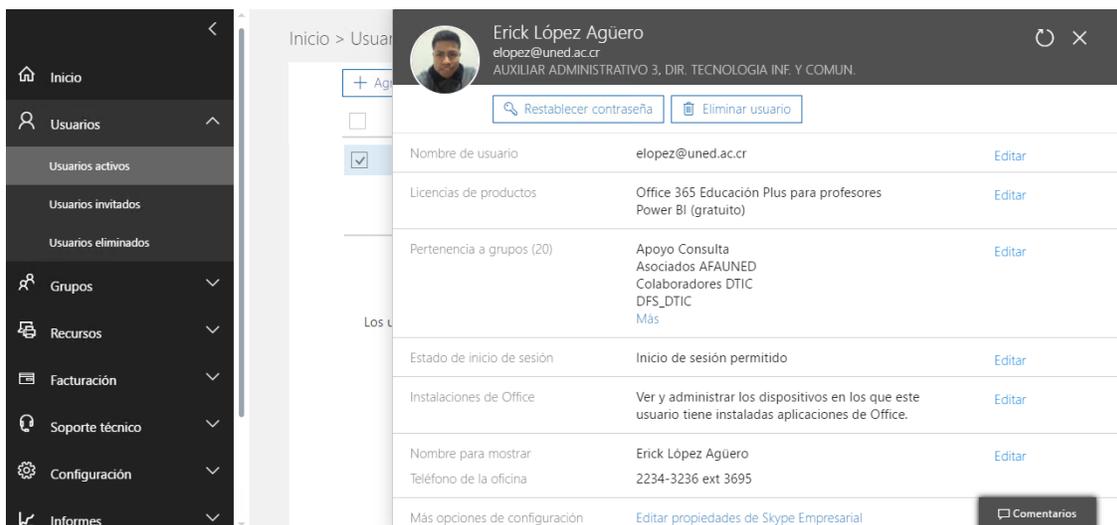
<input type="checkbox"/>	Nombre para mostrar	Nombre de usuario	Estado
<input type="checkbox"/>	Erick López Agüero	elopez@uned.ac.cr	Power BI (gratuito) Office

+ Usuario Tipos de usuarios Filtr

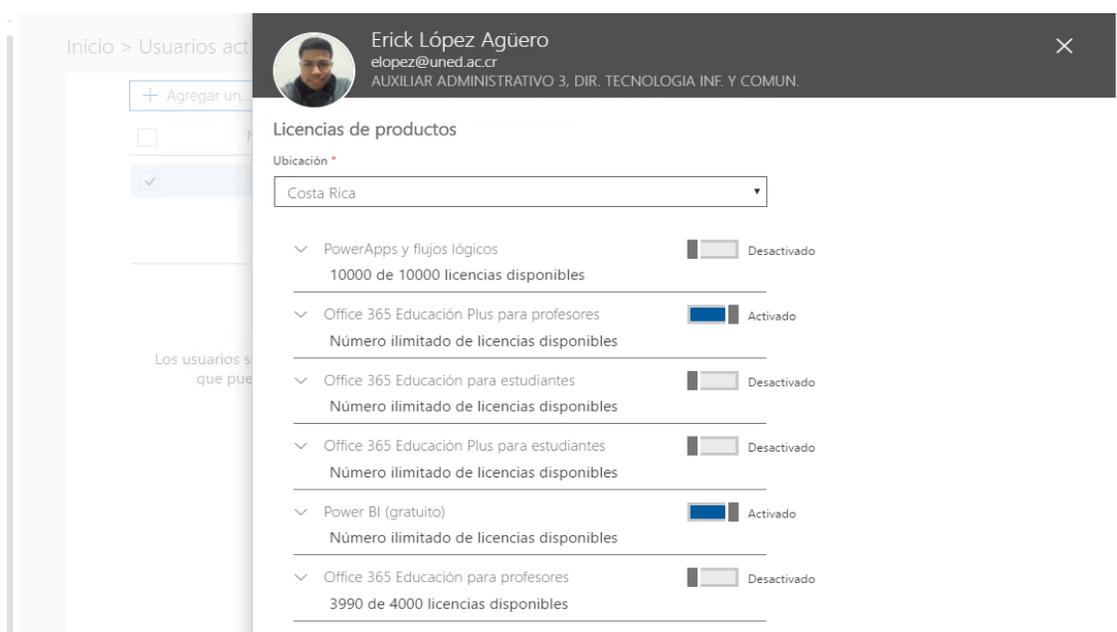
Los usuarios son personas de su organización que pueden acceder a Office 365. Diferentes tipos de usuarios y cuentas pueden usar Office 365 de formas distintas. Descubra cómo los filtros mantienen esta lista bajo control.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

16. Al dar doble clic sobre el nombre se carga las propiedades de Office 365 del usuario deshabilitado. Debe dar clic al enlace **“Editar”** de la opción **“Licencias de productos”**.

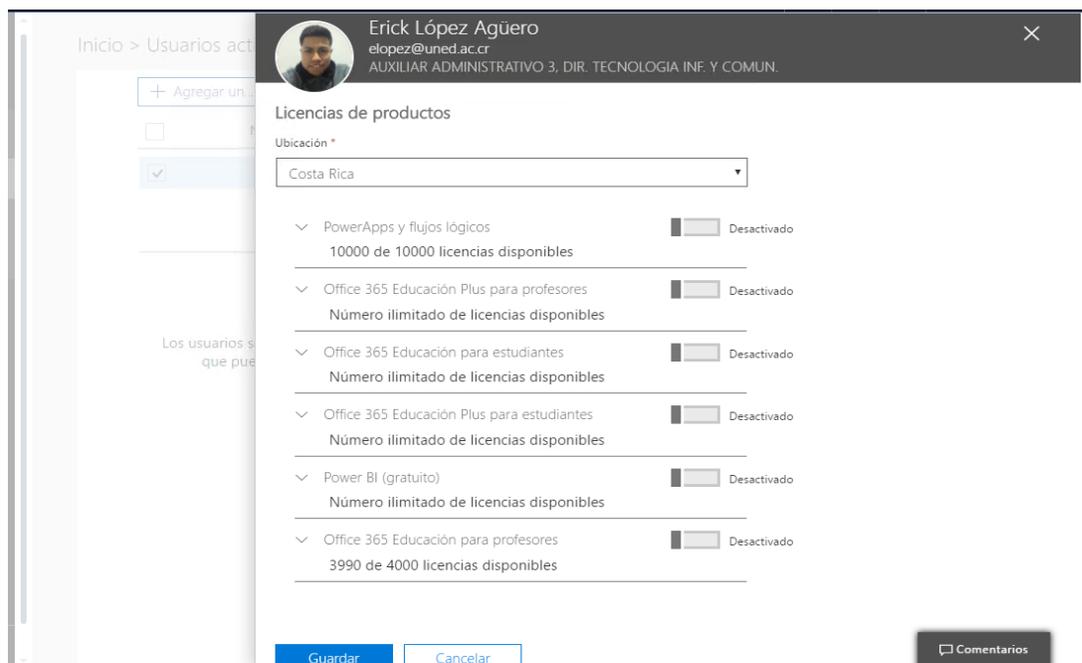


17. En la pantalla de **“Licencias de productos”**, debe desactivar las licencias **“Office 365 Educación Plus para profesores”** y **“Power BI (gratuito)”**.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

18. La pantalla de “**Licencias de productos**” debe quedar de la siguiente forma. Posteriormente debe dar clic al botón “**Guardar**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

**Instructivo para el trámite de solicitud de códigos de usuarios Institucional  
(Cuenta de Correo electrónico Office 365, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional)**

**¿En qué consisten las solicitudes de usuarios?**

Es la gestión entorno a los usuarios de cada uno de los colaboradores de la institución, tanto en la sede central como en los centros universitarios. Se basa en la atención de solicitudes de creación de cuentas de usuarios para el sistema de correo electrónico en la nube Office 365, para ingresar a los equipos de cómputo, así como para los dispositivos tecnológicos y acceso a la red institucional.

**Conceptos**

- **Boleta Código de Usuarios** -*Formulario: Solicitudes códigos de usuarios:* Instrumento para solicitar el correo electrónico en la nube Office 365 y sus respectivos accesos, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional.

**Para la ejecución de las actividades se debe tener en cuenta lo siguiente**

1. La DTIC tendrá un plazo de 2 días para crear y autorizar dichos usuarios.

**Actividades para realizar el trámite de solicitudes de códigos de usuarios**

1. Completar el Formulario Solicitud de Código de usuarios, de conformidad con lo establecido en este instructivo.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



Universidad Estatal a Distancia  
 Rectoría  
 Dirección de Tecnología  
 Información y Comunicaciones



### SOLICITUD CODIGOS DE USUARIOS



Fecha: \_\_\_\_\_

<b>Nombre del solicitante:</b> _____		<b>Cédula:</b> _____	
<b>El solicitante es:</b> <input type="checkbox"/> Administrativo <input type="checkbox"/> Profesional <input type="checkbox"/> Investigador <input type="checkbox"/> Docente		<b>Teléfono Oficina:</b> _____ _____	
<b>Dependencia:</b> _____ <b>Puesto:</b> _____		<b>Condición del Funcionario:</b> <input type="checkbox"/> Propiedad <input type="checkbox"/> A plazo hasta _____	
<b>Autorización del Director de la Escuela o Jefe inmediato</b>			
<b>Nombre Completo:</b> _____		<b>Firma:</b> _____	
<b>Nº de cédula:</b> _____			
<p>El funcionario de la UNED al firmar esta solicitud se hace responsable por los daños que se ocasione a la UNED, personal o entidad externa, por el mal uso de este código. Este código es de uso personal y el funcionario debe cumplir con el Reglamento para Uso de Equipos de Cómputo e Internet de la UNED, aprobado por el Consejo Universitario en sesión N°2336, Art. II, inciso 2-a) del 15 de mayo del 2014 y cualquier otra normativa que le resulte aplicable.          Este reglamento lo debe consultar en: <a href="http://www.uned.ac.cr/reglamento/">http://www.uned.ac.cr/reglamento/</a></p>			
<b>Para uso de la DTIC</b>			
<b>Realizado por:</b> _____ V°B° Director		<b>Código asignado:</b> _____	
<b>Observaciones:</b> _____ _____ _____		<b>Password inicial (contraseña):</b> _____	
		<b>Firma de Recibido:</b> _____	
		Verificación de cédula	

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 1- Datos del solicitante

Fecha: \_\_\_\_\_

<b>Nombre del solicitante:</b> _____	<b>Cédula:</b> _____
<b>El solicitante es:</b> <input type="checkbox"/> Administrativo <input type="checkbox"/> Profesional <input type="checkbox"/> Investigador <input type="checkbox"/> Docente	<b>Teléfono Oficina:</b> _____
<b>Dependencia:</b> _____ <b>Puesto:</b> _____	<b>Condición del Funcionario:</b> <input type="checkbox"/> Propiedad <input type="checkbox"/> A plazo hasta _____

(1) <i>Fecha de Solicitud:</i>	Debe indicarla fecha en la que se solicita la creación del usuario.
(2) <i>Nombre solicitante:</i>	Indicar el nombre completo del solicitante, que requiere la creación del usuario.
(3) <b>Es solicitante es:</b>	Se debe marcar el tipo de puesto que desempeña el solicitante. (Administrativo, Profesional, Docente, Investigador)
(4) <b>Dependencia:</b>	Indicar la dependencia a la cual pertenece el solicitante
(5) <b>Puesto:</b>	Especificar el nombre del puesto que desempeña
(6) <b>Cédula:</b>	Anotar el número de cédula en formato 00-000-000.
(7) <b>Teléfono Oficina:</b>	El solicitante debe indicar los números de teléfono en el cual puede ser contactado.
(8) <b>Condición del Funcionario:</b>	Se debe indicar la condición del solicitante, en propiedad o A plazo. En el caso que seleccione A plazo, debe indicar hasta que día esta su nombramiento.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 2- Autorización del Director de la Escuela o Jefe Inmediato

<b>Autorización del Director de la Escuela o Jefe inmediato</b>	
Nombre Completo: _____	Firma: _____
Nº de cédula: _____	

(9) Nombre Completo	Indicar el nombre completo de la jefatura inmediata
(10) Cédula	Indicar el número de cédula de la jefatura inmediata; en formato 00-0000-0000.
(11) Firma	La firma de la jefatura inmediata constituye la aprobación de la solicitud y es un elemento indispensable para tramitar la misma.

## 3- Recepción de solicitud

Entrega la Solicitud de códigos de usuarios, en la Unidad de Soporte Técnico de la DTIC; serán verificados los datos consignados por el usuario; para corroborar que el formulario esté completo y los datos correspondan a la información solicitada.

El encargado le asigna un consecutivo para que el usuario pueda dar seguimiento si así lo desea y le indica al solicitante los plazos máximos de entrega:

- Cuenta de correo electrónico: 2 días hábiles

Transcurrido el tiempo de entrega, el solicitante deberá presentarse a la *Unidad de Soporte Técnico* con la cédula de identidad para retirar el usuario de correo electrónico.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

#### 4- Datos de recibido

<b>Código asignado:</b> _____
<b>Password inicial (contraseña):</b> _____
<b>Firma de Recibido:</b>
Verificación de cédula

(12) *Firma de Recibido* El solicitante debe firmar la boleta como comprobante de recibido.

(13) *Verificación de cédula* El solicitante debe anotar la cédula en el formulario y mostrar la cedula física al personal de recepción de la DTIC, con el fin que se pueda comprobar que es la misma cédula suministrada.

#### 5- Solicitud de Creación de Usuarios para Centros Universitarios

En caso que el solicitante sea de Centros Universitarios, para solicitar creación de una cuenta de correo electrónico, deberá solicitar la boleta de creación de usuarios al correo electrónico [solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr) o descargarla de la página de la DTIC en la siguiente dirección: <http://www.uned.ac.cr/dtic/documentos#formularios>

Igualmente, para la entrega del formulario se deberá enviar la boleta debidamente llena y escaneada a la dirección de correo electrónico de Soporte Técnico

([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)).

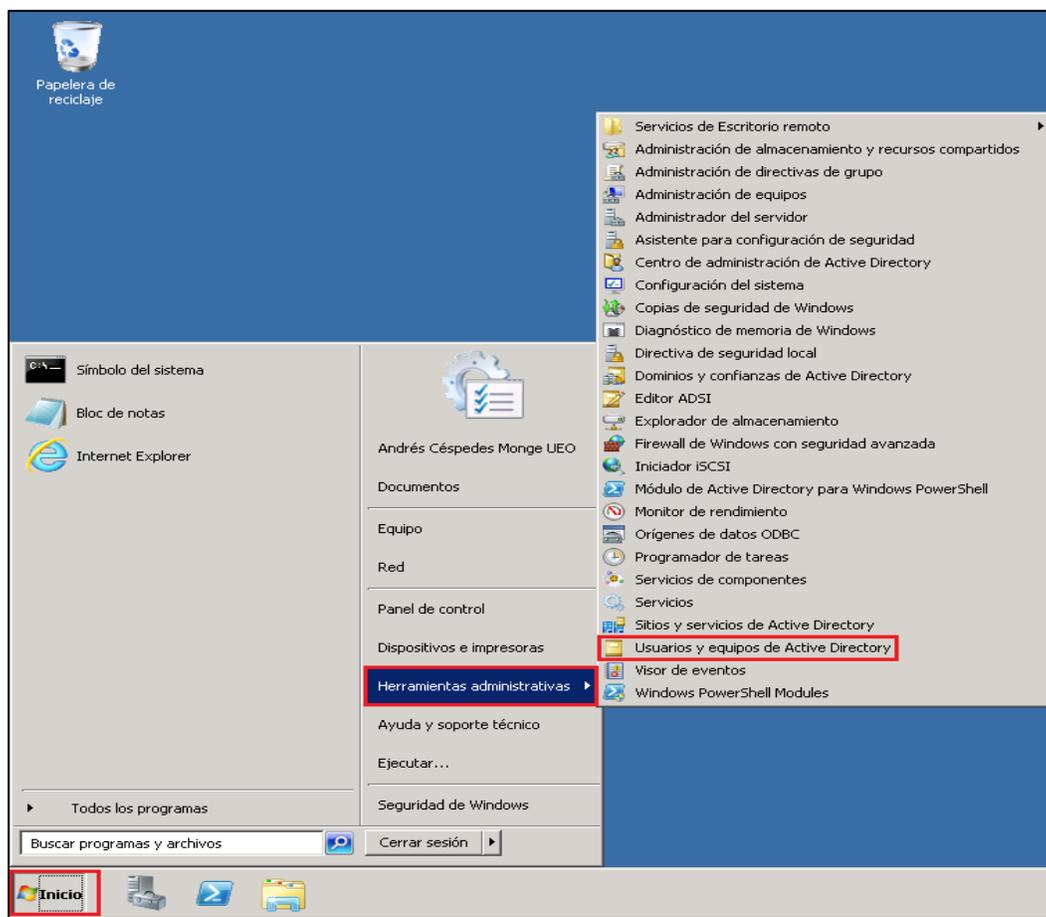
Cuando la solicitud sea atendida por parte de la DTIC (UST), se le notificará por medio de correo electrónico al encargado o asistente del CeU, el usuario y la contraseña para que le sea entregada la información al solicitante; el destinatario deberá responder por medio de correo electrónico ([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)) que recibió satisfactoriamente la información.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 6- Inhabilitar cuentas de usuario (Cuenta de correo electrónico Office 365, código de usuario para los equipos de cómputo, dispositivos tecnológicos y acceso a la red institucional)

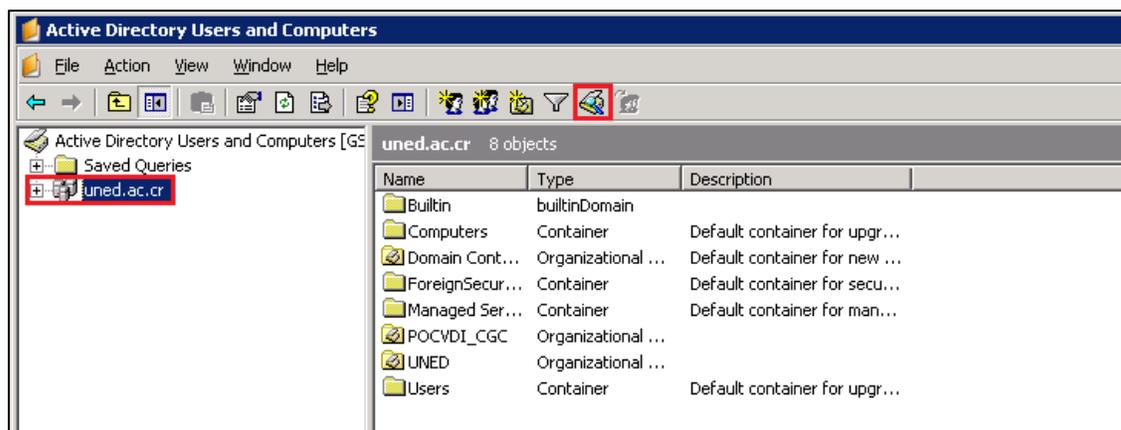
Para proceder a deshabilitar cuentas de usuarios se debe contar con un documento oficial (cese de funciones, defunción, jubilación, entre otros) de Recursos Humanos o un comunicado por correo electrónico del jefe o director dela dependencia que solicite.

1. Una vez recibida la solicitud con su respectivo visto bueno, se deberá ingresar al servidor que tenga el rol de Active Directory. Una vez en el equipo se debe presionar el botón de **Inicio**. buscar la opción **Herramientas Administrativas** y en **Usuarios y Equipos de Active Directory**, dar **Clic**.

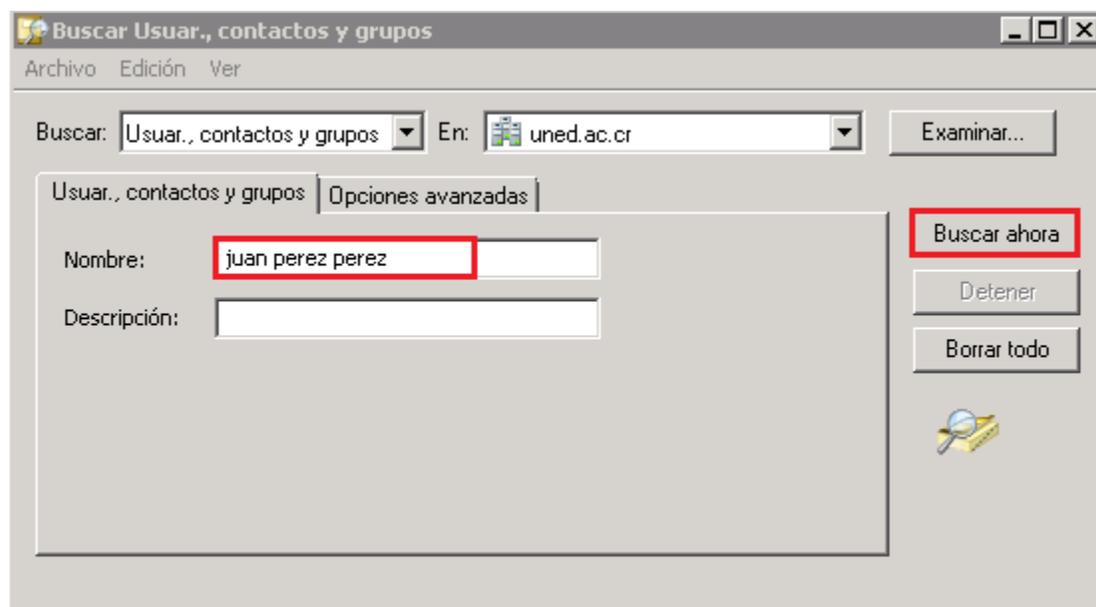


 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

- Se abre la pantalla **Active Directory Users and Computers** donde se selecciona el dominio “**uned.ac.cr**”, luego presionamos la opción de buscar usuarios.

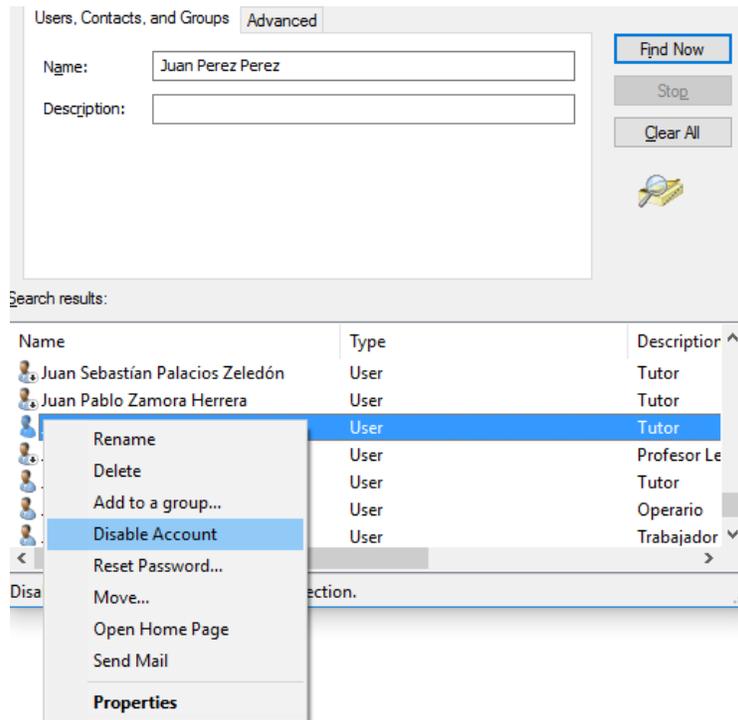


- En la ventana **Buscar Usuar, contactos y grupos**, en el campo llamado **Nombre** se ingresa el nombre del funcionario o persona al cual se le va deshabilitar el usuario y se presiona la opción de **buscar ahora**.

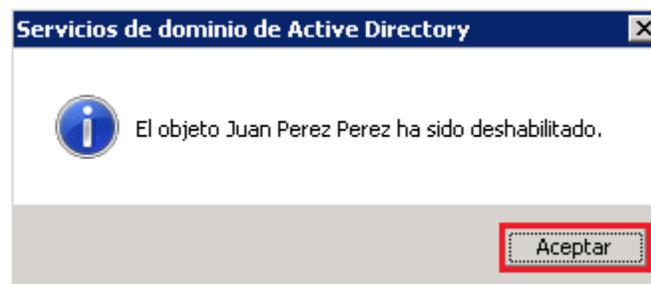


	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. Sobre esa pantalla aparecerá el usuario que se está buscando y sobre el usuario se presiona clic derecho para que aparezcan las opciones de usuario, se selecciona **“Deshabilitar Cuenta (Disable Account)”**,

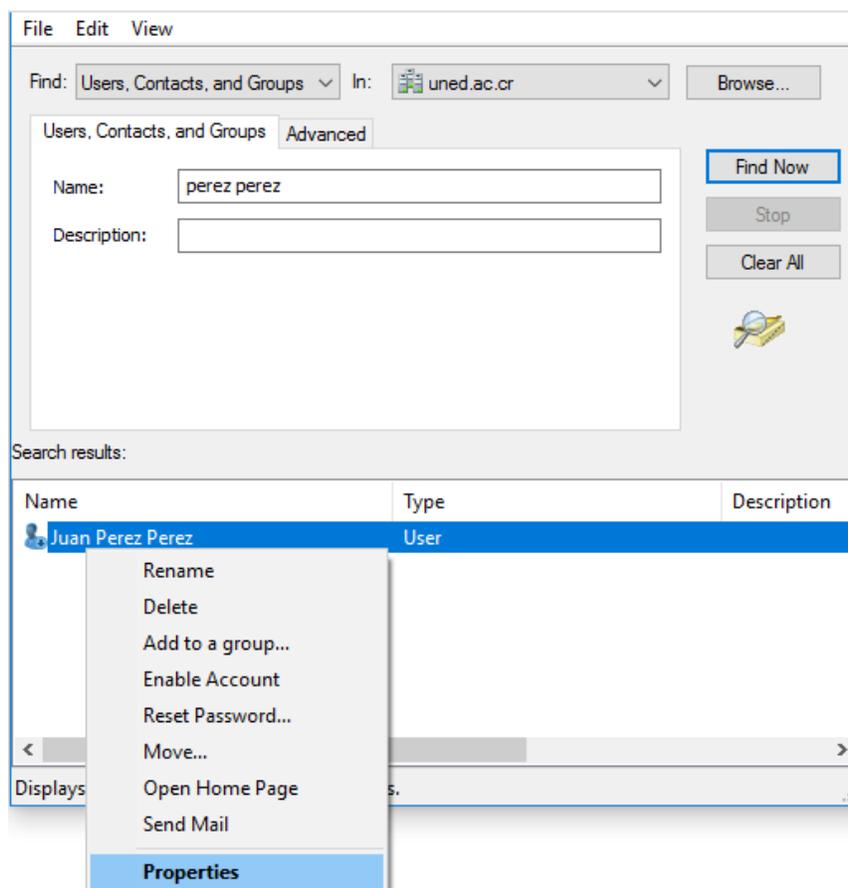


5. Luego de esto saldrá un mensaje comunicando que la cuenta se desactivo y se presiona Aceptar.



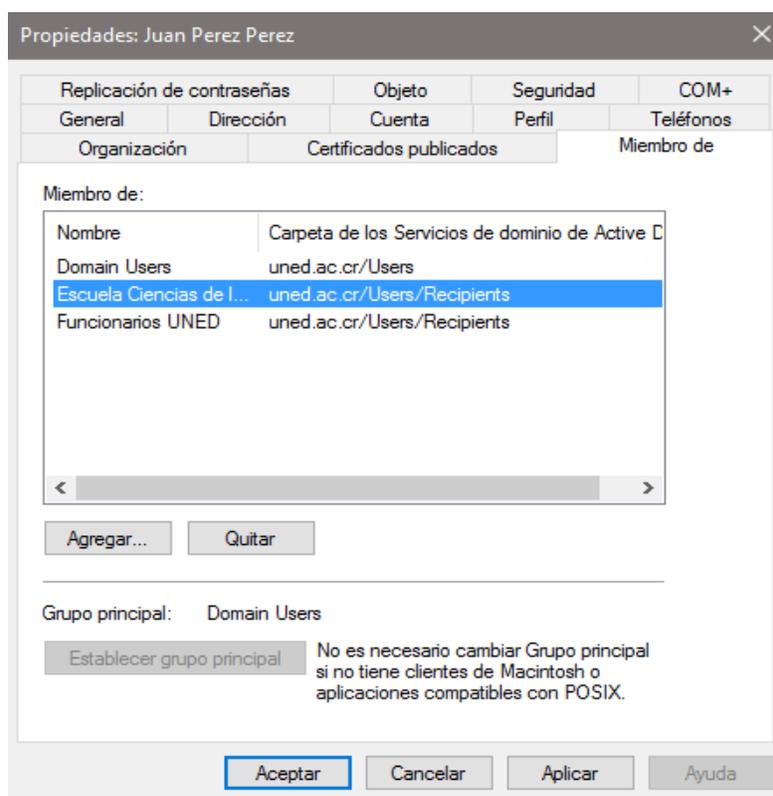
 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

6. Una vez deshabilitada la cuenta, debe dar clic derecho nuevamente sobre el usuario y seleccionar “Propiedades (Properties)”.



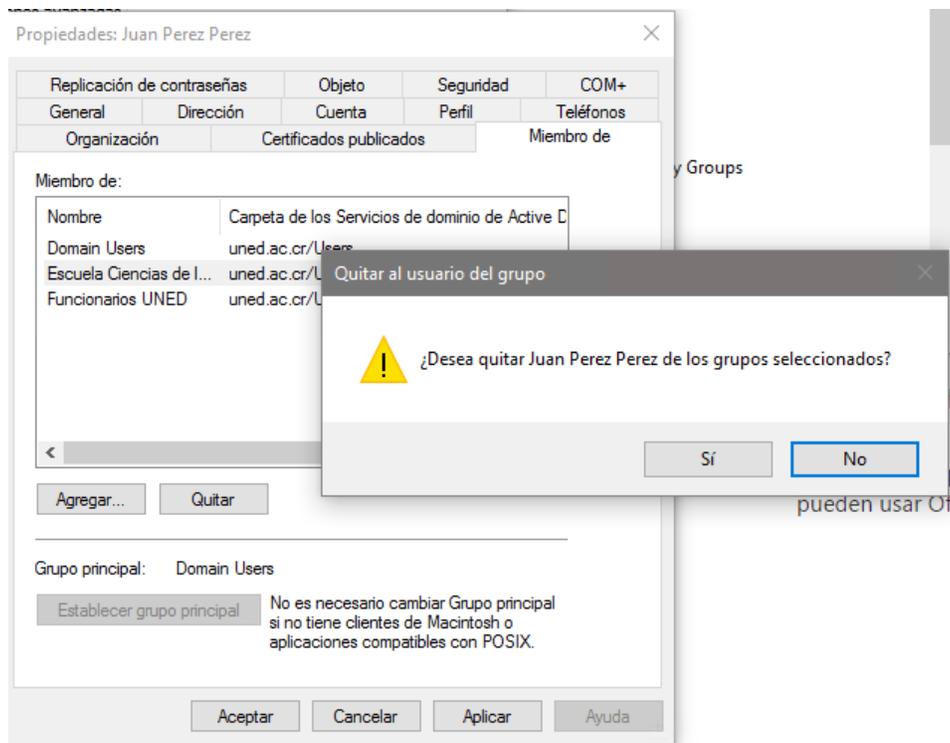
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

7. Sobre esa pantalla aparecerá las propiedades del usuario y debe dar clic sobre la pestaña “**Miembro de**”.



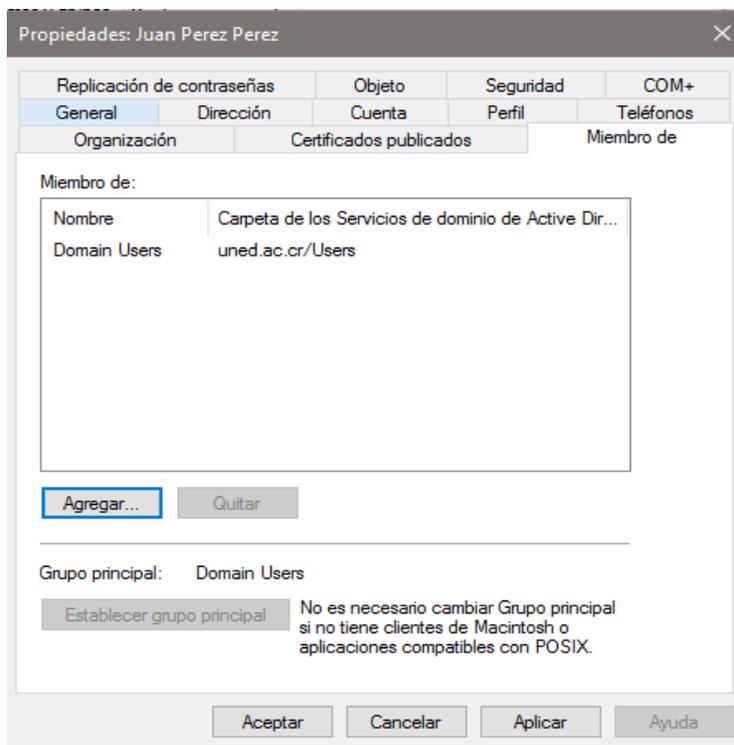
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

8. Ubicado en la pestaña “**Miembro de**” debe seleccionar cada uno de los grupos y dar clic al botón “**Quitar**”, el sistema le consultará si desea quitar al usuario de los grupos seleccionados, para lo cual debe dar clic al botón “**Sí**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

9. En la pestaña “Miembro de” debe asegurarse que el usuario deshabilitado solo quede incluido en el grupo de “**Domain Users**”. Posteriormente se da clic al botón **Aceptar**.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

10. Una vez deshabilitado el usuario y excluido de los grupos al cual pertenecía, se procede a quitar el usuario de la **lista de direcciones**. Se debe ingresar al Centro de Administración de Exchange: <https://correo.uned.ac.cr/ecp/>.

11. En la opción del Menú **“destinatarios”** debe digitar el usuario deshabilitado, y presionar el botón de **“Enter”**, esto con el fin de filtrar la lista de destinatarios. Debe dar doble clic sobre el nombre del funcionario deshabilitado.

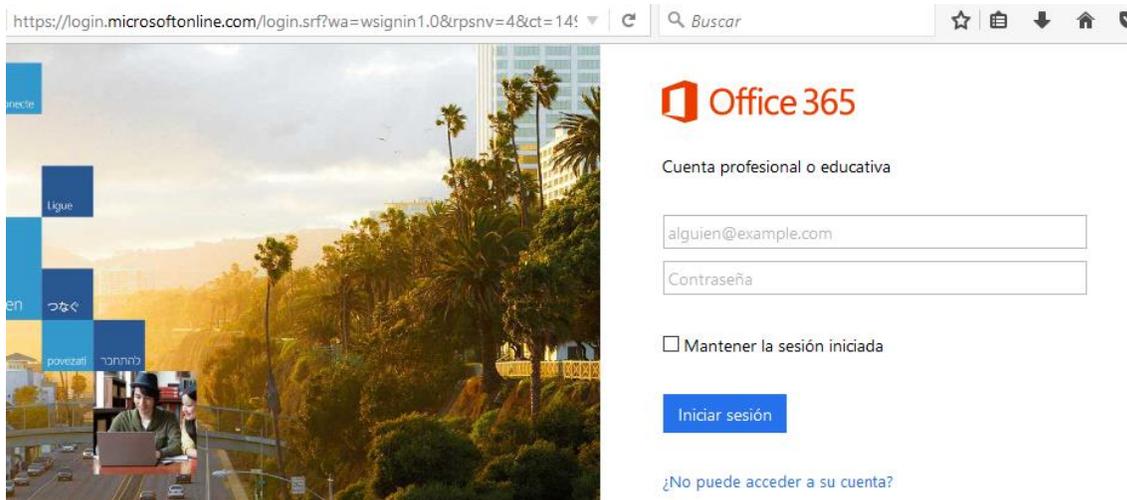
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

12. Al dar doble clic sobre el nombre del funcionario deshabilitado, se abre una pantalla con propiedades del usuario, debe deseleccionar la opción “Ocultar de las listas de direcciones”. Después debe presionar el botón “guardar”.

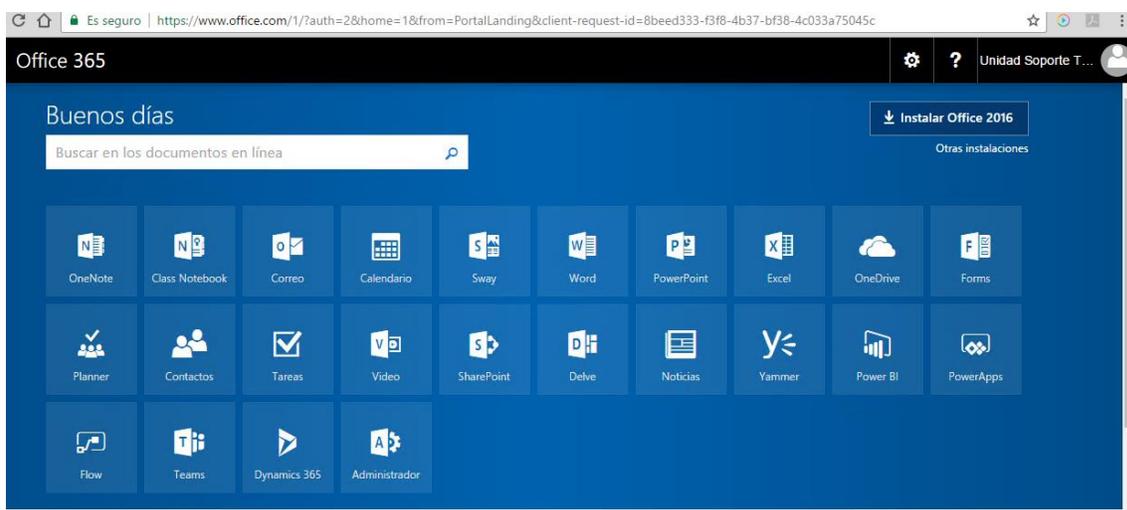
The screenshot shows the 'Edit Remote Mailbox' page for Erick López Agüero. The 'General' section is expanded, showing fields for Name (Erick), Initials, Surname (López Agüero), and various name display options. The checkbox 'Ocultar de las listas de direcciones' is checked. A tooltip points to this checkbox with the text: 'Si seleccionas esta opción, el usuario no aparecerá en la libreta de direcciones de tu organización ni en otras listas de direcciones, pero seguirá recibiendo el correo enviado a él.' At the bottom, there are 'guardar' and 'cancelar' buttons.

13. Como último paso se debe desactivar la licencia de Office 365, para lo cual se debe ingresar al área de “**Administración de Office 365 de la UNED**”. Una vez ingresado las credenciales debe dar clic al botón de “**Iniciar sesión**”.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

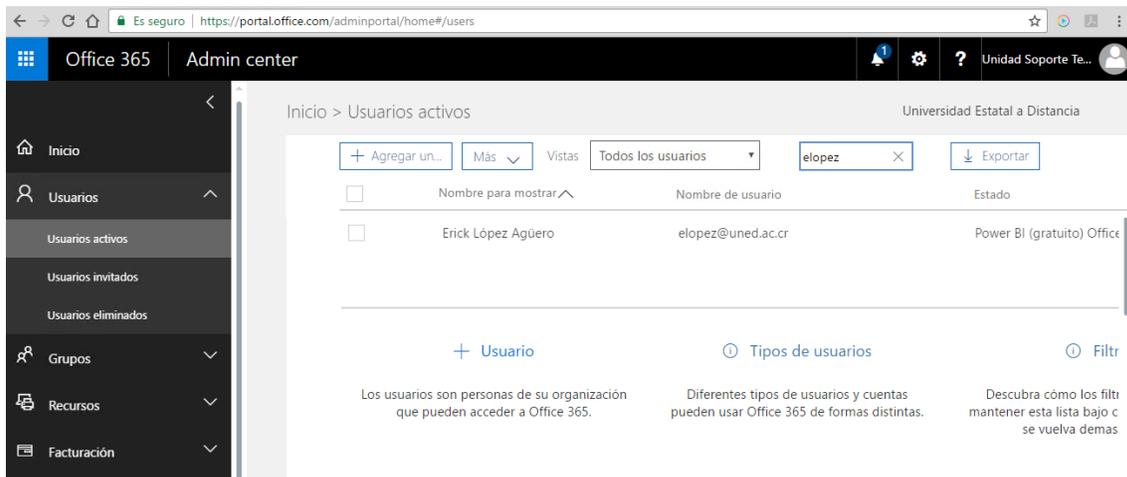


14. En la pantalla de “**Administración de Office 365 de la UNED**”, debe dar clic en la opción de “**Administrador**”.

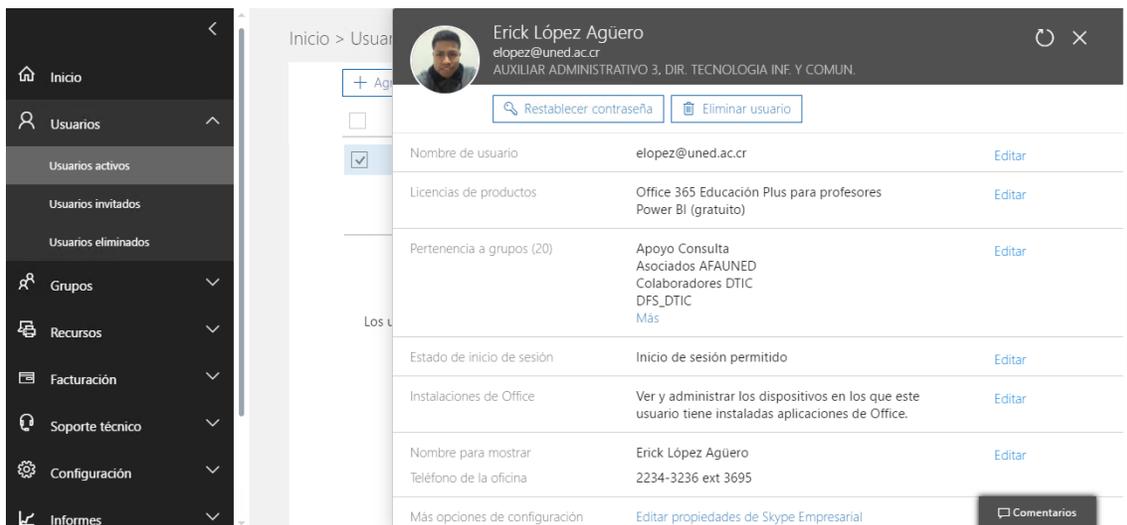


15. En la pantalla de Administrador “**Admin center**”, debe seleccionar la opción “**Usuarios**” del menú vertical y posicionarse en la opción “**Usuarios activos**”. Ubicado en esta pantalla debe digitar el usuario deshabilitado y presionar el botón de “**Enter**” con el fin de filtrar la lista de usuarios. Una vez ubicado, debe dar doble clic sobre el nombre del usuario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

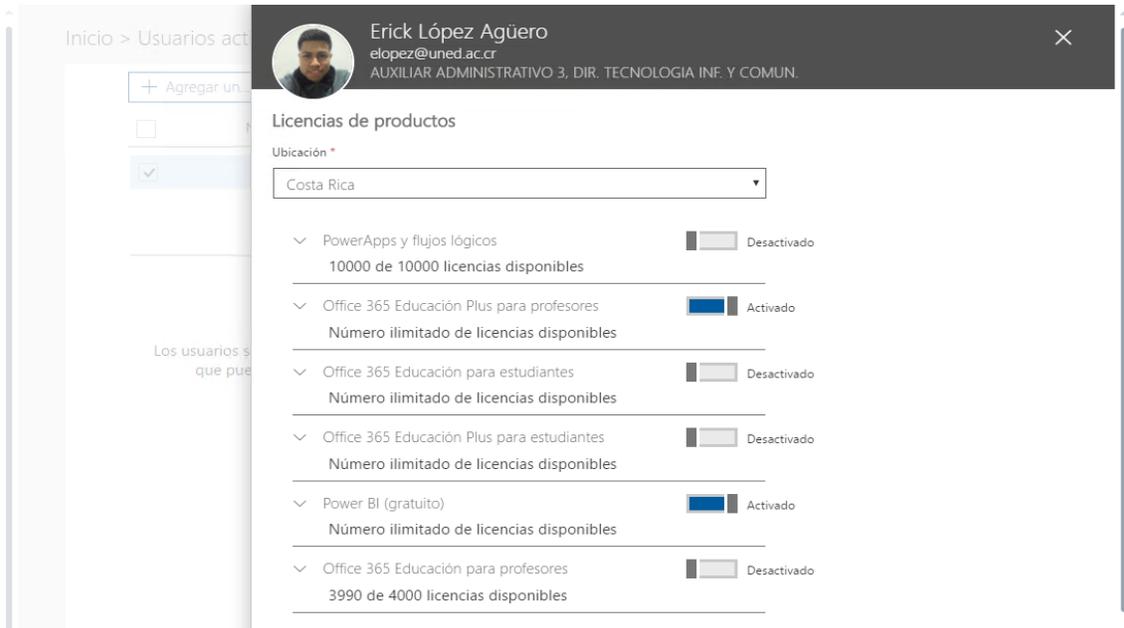


16. Al dar doble clic sobre el nombre se carga las propiedades de Office 365 del usuario deshabilitado. Debe dar clic al enlace **“Editar”** de la opción **“Licencias de productos”**.

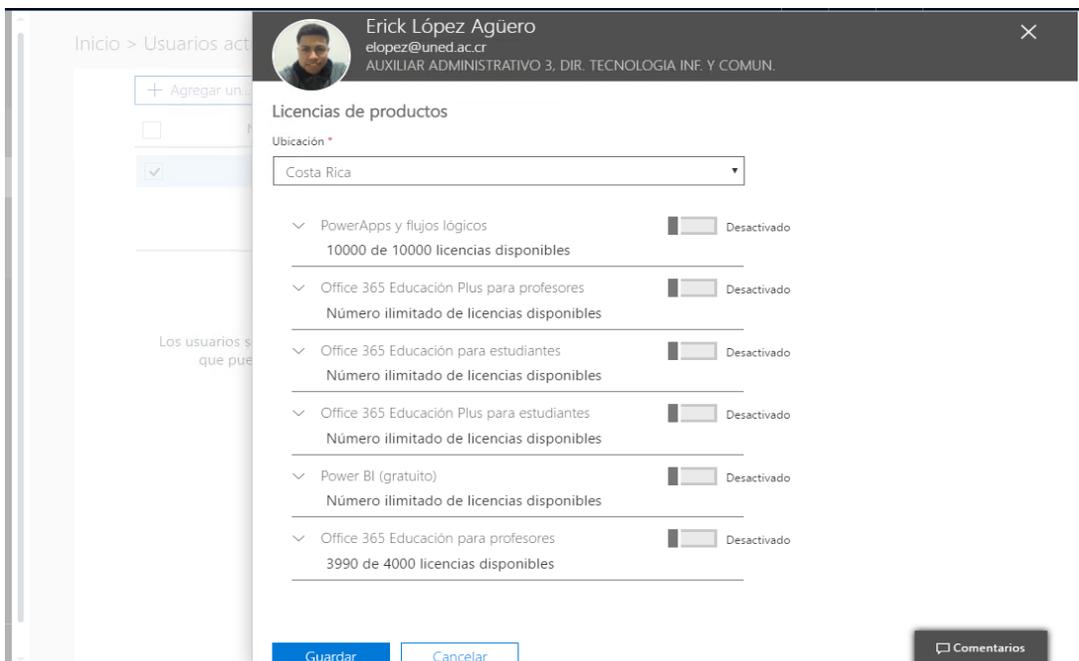


17. En la pantalla de **“Licencias de productos”**, debe desactivar las licencias **“Office 365 Educación Plus para profesores”** y **“Power BI (gratuito)”**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



18. La pantalla de “**Licencias de productos**” debe quedar de la siguiente forma. Posteriormente debe dar clic al botón “**Guardar**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para el trámite de Autorizaciones (Aplicación, VPN, Puerto, Red Social y Otros)

### ¿En qué consiste el trámite de Autorizaciones?

Es la gestión entorno a las autorizaciones que pueden realizar los funcionarios de la institución, así como terceros externos a la UNED, tanto en la sede central como en los centros universitarios. Se basa en la atención de solicitudes de autorización con el fin otorga permisos para el uso de aplicaciones, creación de usuarios de VPN para otorgar acceso remoto a la red institucional, acceso de Redes Sociales, apertura de puertos de red y cualquier otra autorización que se necesite.

### Conceptos

- **Boleta USD-FA-001: Formulario de Autorizaciones:** instrumento para solicitar autorización para el uso de aplicaciones, utilizar redes sociales, otorgar acceso remoto a la red institucional (VPN), acceso a Redes Sociales, apertura de puertos de red, entro otros tipos de autorizaciones.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

1. La solicitud se entrega en la recepción de la DTIC la solicitud.
2. La recepción de la DTIC debe verificar los datos consignados por el usuario; para corroborar que el formulario esté completo y los datos correspondan a la información solicitada, además, se le indica al solicitante los plazos máximos de entrega.
3. Un funcionario de la Unidad de Seguridad Digital le asigna un consecutivo para llevar el control de autorizaciones.
4. Si la solicitud es para un usuario de VPN, el solicitante recibirá las credenciales por medio de correo electrónico.
5. La DTIC tendrá un plazo de 4 días para crear y autorizar el usuario de VPN.
6. En cuanto autorizaciones de aplicaciones, apertura de puertos, acceso a redes sociales y cualquier otro tipo de autorizaciones la DTIC tendrá un plazo de 2 meses para realizar las configuraciones y pruebas necesarias, con el fin de cumplir con el principio de mínimo privilegio y acatar lo que establece el Reglamento para uso de Equipos de cómputo e Internet.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

7. En cuanto a la Solicitud de Autorizaciones para Centros Universitarios,
  - a. El solicitante debe solicitar y completar el formulario de autorizaciones al correo electrónico [solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr) o descargarla de la página de la DTIC en la siguiente dirección: <http://www.uned.ac.cr/dtic/documentos#formularios>
  - b. Enviar la boleta debidamente llena, con las firmas y sello respectivo y escaneada a la dirección de correo electrónico de Soporte Técnico ([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)).
  - c. Cuando la solicitud sea atendida por parte de la DTIC (USD), se le notifica por medio de correo electrónico al solicitante, éste deberá responder por medio de correo electrónico ([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)) que recibió satisfactoriamente la información.
8. En caso de que la solicitud de Autorizaciones de VPN sea para personal <sup>25</sup>externo a la UNED, deberá completar el formulario de autorizaciones “**Boleta USD-FA-001**”.
9. La DTIC (USD), notifica por medio de correo electrónico al responsable de la contratación de personal externo, el cual debe responder por medio de correo electrónico ([solicitudsoporte@uned.ac.cr](mailto:solicitudsoporte@uned.ac.cr)) que recibió satisfactoriamente la información.

### Actividades para realizar el trámite de Autorizaciones

1. Completar el Formulario de autorizaciones, de conformidad con lo establecido en este instructivo.

<sup>25</sup>El cual está realizando algún tipo de actividad contratada por la institución, el funcionario responsable de la contratación deberá llenar y entregar el formulario de autorizaciones en la recepción de la DTIC.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



**Formulario de AUTORIZACIONES**



Fecha de Solicitud:    /    /	
Nombre solicitante: _____	Firma: _____
Teléfonos:            /	Cédula: _____
Dependencia: _____	Puesto: _____
Solicitante es: <input type="radio"/> Administrativo <input type="radio"/> Profesional <input type="radio"/> Docente <input type="radio"/> Investigación	
<b>DETALLE DE LA SOLICITUD (AUTORIZACIÓN)</b>	
<input type="radio"/> Aplicación <input type="radio"/> VPN <input type="radio"/> Puerto <input type="radio"/> Red Social <input type="radio"/> Otro: _____	
Detalle de la Autorización:	
Vigencia del acceso:	
Justificación de la Autorización y la relación con sus labores:	
<b>VISTO BUENO JEFE INMEDIATO</b>	
Nombre Completo: _____	Cédula: _____
Firma _____	Sello: <div style="border: 1px solid black; width: 50px; height: 30px; display: inline-block;"></div>
<b>VISTO BUENO (PARA USO DE LA DTIC)</b>	
Mag. Francisco Durán Montoya VoBo Director DTIC	Unidad de Seguridad Digital VoBo
Realizado Por: _____	Fecha Realizado:    /    /
Código Asignado: _____	Contraseña Inicial: _____
Consecutivo: _____	
<b>OBSERVACIONES</b>	
<p><small>El usuario de la UNED al firmar esta solicitud se hace responsable por los daños que se ocasionen a la universidad y por el mal uso de esta autorización. Esta habilitación solo puede ser utilizada por el usuario que realiza esta solicitud, por tanto debe cumplir con Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, aprobado por el Consejo Universitario en sesión Nº 2336, Art. II, inciso 2-a) del 15 de mayo del 2014 y cualquier otra normativa que le resulte aplicable. Este reglamento lo debe consultar en: <a href="http://www.uned.ac.cr/reglamento/">http://www.uned.ac.cr/reglamento/</a></small></p>	

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 1- Datos del Solicitante

Fecha de Solicitud:	/ /	
Nombre solicitante:	_____	Firma: _____
Teléfonos:	_____ / _____	Cédula: _____
Dependencia:	_____	Puesto: _____
Solicitante es:	<input type="radio"/> Administrativo <input type="radio"/> Profesional <input type="radio"/> Docente <input type="radio"/> Investigación	

<b>(1) Fecha de Solicitud:</b>	Debe indicarla fecha en la que se solicita la autorización.
<b>(2) Nombre solicitante:</b>	Indicar el nombre completo del solicitante, que requiere la autorización.
<b>(3) Firma:</b>	Firma del solicitante, que requiere la autorización.
<b>(4) Teléfonos:</b>	Brindar los números de teléfono donde se pueda contactar.
<b>(5) Cédula:</b>	Anotar el número de cédula en formato 00-000-000.
<b>(6) Dependencia:</b>	Indicar la dependencia a la cual pertenece el solicitante
<b>(7) Puesto:</b>	Especificar el nombre del puesto que desempeña
<b>(8) Es solicitante es:</b>	Se debe seleccionar el tipo de puesto que desempeña el solicitante. (Administrativo, Profesional, Docente, Investigador)

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 2- Detalle de la solicitud

DETALLE DE LA SOLICITUD (AUTORIZACIÓN)	
<input type="radio"/> Aplicación <input type="radio"/> VPN <input type="radio"/> Puerto <input type="radio"/> Red Social <input type="radio"/> Otro: _____	
<b>Detalle de la Autorización:</b>  	
	<b>Vigencia del acceso:</b>
<b>Justificación de la Autorización y la relación con sus labores:</b>  	

<p><b>(9) Tipo de Autorización:</b> El solicitante puede seleccionar uno o varios tipos de autorización, las cuales son: Aplicación, VPN, Puerto, Red Social y Otro.</p>
<p><b>(10) Detalle de la Autorización:</b> Se refiere al tipo de autorización y como el solicitante va hacer uso de la misma, aportando mayores detalles que puedan ser utilizados por la DTIC para trabajar la configuración respectiva.</p>
<p><b>(11) Vigencia del acceso (Autorización):</b> El solicitante debe indicar por cuanto tiempo debe contar con esta autorización.</p>
<p><b>(12) Justificación de la Autorización y la relación con sus labores:</b> se refiere a la explicación del porqué de la excepción al Reglamento para uso de equipo computo e internet y la relación de esta autorización con las funciones que desempeña en la UNED.</p>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 3- Visto Bueno del Jefe Inmediato

VISTO BUENO JEFE INMEDIATO	
Nombre Completo: _____	Cédula: _____
Firma _____	Sello: <div style="border: 1px solid black; width: 100px; height: 30px; display: inline-block;"></div>

<i>(13) Nombre Completo</i>	<i>Indicar el nombre completo de la jefatura inmediata</i>
<i>(14) Cédula</i>	<i>Indicar el número de cédula de la jefatura inmediata; en formato 00-0000-0000.</i>
<i>(15) Firma</i>	<i>La firma de la jefatura inmediata constituye la aprobación de la solicitud y es un elemento indispensable para tramitar la misma.</i>
<i>(16) Sello</i>	<i>Estampar el sello de la dependencia.</i>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

#### 4- Datos del trámite realizado

VISTO BUENO (PARA USO DE LA DTIC)	
_____ Mag. Francisco Durán Montoya VoBo Director DTIC	_____ Unidad de Seguridad Digital VoBo
Realizado Por: _____	Fecha Realizado: ____ / ____ / ____
Código Asignado: _____	Contraseña Inicial: _____
Consecutivo: _____	
OBSERVACIONES	
<p>El usuario de la UNED al firmar esta solicitud se hace responsable por los daños que se ocasione a la universidad y por el mal uso de esta autorización. Esta habilitación solo puede ser utilizada por el usuario que realiza esta solicitud, por tanto debe cumplir con Reglamento para Uso de Equipos de Cómputo e Internet de la Universidad Estatal a Distancia, aprobado por el Consejo Universitario en sesión Nº 2336, Art. II, inciso 2-a) del 15 de mayo del 2014 y cualquier otra normativa que le resulte aplicable. Este reglamento lo debe consultar en: <a href="http://www.uned.ac.cr/reglamento/">http://www.uned.ac.cr/reglamento/</a></p>	

(17) VoBo Director DTIC	Firma del Director dando visto bueno a la autorización.
(18) VoBo Unidad de Seguridad Digital	Firma de un funcionario de la Unidad de Seguridad Digital, dando el visto bueno sobre tipo de autorización que se está solicitando. Debe contemplar el Reglamento para uso de equipo computo e internet y el posible riesgo que puede generar la autorización.
(19) Realizado por:	Una vez realizada la solicitud, se debe indicar por parte del funcionario que tramitó el nombre completo, la fecha de atención de la solicitud y la respectiva firma.
(20) Fecha Realizado:	Se indica la fecha en que la autorización fue realizada.
(21) Código Asignado:	Nombre de usuario asignado cuando se solicita la creación de un usuario de VPN.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

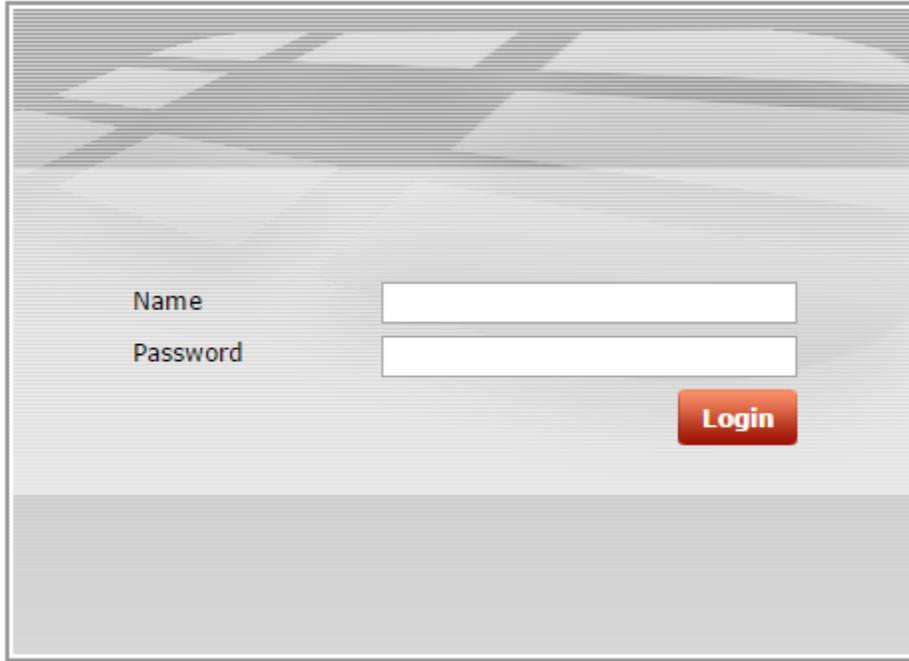
<p>(22) <i>Contraseña Inicial:</i> Contraseña asignada inicialmente por la DTIC cuando se crea un usuario de VPN Externo.</p>
<p>(23) <i>Consecutivo:</i> Este número es asignado por la DTIC al momento de recibir la solicitud.</p>
<p>(24) <i>Observaciones:</i> Se puede incluir cualquier observación aclaratoria referente al trámite realizado.</p>

### 5- Inhabilitar cuentas de usuario de VPN

Para proceder a deshabilitar cuentas de usuarios de VPN se debe contar con:

- Un documento oficial (cese de funciones, defunción, jubilación, entre otros) de Recursos Humanos o un comunicado por correo electrónico del jefe o director de la dependencia que solicite.
  - Por actividades anormales detectadas por la DTIC producto de monitoreos preventivos y estudios necesarios.
  - Después de dos meses de inactividad en el uso del acceso VPN.
  - Finalizado la fecha de vigencia de la autorización indicado en el formulario de autorización.
  - A solicitud del usuario cuando éste ya no utilice el acceso.
  - Cuando se termine algún trabajo, actividad o contratación (en el caso de personal externo a la UNED).
1. Se ingresa al concentrador de VPN. Esta actividad solo la puede realizar un funcionario de la Unidad de Seguridad Digital o personal del área de redes de la Unidad de Infraestructura Tecnológica.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



The image shows a login interface with a light gray background and a subtle geometric pattern. It contains two input fields: one for 'Name' and one for 'Password'. Below the password field is a red 'Login' button with white text.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

2. Se da clic a la opción **“User & Device”** del menú principal del concentrador de VPN, ubicado en esta opción, se da clic a **“User”**, de éste submenú que se despliega, se da clic a la opción **“User Definition”**. Al dar clic en la opción **“User Definition”** se desplegará la lista de usuarios de VPN que existen.



3. En la ventana **User Definition**, una vez desplegado la lista de usuarios, se debe seleccionar el usuario de VPN a deshabilitar. Se puede localizar un usuario de VPN de la siguiente forma:
  - a. Navegando cada una de las páginas de usuarios que existe, puede utilizar un ordenamiento alfabético dando clic sobre **“User Name”**
  - b. Realizando una búsqueda con la opción **“Search”**

Una vez ubicado el usuario de VPN, se debe dar clic sobre él y seleccionar la opción **“Edit”** del menú superior.



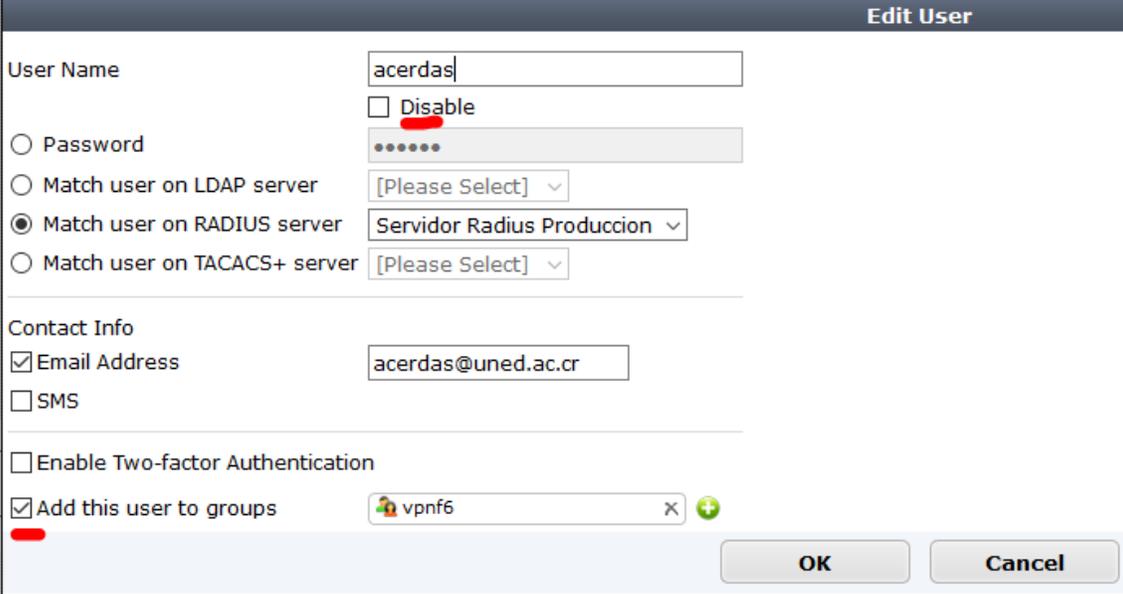
**Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia**

Dependencia	Dirección de Tecnología, información Y comunicaciones
Fecha Aprobación	26/06/2017
Fecha revisión	26/06/2019
Código	MEGAC-PEGAC.03-PR-06

Create New	Edit	Delete	Search
User Name	Type	Two-factor Authentication	Ref.
SWS	LOCAL		0
aacon	RADIUS		0

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

Al dar clic a la opción **“Edit”**, se abre todas las propiedades asociadas al usuario de VPN seleccionado. Se debe dar clic al cuadro de **“Disable”** para deshabilitar el usuario y deseleccionar el cuadro **“Add this user to groups”** para quitar al usuario del grupo de VPN al cual pertenecía, posteriormente debe dar clic al botón **“Ok”**.



**Edit User**

User Name:

**Disable**

Password:

Match user on LDAP server:

Match user on RADIUS server:

Match user on TACACS+ server:

---

Contact Info

Email Address:

SMS

---

Enable Two-factor Authentication

Add this user to groups:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructiva creación de cuentas de usuarios de VPN

### ¿En qué consiste la creación de cuentas de usuarios de VPN?

Es la gestión entorno a la creación de usuarios de VPN que pueden solicitar los funcionarios de la UNED, así como terceros externos a la institución, tanto en la sede central como en los centros universitarios.

### Conceptos

- **Boleta USD-FA-001: Formulario de Autorizaciones:** instrumento para solicitar autorización para el uso de aplicaciones, utilizar redes sociales, creación de usuarios de accesos remoto (VPN), acceso a Redes Sociales, apertura de puertos de red, entre otros tipos de autorizaciones.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

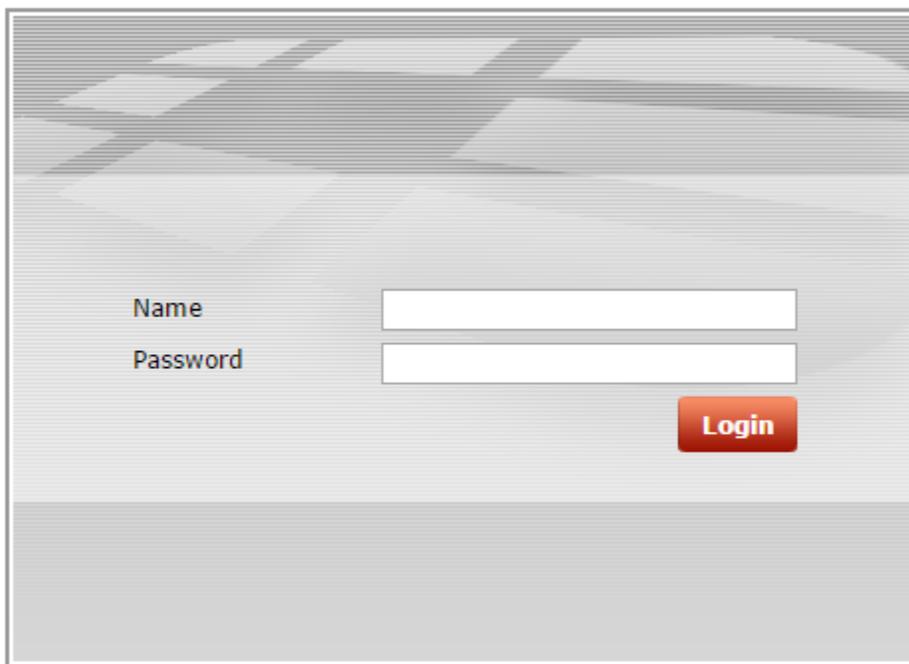
En el caso que la solicitud es de un usuario de VPN, el solicitante recibirá las credenciales por medio de correo electrónico, la DTIC tendrá un plazo de 4 días para crear y autorizar dicho usuario.

## Actividades para realizar la Creación de Usuarios de VPN

### 1. Creación de Usuarios

1. Completar y presentar el “**Formulario USD-FA-001 Formulario de Autorizaciones**” siguiendo las instrucciones que se detallan.
2. Se ingresa al concentrador de VPN. Esta actividad solo la puede realizar un funcionario de la Unidad de Seguridad Digital o personal del área de redes de la Unidad de Infraestructura Tecnológica

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06



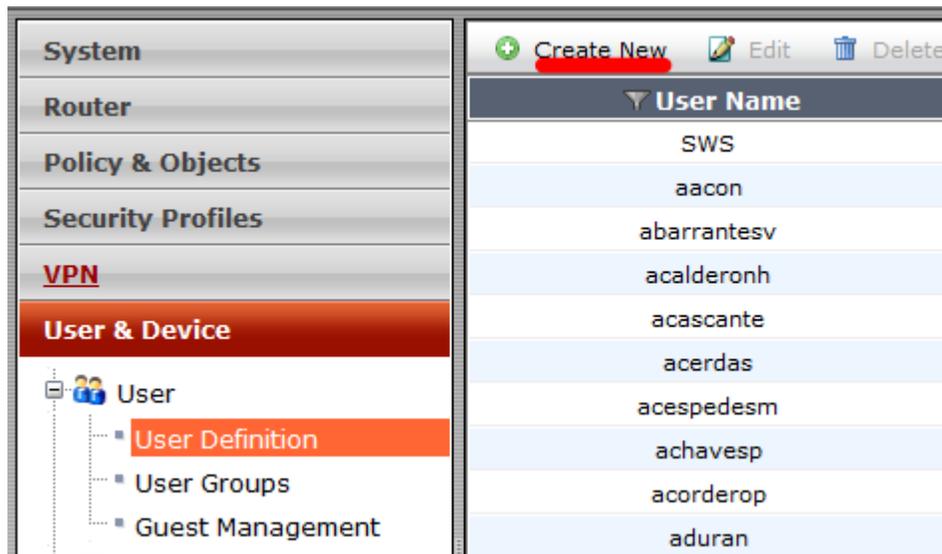
The image shows a login interface with a light gray background and a subtle geometric pattern. It features two input fields: one labeled "Name" and another labeled "Password". Below these fields is a red button with the text "Login" in white. The entire form is enclosed in a thin gray border.

1. Se da clic a la opción **“User & Device”** del menú principal del concentrador de VPN, ubicado en esta opción, se da clic a **“User”**, de éste submenú que se despliega, se da clic a la opción **“User Definition”**.

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

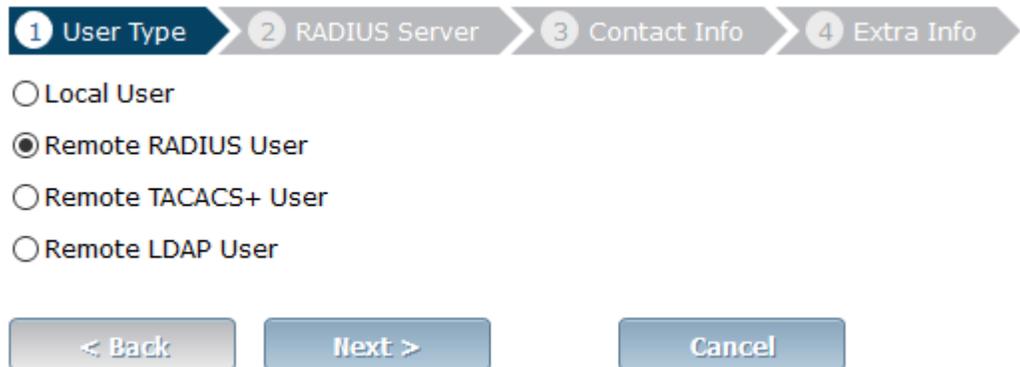


2. En la ventana **User Definition**, una vez desplegado la lista de usuarios, se debe dar clic a la opción **“Create New”** del menú superior.

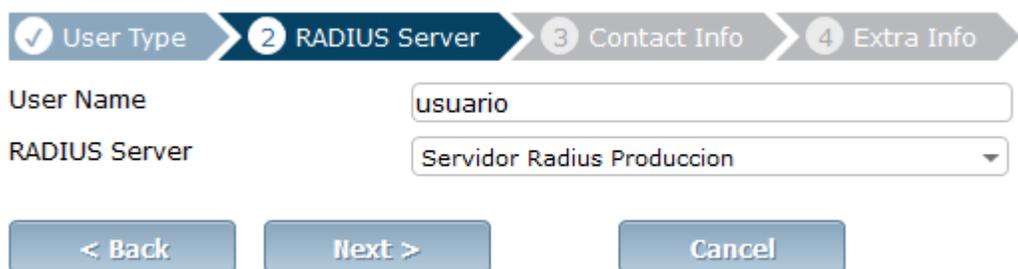


 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

3. Al dar clic a la opción **“Create New”**, se abre el asistente **“wizard”** con los siguientes pasos para crear un usuario”.
  - a. Seleccionar el tipo de usuario **“Remote RADIUS User”**. Dar clic al botón **Next**.



- b. Ingresar el usuario **“User Name”**.
      - i. Para el caso de los funcionarios el usuario de correo electrónico sin el **“@uned.ac.cr”**.
      - ii. Para el caso de personal externo, debe seguir las indicaciones de la Directriz sobre el Uso de Redes Privadas Virtuales (VPN) UNED.
      - iii. Dar clic al botón **Next**.



- c. Incluir una cuenta de correo electrónico de contacto. Dar clic al botón **Next**.

 <p>UNED UNIVERSIDAD ESTADAL COSTARRICENSE Instituto Tecnológico de la Educación y la Cultura</p>	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

User Type >  RADIUS Server > **3 Contact Info** > 4 Extra Info

Email Address

SMS

- d. Dar clic a cuadro de **“Enable”** para habilitar el acceso y dar clic al cuadro de **“User Group”** y seleccionando el grupo vpnf6. Dar clic al botón **Create** con el cual se crea el usuario vpn solicitado.

User Type >  RADIUS Server >  Contact Info > **4 Extra Info**

Enable

Two-factor Authentication

User Group

## 2. Entrega del Usuario

1. Una vez finalizada la creación del usuario, se llena el documento **USD-FA-001** con los datos:
  - a. Nombre de la persona que creo el usuario (Realizado Por:).
  - b. Fecha Realizado
  - c. Código Asignado
  - d. Contraseña Inicial
  - e. Observaciones

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

VISTO BUENO (PARA USO DE LA DTIC)	
_____ Mag. Francisco Durán Montoya VoBo Director DTIC	_____ Unidad de Seguridad Digital VoBo
Realizado Por: _____	Fecha Realizado: ____ / ____ / ____
Código Asignado: _____	Contraseña Inicial: _____
Consecutivo: _____	
OBSERVACIONES	

- Un funcionario de la Unidad de Seguridad Digital envía un correo electrónico al solicitante, mostrando los pasos a seguir para utilizar el acceso remoto. En dicho correo se indica la dirección URL de acceso y los datos de usuario y contraseña VPN.

**De:** Unidad de Seguridad Digital  
**Enviado el:** jueves, 30 de marzo de 2017 4:25 p. m.  
**Para:** usuaria@uned.ac.cr>  
**Asunto:** Acceso remoto VPN  
**Importancia:** Alta

Estimada Usuaría,

La cuenta de acceso remoto es la siguiente:

Usuario: **usuaria**

Contraseña: **La contraseña utilizada es la misma para acceder al computador o el correo electrónico institucional.**

URL de acceso es: <https://reduned2.uned.ac.cr/>

Cualquier inconveniente favor indicarnos.

**Cuando finaliza el Plan de Contingencia??**

Saludos!!!

Ing. Johnny Saborío Alvarez  
 Seguridad Digital, DTIC-UNED.

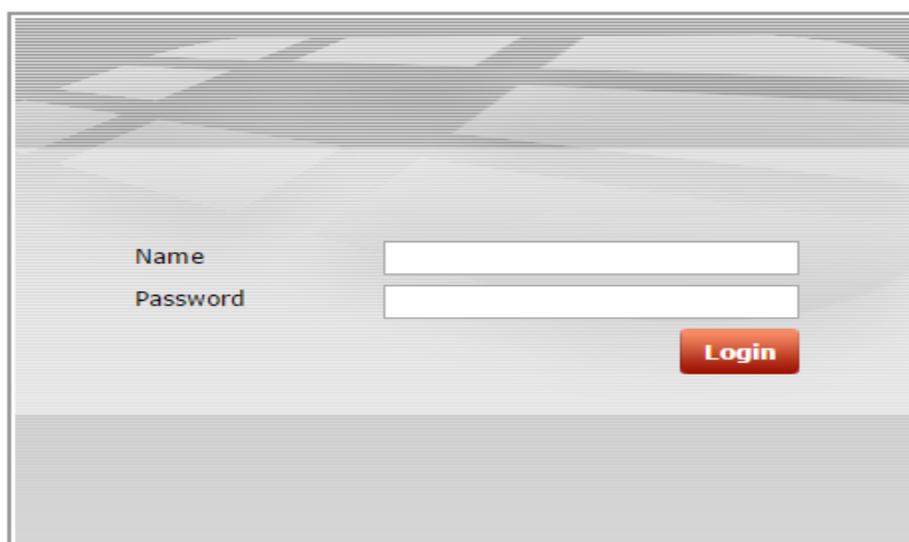
- Se entrega la boleta a la persona encargada de recepción de la DTIC para que proceda archivarla.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 3. Inhabilitar cuenta de usuario

Para proceder a deshabilitar cuentas de usuarios de VPN se debe contar con:

- Un documento oficial (cese de funciones, defunción, jubilación, entre otros) de Recursos Humanos o un comunicado por correo electrónico del jefe o director de la dependencia que solicite.
  - Por actividades anormales detectadas por la DTIC producto de monitoreos preventivos y estudios necesarios.
  - Después de dos meses de inactividad en el uso del acceso VPN.
  - Finalizado la fecha de vigencia de la autorización indicado en el formulario de autorización.
  - A solicitud del usuario cuando éste ya no utilice el acceso.
  - Cuando se termine algún trabajo, actividad o contratación (en el caso de personal externo a la UNED).
4. Se ingresa al concentrador de VPN. Esta actividad solo la puede realizar un funcionario de la Unidad de Seguridad Digital o personal del área de redes de la Unidad de Infraestructura Tecnológica.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

5. Se da clic a la opción **“User & Device”** del menú principal del concentrador de VPN, ubicado en esta opción, se da clic a **“User”**, de éste submenú que se despliega, se da clic a la opción **“User Definition”**. Al dar clic en la opción **“User Definition”** se desplegará la lista de usuarios de VPN que existen.



6. En la ventana **User Definition**, una vez desplegado la lista de usuarios, se debe seleccionar el usuario de VPN a deshabilitar. Se puede localizar un usuario de VPN de la siguiente forma:
  - a. Navegando cada una de las páginas de usuarios que existe, puede utilizar un ordenamiento alfabético dando clic sobre **“User Name”**
  - b. Realizando una búsqueda con la opción **“Search”**

Una vez ubicado el usuario de VPN, se debe dar clic sobre él y seleccionar la opción **“Edit”** del menú superior.



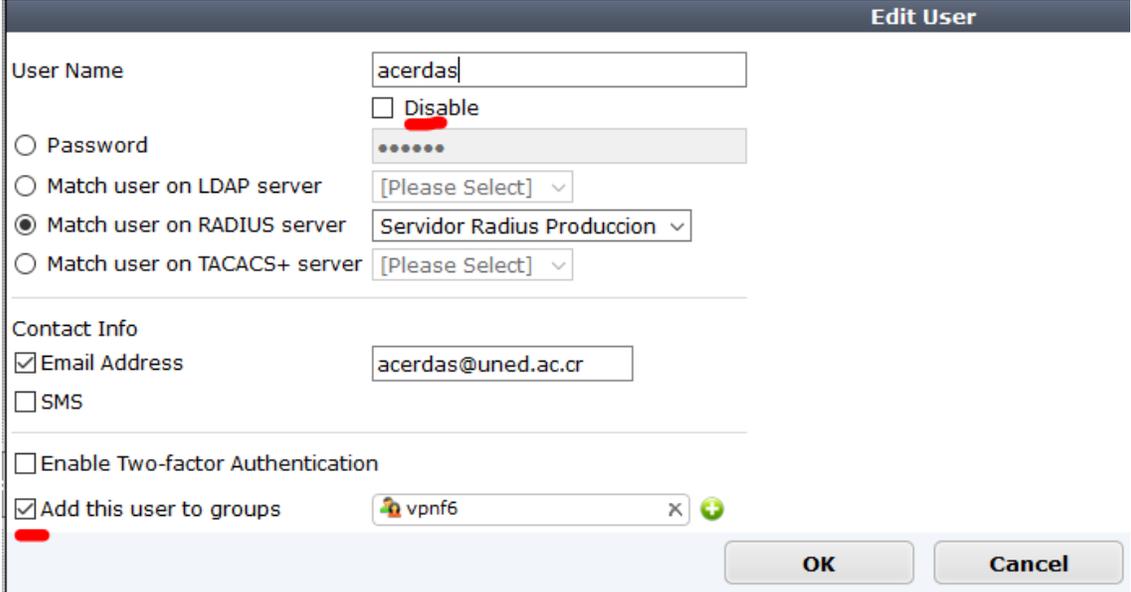
**Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia**

Dependencia	Dirección de Tecnología, información Y comunicaciones
Fecha Aprobación	26/06/2017
Fecha revisión	26/06/2019
Código	MEGAC-PEGAC.03-PR-06

User Name	Type	Two-factor Authentication	Ref.
SWS	LOCAL		0
aacon	RADIUS		0

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

7. Al dar clic a la opción “**Edit**”, se abre todas las propiedades asociadas al usuario de VPN seleccionado. Se debe dar clic al cuadro de “**Disable**” para deshabilitar el usuario y deseleccionar el cuadro “**Add this user to groups**” para quitar al usuario del grupo de VPN al cual pertenecía, posteriormente debe dar clic al botón “**Ok**”.



**Edit User**

User Name:

**Disable**

Password:

Match user on LDAP server:

Match user on RADIUS server:

Match user on TACACS+ server:

---

Contact Info

Email Address:

SMS

---

Enable Two-factor Authentication

Add this user to groups:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para el trámite del código de usuarios de desarrollo

### ¿En qué consiste el trámite del código de usuarios de desarrollo?

Es la gestión entorno a la creación de usuarios para el desarrollo de aplicaciones y sistemas que serán utilizados por los colaboradores de la institución, tanto en la sede central como en los centros universitarios. Se basa en la atención de solicitudes de creación de cuentas de usuarios para el sistema de correo electrónico en la nube Office 365, creación de grupos, lista de distribución, usuarios del AS400, entre otros.

### Conceptos

- **Boleta UEO-PL-001: Solicitud código de usuarios desarrollo: Solicitud de usuarios o grupos:** instrumento para solicitar acceso a algún ambiente de los diferentes sistemas, y debe ser entregado al Coordinador de Proyectos.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

En el caso que el usuario a crear sea nuevo, para la configuración de los accesos, estos deberán ser solicitados por medio de correo electrónico al Coordinador de Proyectos encargado, el cual tendrá un plazo de 4 días para generarlos y responder la solicitud.

### Actividades para realizar el trámite de Código de usuarios

1. Completar y presentar la solicitud siguiendo las instrucciones que se detallan:



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 1- Datos del Solicitante

Solicitud de usuarios o grupos (DTIC)	
(1) Fecha solicitud:	_____
(2) Nombre del solicitante:	_____ (3) Puesto: _____
(4) Tipo de solicitud:	<input type="checkbox"/> Usuario <input type="checkbox"/> Buzón <input type="checkbox"/> Grupo <input type="checkbox"/> Lista de distribución
(5) Ambiente:	<input type="checkbox"/> Desarrollo <input type="checkbox"/> Pruebas
(6) Utilización:	<input type="checkbox"/> Tiempo Indefinido <input type="checkbox"/> Periodo Definido _____ <span style="margin-left: 300px;">Desde: dd/mm/aaaa    Hasta: dd/mm/aaaa</span>
(7) Descripción de la Solicitud (AS400, Active Directory) :	_____
(8) Nombre del Proyecto:	_____

(1) <i>Fecha de Solicitud:</i>	Debe indicar la fecha en la que se solicita la creación del usuario.
(2) <i>Nombre solicitante:</i>	Indicar el nombre completo del solicitante, que requiere la creación del usuario.
<b>(3) Puesto:</b>	Especificar el nombre del puesto que desempeña
<b>(4) Tipo Solicitud:</b>	Indicar el tipo de solicitud, marcando la casilla que corresponda (Usuario, Buzón, Grupo o Lista de distribución).
<b>(5) Ambiente:</b>	Indicar el tipo de ambiente donde se requiere le acceso, marcando la casilla que corresponda (Desarrollo, Pruebas).
<b>(6) Utilización:</b>	Indicar el periodo durante el cual se requiere la solicitud, si es indefinido marcar la casilla y si es definido se debe indicar el periodo de utilización.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

**(7) Descripción de la solicitud:**

Se debe indicar un detalle de la solicitud, donde se identifique claramente la necesidad, indicando la plataforma donde requiere los permisos (AS400, Active Directory).

**(8) Nombre del proyecto:** Indicar el nombre del proyecto en el que el solicitante requiere los permisos.

**2- Visto Bueno del Coordinador de Proyectos**

**(9) Autorización del Líder de Proyectos**

Nombre Completo: \_\_\_\_\_

Firma: \_\_\_\_\_

**Datos a completar**

**El funcionario que completa debe tener en cuenta lo siguiente**

**(9) Autorización Líder del Proyectos:**

El Coordinador de Proyectos a cargo, debe dar la autorización de la solicitud, debe escribir su nombre completo y la firma.

**3- Datos del trámite realizado**

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

<b>(10) Realizado por</b>	Fecha: _____
Nombre Completo: _____	Firma: _____
<b>(11) Descripción de lo realizado:</b>	
Usuarios:	
Grupos:	
Listas de distribución:	
<b>(12) Observaciones:</b>	
_____	
_____	

**(10) Realizado por:** Una vez realizada la solicitud, se debe indicar por parte del funcionario que tramitó el nombre completo, la fecha de atención de la solicitud y la respectiva firma.

**(11) Descripción de lo realizado:** Se debe detallar la labor realizada, por parte del que tramitó la solicitud, indicando las acciones realizadas ya sea para; usuarios, grupos o listas de distribución”

**(12) Observaciones:** Se puede incluir cualquier observación aclaratoria referente al trámite realizado.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para la Creación e inhabilitación de usuarios de la plataforma AS400

### ¿En qué consiste la creación de usuarios e inhabilitación de AS-400?

Es la gestión relacionada a los usuarios de cada uno de los colaboradores de la institución, tanto en la sede central como en los centros universitarios. Se basa en la atención de solicitudes de creación, modificación y deshabilitación de cuentas en el sistema de correo y en el AS/400.

### Conceptos

- **AS-400:** Servidor donde residen una gran parte de los sistemas institucionales.
- **Creación de usuarios:** acción para crear y habilitar cuentas de usuario a funcionarios de la UNED que acceden a los sistemas institucionales.
- **Inhabilitación de usuarios:** acción que se debe realizar una vez que una persona deja de ser funcionario de la UNED, cambia de funciones dentro de la institución o por solicitud de su jefatura o del Líder de servicio.
- **Boleta UEO-PL-001 Solicitud código de usuarios Desarrollo:** Instrumento para solicitar la creación de usuarios para desarrollo de sistemas, pruebas de aplicaciones, entre otros.
- **Boleta UIT-PL-002: Formulario: Solicitudes códigos de usuarios:** Instrumento para solicitar el correo electrónico en la nube Office 365, cuentas de usuario para AS/400 y sus respectivos accesos, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

1. Toda solicitud de creación de cuentas de usuario deberá ser autorizada por la jefatura inmediata (el jefe inmediato del funcionario que solicita).
2. La jefatura inmediata deberá consultar con el Líder de servicio el criterio técnico respectivo en cuanto a los accesos y menú del usuario solicitante.
3. En caso de que el usuario necesite acceso a otros sistemas, deberá solicitar el criterio técnico al Líder de servicio correspondiente (no es necesaria la aprobación de la jefatura del Líder de servicio).
4. En el caso que la solicitud es de un usuario del AS/400 y el funcionario que lo solicita cuenta con correo electrónico institucional, recibirá las credenciales por medio de correo, la DTIC tendrá un plazo de 4 días para crear y autorizar dicho usuario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Equipo	Nombre de Equipo
Producción	S1030557
Desarrollo	Sistemas

**Actividades para creación de usuarios e inhabilitación de AS-400**

1. En la línea de comandos del AS400 se utiliza el comando “**WRKUSRPRF**”, luego se presiona F4



2. Después de presionar saldrá una pantalla de perfil de usuario con un espacio en blanco donde se deberá digitar **\*all** y se presiona Enter



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Se despliega la lista de todos los usuarios que se encuentran creados en el sistema del AS400. En esta pantalla en la parte de **OPC** se deberá digitar el número “1” que corresponde a la opción para crear usuarios.

```

Trabajar con Perfiles de Usuario

Teclee opciones, pulse Intro.
 1=Crear  2=Cambiar  3=Copiar  4=Suprimir  5=Visualizar
12=Trabajar con objetos por propietario

      Perfil
Opc  Usuario  Texto
1_   acespedes
___   AABARCA   Amalfi Abarca Ortiz-San Cañas-Certificaciones'
___   AABDALLAH Adib Abdallah Arrieta
___   AACON1    Ariana Acon PAA
___   AAGUERO   Encargado Catedra-Ana Aguero Brenes
___   AALVAREZ  Amanda Álvarez Cordero - Centro de Idiomas
___   AARAYA    Encargado Catedra-Jose Araya'
___   AARCE     Alejandro Arce Mora
___   ABOLANOS  Andrea Bolaños Extension AMMU88
___   ABOLANOSM ANA BOLAÑOS MORA EXTENSION

MÁS...

Parámetros para opciones 1, 2, 3, 4 y 5 o mandato
==>
F3=Salir  F5=Renovar  F12=Cancelar  F16=Repetir situar en  F17=Situat en
F21=Seleccionar nivel ayuda  F24=Más teclas

```

- Se despliega la pantalla de perfil de usuario, donde se digita el usuario solicitado y se presiona Enter. Para que aparezca la pantalla donde se digitan los datos del nuevo usuario. Otra manera para crear un usuario, es en la línea de comandos utilizar es el comando “**CRTUSRPRF**” y presionar Enter. Aparecerá la pantalla donde se digitarán los datos del nuevo usuario (Ilustración 4).

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

```

12:20:01          Menú MNUCLOP          23/11/12

Seleccione una de las siguientes opciones

1. RespalDOS
2. Listados
3. Trabajar con Controladores WRKCFGSTS CTL
4. Trabajar con Lineas          LIN
5. Trabajar con Dispositivos   DSP
6. Trabajar con Impresoras     WRKWTR
7. Valores del Sistema         WRKSYSVAL

OFICINA DE SISTEMAS

Selección o mandato
==> CRTUSRPRF

```

5. Una vez presionado **Enter** la siguiente pantalla mostrará las opciones a modificar:

```

          Crear perfil de usuario (CRTUSRPRF)

Teclee elecciones, pulse Intro.

Perfil de usuario . . . . . > ACESPEDES      Nombre
Contraseña de usuario . . . . . uned2012    Valor tipo carácter...
Contraseña caducada . . . . . *yes      *NO, *YES
Estado . . . . . *ENABLED      *ENABLED, *DISABLED
Clase de usuario . . . . . *USER      *USER, *SYSOPR, *PGMR...
Nivel de ayuda . . . . . *SYSVAL      *SYSVAL, *BASIC, *INTERMED...
Biblioteca actual . . . . . *CRTDFT      Nombre, *CRTDFT
Programa inicial a llamar . . . . . *NONE      Nombre, *NONE
  Biblioteca . . . . .          Nombre, *LIBL, *CURLIB
Menú inicial . . . . . MAIN          Nombre, *SIGNOFF
  Biblioteca . . . . . *LIBL      Nombre, *LIBL, *CURLIB
Limitar posibilidades . . . . . *NO      *NO, *PARTIAL, *YES
Texto descriptivo . . . . . *BLANK

```

5.1. *Contraseña de usuario:* se asigna una contraseña temporal que después el funcionario es responsable de cambiarla

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

5.2. <i>Contraseña caduca:</i>	se digita “ <b>*yes</b> ”, esto para que el usuario obligatoriamente deba cambiar la clave la primera vez que ingresa
5.3. <i>Estado:</i>	<i>debe de estar “ENABLED”</i>
5.4. <i>Programa inicial a llamar:</i>	<i>digitar el programa, que, según las necesidades del usuario, el analista encargado debe anotar en la boleta los datos de programa inicial, menús y permisos correspondientes</i>
5.5. <i>Biblioteca:</i>	<i>(debajo Programa Inicial) se digita la biblioteca donde se encuentra alojado el programa que se va a utilizar.</i>
5.6. <i>Menú inicial:</i>	<i>se digita el menú que debe tener el nuevo usuario</i>
5.7. <i>Biblioteca:</i>	<i>(debajo de Menú Inicial) se digita la biblioteca donde se encuentra ese menú</i>
5.8. <i>Texto Descriptivo:</i>	<i>se digita el nombre completo del nuevo usuario, su cedula, una breve descripción de la dependencia y que ejecutara ese usuario</i>

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Una vez completa ésta información se presiona **F9** para que habilite más opciones y utilizando las teclas **Re Pag** y **Av Pag** para navegar sobre las pantallas de opciones



- Se desplaza entre pantallas hasta llegar al espacio *Descripción de Trabajo* donde se digita la descripción del grupo de trabajo junto y la *biblioteca* donde se encuentra esa descripción.
- En el espacio de Perfil de Grupo de digita el grupo en el cual se encuentra el usuario

```

Cambiar perfil de usuario (CHGUSRPRF)

Teclee elecciones, pulse Intro.

Descripción de trabajo . . . . . QDFTJOB D Nombre, *SAME
Biblioteca . . . . . QGPL Nombre, *LIBL, *CURLIB
Perfil de grupo . . . . . GRPOBJETOS Nombre, *SAME, *NONE
Propietario . . . . . *USRPRF *SAME, *USRPRF, *GRPPRF
Autorización de grupo . . . . . *NONE *SAME, *NONE, *ALL...
Tipo autorización grupo . . . . . *PRIVATE *PRIVATE, *PGP, *SAME
Grupos suplementarios . . . . . *NONE Nombre, *SAME, *NONE
+ para más valores
Código de contabilidad . . . . . *BLANK
Contraseña de documento . . . . . *SAME Nombre, *SAME, *NONE
Cola de mensajes . . . . . OPACM Nombre, *SAME, *USRPRF
Biblioteca . . . . . QUSRSYS Nombre, *LIBL, *CURLIB
Entrega . . . . . *NOTIFY *SAME, *NOTIFY, *BREAK...
Filtro del código de gravedad . . . . . 0 0-99, *SAME
Dispositivo de impresión . . . . . *WRKSTN Nombre...

Más...

```

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Una vez completados estos pasos se presiona **Enter** para que se cree el usuario en el sistema del AS400. Retornara a la pantalla donde se muestran todos los usuarios.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### Entrega del usuario

1. Una vez finalizada la creación del usuario, se llena el documento **UEO-PL-002** con los datos:
  - a. Nombre de la persona que creo el usuario
  - b. Fecha de realización
  - c. Firma

Realizado por _____	(b) Fecha: _____
(a) Nombre Completo: _____	(c) Firma: _____
Descripción de lo realizado:	
Usuarios:	
Grupos:	
Listas de distribución:	
Observaciones: _____	
_____	

2. Se deberá entregar la boleta al coordinador de la Unidad de Seguridad Digital
3. El coordinador de la Unidad de Seguridad Digital verifica que el usuario fue creado según los requerimientos establecidos en la boleta y pasa la boleta al encargado de recepción.
4. El encargado de recepción comunica a los usuarios que se debe presentar a la oficina de la Dirección de Tecnología, con su respectiva cedula, para la entrega de su usuario y contraseña.
5. El encargado de recepción después de entregar la información al usuario; archivar la respectiva boleta.

### Inhabilitar usuario AS400

Para proceder a la inhabilitación de usuarios se debe contar con un documento oficial (cese de funciones, defunción, jubilación) de Recursos Humanos o un comunicado por correo electrónico del jefe del área que solicite.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

1. En la pantalla principal del AS400 en la línea de comando se digita el siguiente comando “**WRKUSRPRF USUARIO** (donde USUARIO es el nombre de usuario del funcionario a inhabilitar)” y se presiona **Enter**.

```

08:19:35                               Menú MNUCLOP                               9/11/12
Seleccione una de las siguientes opciones
-----
1. Respaldos
2. Listados
3. Trabajar con Controladores WRKCFGSTS CTL
4. Trabajar con Lineas
5. Trabajar con Dispositivos
6. Trabajar con Impresoras WRKWTR
7. Valores del Sistema WRKSYSVAL OFICINA DE SISTEMAS

Selección o mandato
==> wrkusrprf aabarca

```

2. La pantalla siguiente muestra en donde aparecerá el usuario junto con la descripción, en el apartado **Opc** se deberá digitar la opción 2 y presionar Enter, esto permitirá cambiar opciones en del usuario.

```

Trabajar con Perfiles de Usuario

Teclee opciones, pulse Intro.
  1=Crear  2=Cambiar  3=Copiar  4=Suprimir  5=Visualizar
  12=Trabajar con objetos por propietario

Perfil
Opc  Usuario      Texto
-----
  2_  AABARCA      Amalfi Abarca Ortiz-San Cañas-Certificaciones'

```

 <p>UNED UNIVERSIDAD ESTADAL CUBANA Instituto Cubano de la Educación y la Cultura</p>	<p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- En las opciones de usuario, en el espacio **Estado** se deberá digitar “**\*DISABLED**” y en el espacio de **texto descriptivo** se indicará el **Oficio** que justifica dicha deshabilitación y se presiona **Enter**.

```

Cambiar perfil de usuario (CHGUSRPRF)

Teclee elecciones, pulse Intro.

Perfil de usuario . . . . . > AABARCA      Nombre
Contraseña de usuario . . . . . *SAME_____ Valor tipo carácter...
Contraseña caducada . . . . . *NO_____ *SAME, *NO, *YES
Estado . . . . . *disabled *SAME, *ENABLED, *DISABLED
Clase de usuario . . . . . *USER_____ *SAME, *USER, *SYSOPR...
Nivel de ayuda . . . . . *SYSVAL_____ *SAME, *SYSVAL, *BASIC...
Biblioteca actual . . . . . *CRTDFT_____ Nombre, *SAME, *CRTDFT
Programa inicial a llamar . . . . . TCCDCUPRR Nombre, *SAME, *NONE
  Biblioteca . . . . . PRODUCCION Nombre, *LIBL, *CURLIB
Menú inicial . . . . . *SIGNOFF_____ Nombre, *SAME, *SIGNOFF
  Biblioteca . . . . . _____ Nombre, *LIBL, *CURLIB
Limitar posibilidades . . . . . *YES_____ *SAME, *NO, *PARTIAL, *YES
Texto descriptivo . . . . . 'Amalfi Abarca Ortiz-San Cañas-Certificacion
es'_____

```

- Una vez deshabilitado el usuario, el documento que origina la solicitud, se debe indicar el nombre del funcionario que procesó la solicitud y la fecha de realización y entregar al encargado de la Unidad de Seguridad Digital el documento para que verifique que el usuario fue deshabilitado y posteriormente entregue el documento al encargado de recepción de la DTIC para que lo archive.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para la creación de cuentas de usuarios en Active Directory

### ¿En qué consisten las solicitudes de usuarios?

Es la gestión entorno a los usuarios de cada uno de los colaboradores de la institución, tanto en la sede central como en los centros universitarios. Se basa en la atención de solicitudes de creación de cuentas de usuarios para el sistema de correo electrónico en la nube Office 365, para ingresar a los equipos de cómputo, así como para los dispositivos tecnológicos y acceso a la red institucional.

### Conceptos

- **Boleta UIT-PL-002- Formulario: Solicitudes códigos de usuarios:** Instrumento para solicitar el correo electrónico en la nube Office 365, cuentas de usuario para AS/400 y sus respectivos accesos, código de usuario para los equipos de cómputo como para los dispositivos tecnológicos y acceso a la red institucional.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

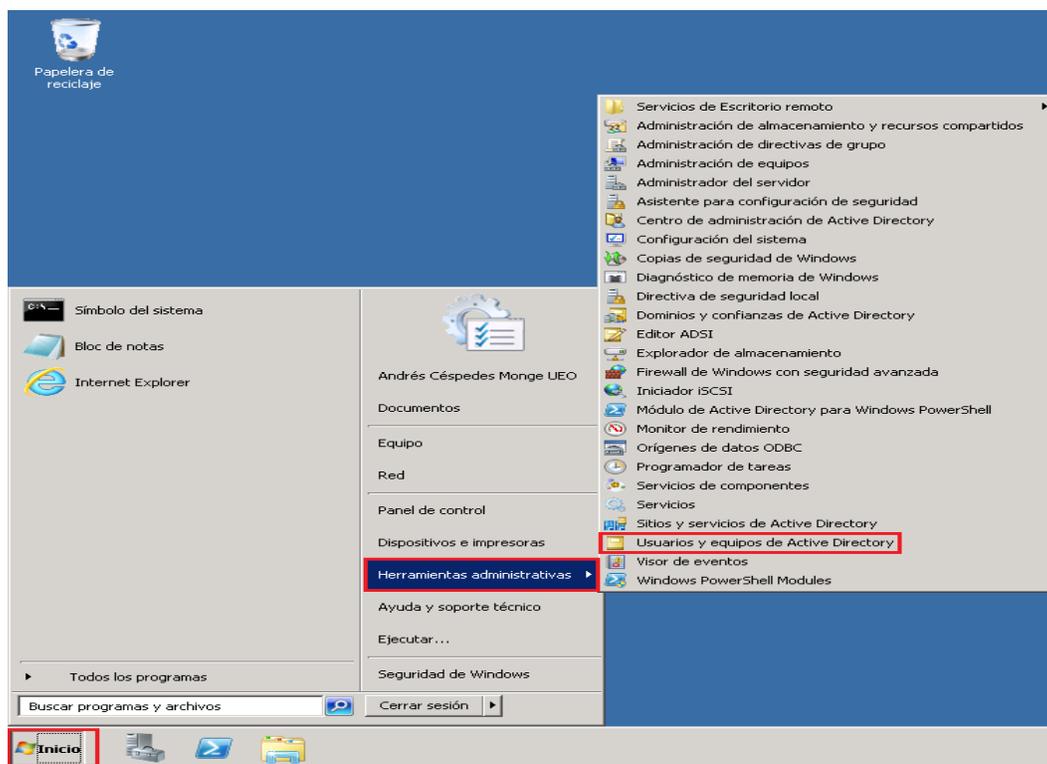
1. La DTIC tendrá un plazo de 2 días para crear y autorizar dichos usuarios.

### Actividades para creación de cuentas de usuarios en Active Directory

#### 1. Cuentas usuario Active Directory - Creación de Usuarios sin correo electrónico

El encargado deberá ingresar al servidor que tenga el rol de **Active Directory** instalado, una vez en el equipo, debe presionar el botón de **Inicio**, para buscar el menú de **Herramientas Administrativas** y en la opción **Usuarios y Equipos de Active Directory**, se le da **Clic**.

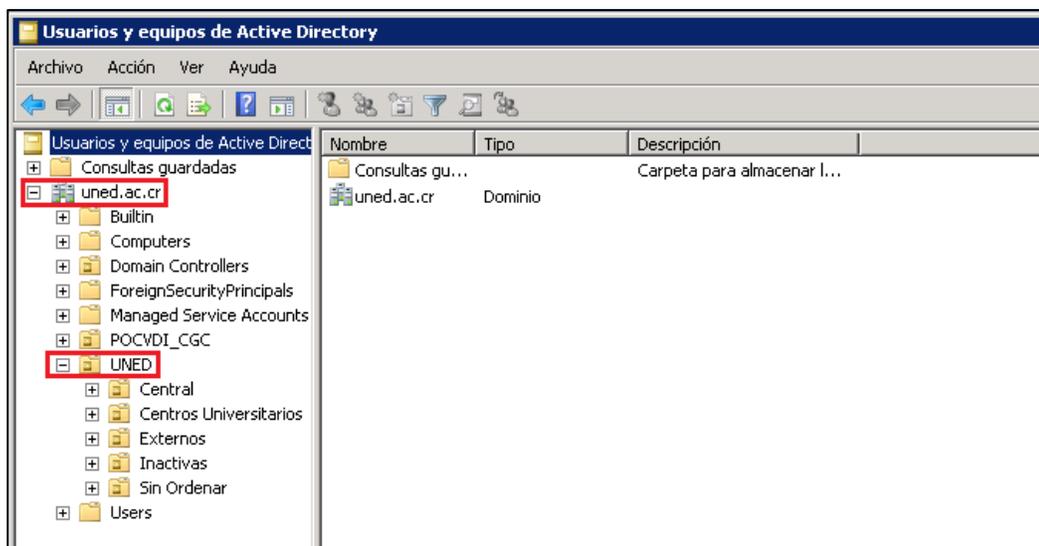
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



1. En la opción **usuarios y equipos de Active Directory**, saldrá una pantalla para búsqueda de la dependencia donde se creará el usuario.
  - 1.1. Se expande el dominio “**uned.ac.cr**”
  - 1.2. Luego se expande la unidad organizacional (de ahora en adelante OU) **UNED**; donde se encuentran distribuidas las dependencias y los centros de la Universidad,
  - 1.3. Se siguen expandiendo las diferentes OU’s hasta ubicar la que se requiere

De no encontrar la OU buscada, existe una OU llamada Sin Ordenar en donde podremos crear al usuario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



- Una vez ubicada la dependencia o centro, se le da click derecho sobre el OU, con el mouse se posiciona en **Nuevo** y se le da click a la opción **Usuario**.



**Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia**

Dependencia

Dirección de Tecnología, información Y comunicaciones

Fecha Aprobación

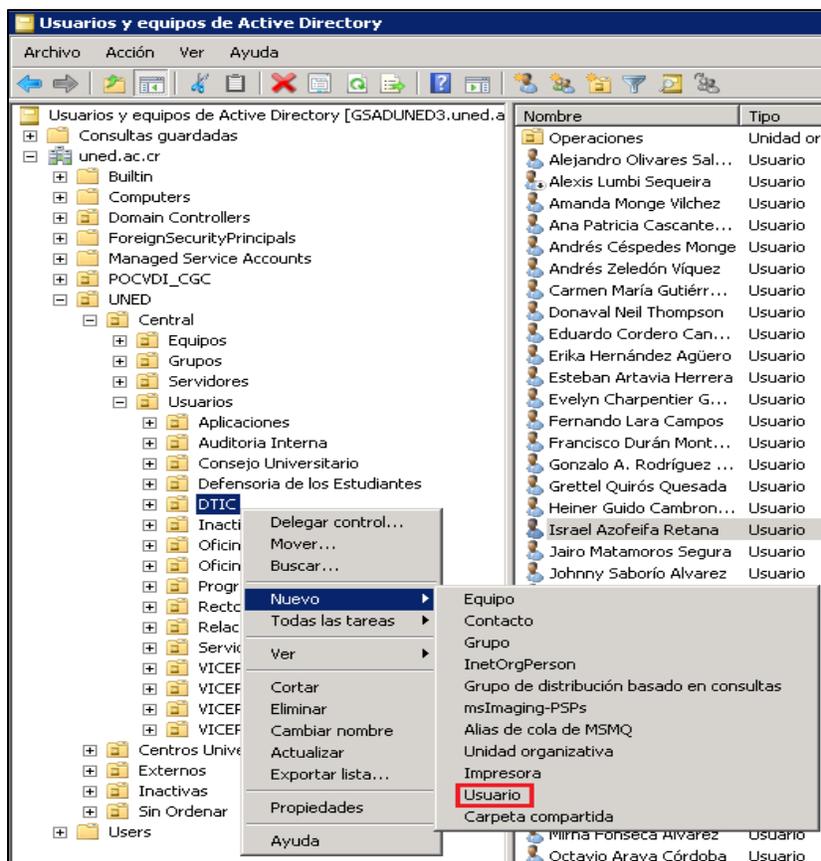
26/06/2017

Fecha revisión

26/06/2019

Código

MEGAC-PEGAC.03-PR-06



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

3. En la pantalla nuevo objeto usuario se ingresan los datos del usuario:
  - 3.1. Nombre
  - 3.2. Apellidos
  - 3.3. Nombre de inicio de sesión de usuario el cual se define de la siguiente forma:
    - 3.3.1. La primera letra del nombre y el apellido completo.
    - 3.3.2. En el caso de que este usuario ya exista se usara la primera letra del nombre, el primer apellido y la primera letra del segundo apellido
    - 3.3.3. En el caso que el usuario también existe se agregan las letras del nombre hasta que ya acepté el nombre de inicio, después se presiona **Siguiente**.

**Nuevo objeto: Usuario**

Crear en: uned.ac.cr/UNED/Central/Usuarios/DTIC

Nombre de pila:  Iniciales:

Apellidos:

Nombre completo:

Nombre de inicio de sesión de usuario:

@uned.ac.cr

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

< Atrás **Siguiente >** Cancelar

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. En la siguiente pantalla debe introducir una contraseña temporal para el usuario, y verificar que únicamente la opción **“El usuario deberá cambiar la contraseña en el siguiente inicio de sesión”** debe estar marcada con un “check” y presiona

siguiente.

5. La pantalla siguiente muestra el resumen de creación del usuario, se verifica la información y se presiona **Finalizar** para terminar la creación del usuario.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

**Nuevo objeto: Usuario**

Crear en: uned.ac.cr/UNED/Central/Usuarios/DTIC

Quando haga clic en Finalizar, se creará el siguiente objeto:

Nombre completo: Juan Perez Perez  
Nombre de inicio de sesión del usuario: jperezp@uned.ac.cr  
El usuario debe cambiar la contraseña en el siguiente inicio de sesión.

< Atrás **Finalizar** Cancelar

## 2. Creación de Cuentas de Usuario con Correo Electrónico

1. Una vez recibida la solicitud en el documento **UEO-PL-002** con su respectivo visto bueno, se deberá ingresar al Centro de Administración de Exchange.

Centro de administración de Exchange

Dirección de correo electrónico:

Contraseña:

iniciar sesión

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- En el Centro de Administración de Exchange se debe posicionar en la opción del Menú Vertical “destinatarios” dar clic en la pestaña “buzones”. Ubicado en esta opción se debe dar clic al botón “+” y seleccionar “Buzón de Office 365”.

Centro de administración de Exchange

destinatarios | buzones | grupos | recursos | contactos | compartido | migración

Es seguro | https://correo.uned.ac.cr/ecp/

Empresa Office 365

+ - elopez

TIPO DE BUZÓN	DIRECCIÓN DE CORREO ELECTRÓNICO
Office 365	elopez@uned.ac.cr

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

3. En la opción “**nuevo buzón de Office 365**”, se despliega una pantalla donde se ingresa los datos del nuevo usuario.

Buzón de Office 365 - Google Chrome

Es seguro | [https://correo.uned.ac.cr/ecp/UsersGroups/NewRemoteMailbox.:](https://correo.uned.ac.cr/ecp/UsersGroups/NewRemoteMailbox.)

Ayuda

nuevo buzón de Office 365

Nombre:

Iniciales:

Apellidos:

\*Nombre:

\*Nombre de inicio de sesión del usuario:  @ uned.ac.cr ▼

\*Tipo de buzón: Buzón de usuario ▼

\*Nueva contraseña:

\*Confirmar la contraseña:

Pedir el cambio de contraseña en el siguiente inicio de sesión

Crear un buzón de correo de archivo

guardar cancelar

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. La pantalla con los datos del nuevo usuario debe quedar de la siguiente forma.

Buzón de Office 365 - Google Chrome

Es seguro | [https://correo.uned.ac.cr/ecp/UsersGroups/NewRemoteMailbox.:](https://correo.uned.ac.cr/ecp/UsersGroups/NewRemoteMailbox.)

nuevo buzón de Office 365 [Ayuda](#)

Nombre: Vernor

Iniciales:

Apellidos: Muñoz Villalobos

\*Nombre: Vernor Muñoz Villalobos

\*Nombre de inicio de sesión del usuario: vmunoz @ uned.ac.cr

\*Tipo de buzón: Buzón de usuario

\*Nueva contraseña: .....

\*Confirmar la contraseña: .....

Pedir el cambio de contraseña en el siguiente inicio de sesión

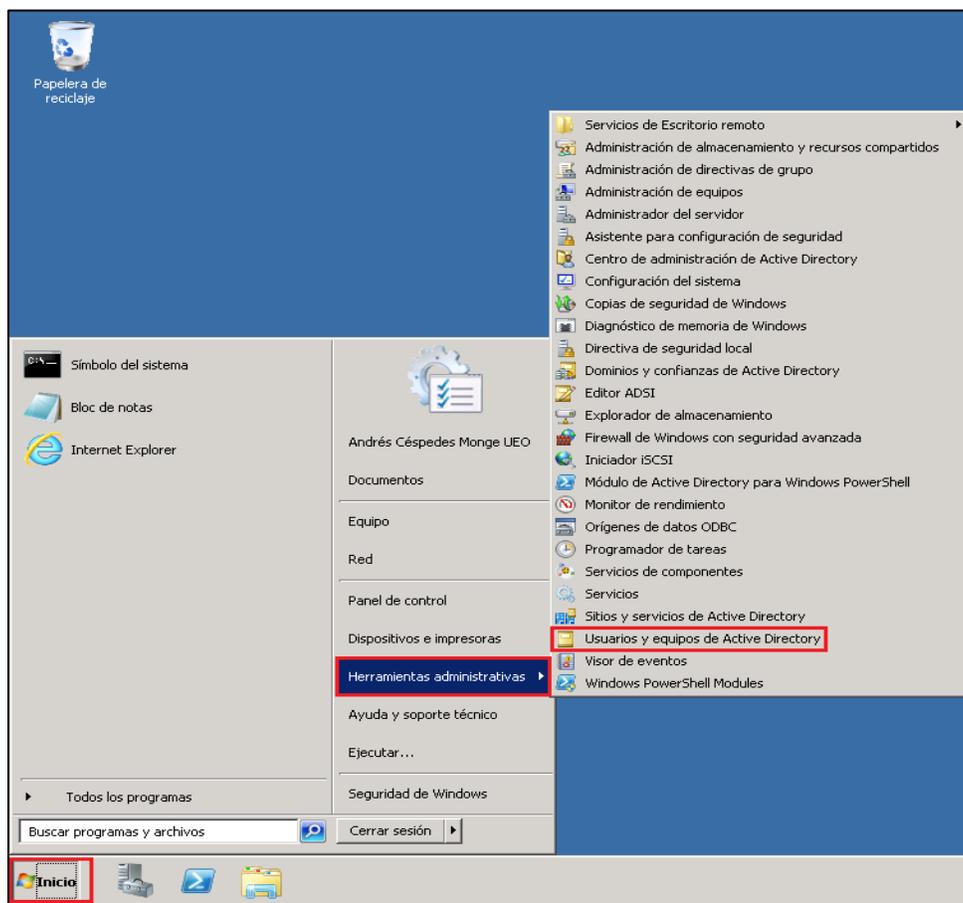
Crear un buzón de correo de archivo

guardar cancelar

Vuelve a escribir la contraseña para comprobar que la escribiste correctamente.

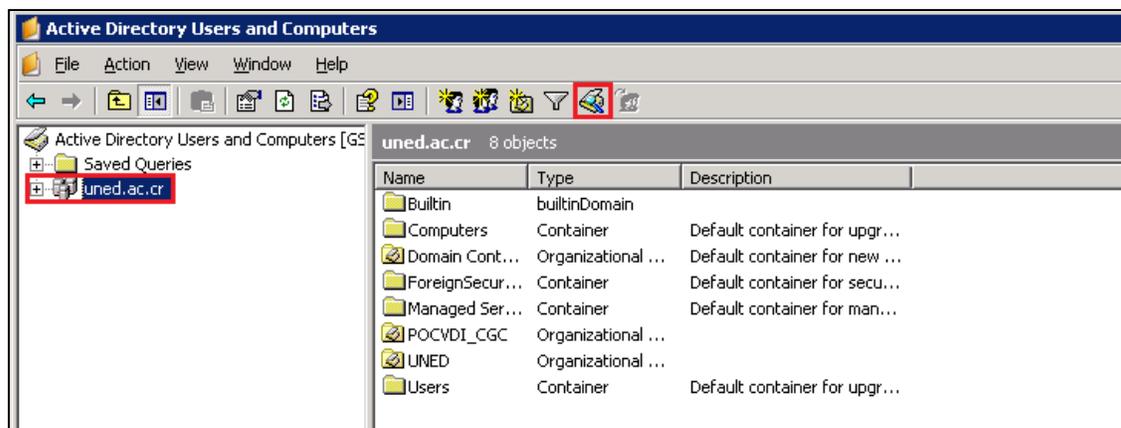
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Posteriormente se deberá ingresar al servidor que tenga el rol de Active Directory. Una vez en el equipo se debe presionar el botón de **Inicio**. buscar la opción **Herramientas Administrativas** y en **Usuarios y Equipos de Active Directory**, dar **Clic**.



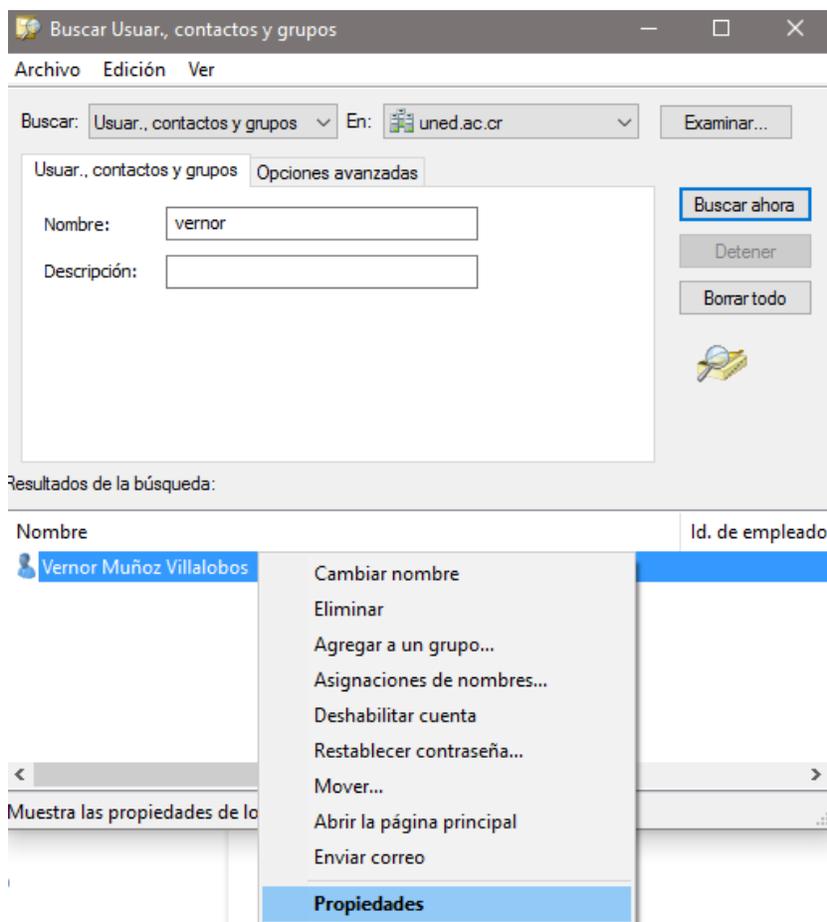
- Se abre la ventana **Active Directory Users and Computers** donde se selecciona el dominio **“uned.ac.cr”**, luego presionamos la opción de **buscar** usuarios.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



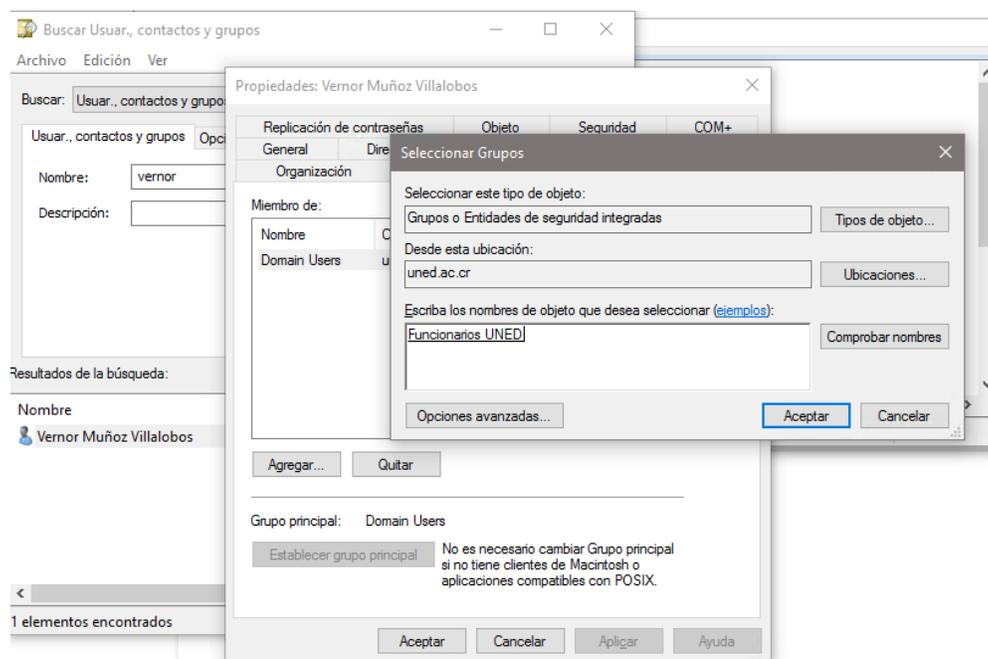
- En la ventana **Buscar Usuar., contactos y grupos**, en el campo llamado **Nombre** se ingresa el nombre del funcionario o persona al cual se le creó el usuario y se presiona la opción de **buscar** ahora. Una vez encontrado el usuario se da clic derecho sobre él y se da clic a la opción de **“Propiedades”**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



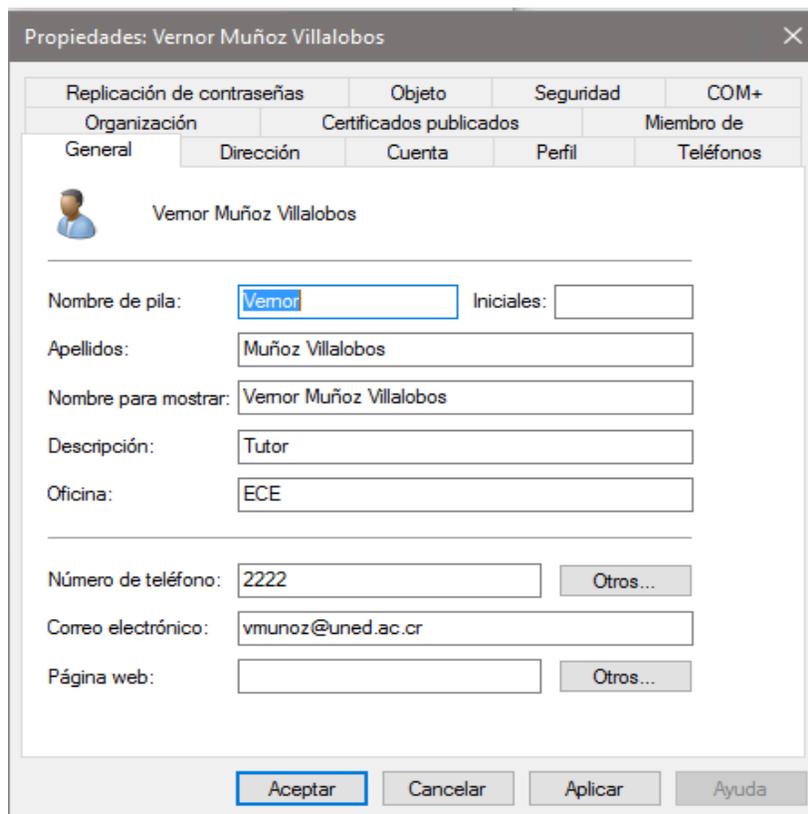
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

8. En la ventana de **propiedades** se debe de ubicar en la pestaña “**Miembro de**” y le da clic al botón **Agregar**, donde debe digitar los nombres de los grupos al cual pertenece el usuario, separados por un punto y coma en caso de que sean varios grupos. Puede dar clic al botón “**Comprobar nombres**” para verificar que los nombres de los grupos es el correcto, puede realizar esta acción las veces que lo requiera. Una vez agregado todos los grupos debe dar clic al botón “**Aceptar**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

9. En la ventana de propiedades, en la pestaña “General” se debe completar las calidades del usuario nuevo.



Propiedades: Vernor Muñoz Villalobos

Replicación de contraseñas    Objeto    Seguridad    COM+

Organización    Certificados publicados    Miembro de

General    Dirección    Cuenta    Perfil    Teléfonos

 Vernor Muñoz Villalobos

Nombre de pila:  Iniciales:

Apellidos:

Nombre para mostrar:

Descripción:

Oficina:

Número de teléfono:

Correo electrónico:

Página web:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

10. En la ventana de propiedades, en la pestaña de “Cuenta” se especifica si el usuario expira en una fecha determinada (esto en función del tipo de nombramiento o de la función que vaya a realizar este usuario).

Propiedades: Vernor Muñoz Villalobos

Replicación de contraseñas    Objeto    Seguridad    COM+

Organización    Certificados publicados    Miembro de

General    Dirección    Cuenta    Perfil    Teléfonos

Nombre de inicio de sesión de usuario:  
 vmunoz    @uned.ac.cr

Nombre de inicio de sesión de usuario (anterior a Windows 2000):  
 uned.ac.cr\    vmunoz

Horas de inicio de sesión...    Iniciar sesión en...

Desbloquear cuenta

Opciones de cuenta:

- El usuario debe cambiar la contraseña en el siguiente inicio de sesión
- El usuario no puede cambiar la contraseña
- La contraseña nunca expira
- Almacenar contraseña utilizando cifrado reversible

La cuenta expira

Nunca

Fin de:    lunes, 15 de junio de 2017

Aceptar    Cancelar    Aplicar    Ayuda

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

11. En la ventana de propiedades, en la pestaña de “Organización” se ingresa la información laboral del usuario.

Propiedades: Vernor Muñoz Villalobos

Replicación de contraseñas	Objeto	Seguridad	COM+
General	Dirección	Cuenta	Perfil
Organización	Certificados publicados	Miembro de	

Puesto:

Departamento:

Organización:

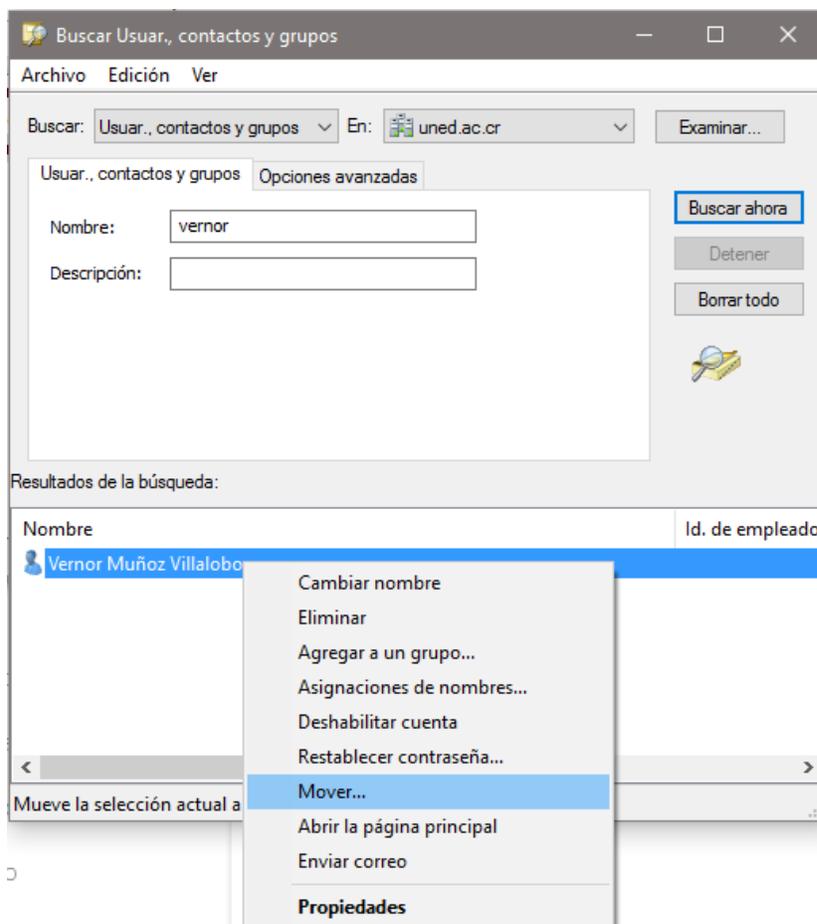
Administrador

Nombre:

Supervisa a:

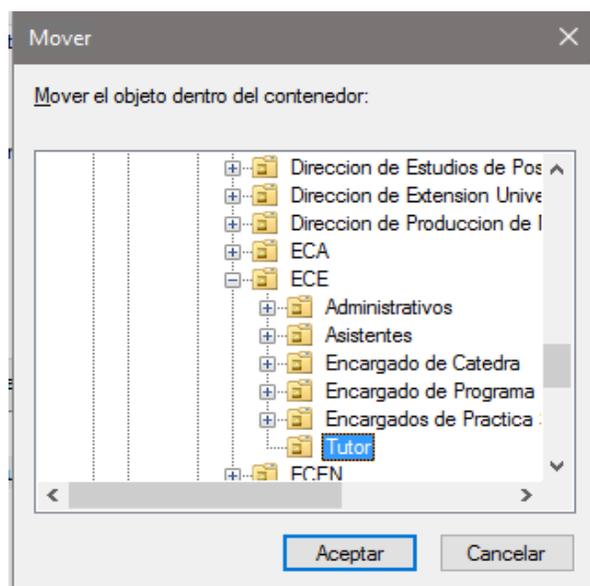
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

12. En la ventana **Buscar Usuar., contactos y grupos**, en el campo llamado **Nombre** se ingresa el nombre del funcionario o persona al cual se le creó el usuario y se presiona la opción de buscar ahora. Una vez encontrado el usuario se da clic derecho sobre él y se da clic izquierdo a la opción de **“Mover”**.



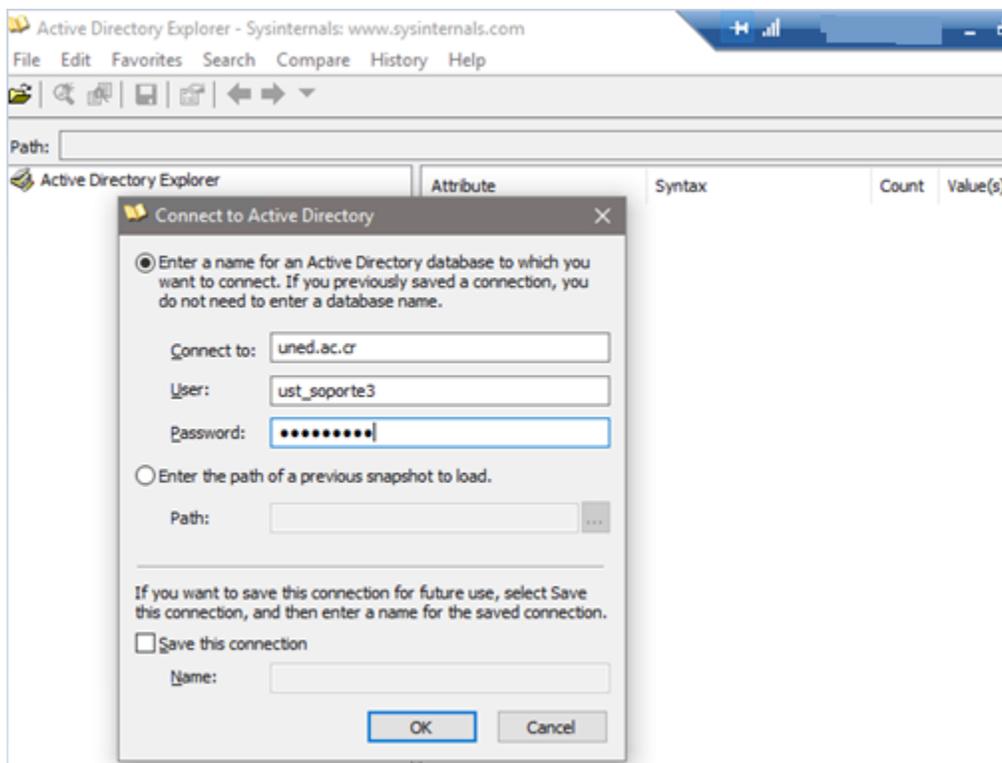
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

13. En la ventana “**Mover**” debe seleccionar la Unidad Organizacional donde debe estar ubicado el usuario nuevo. Una vez seleccionado debe dar clic al botón **Aceptar**.



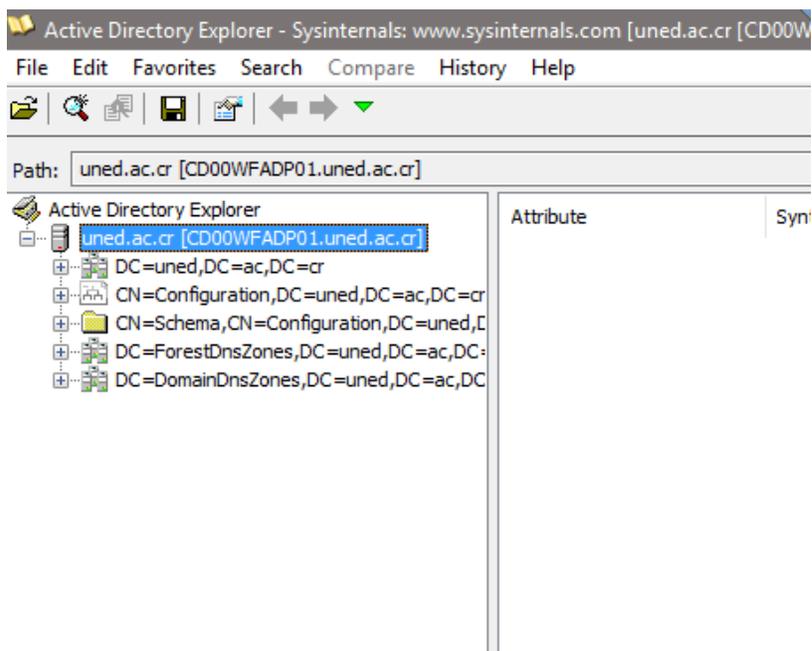
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

14. Si el usuario nuevo pertenece a un funcionario de la UNED, se debe agregar el número de cedula a las propiedades del usuario en el **Directorio Activo (Active Directory)**. Para esto debe ingresar al **Active Directory Explorer** y suministrar sus datos para validarse, luego dar clic al botón **OK**.



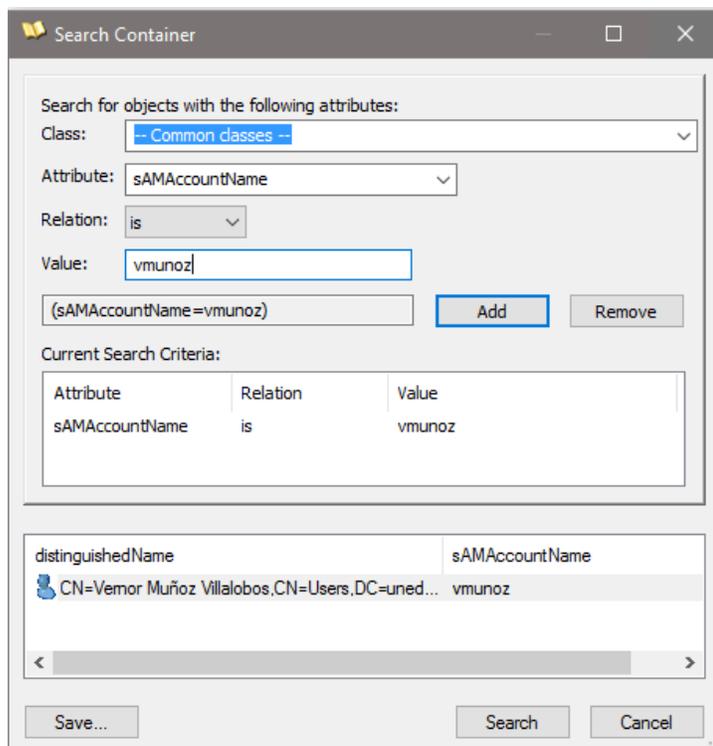
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

15. En la venta de “Active Directory Explorer” debe seleccionar “**uned.ac.cr**” y dar clic a la opción “**Search**” de menú superior.



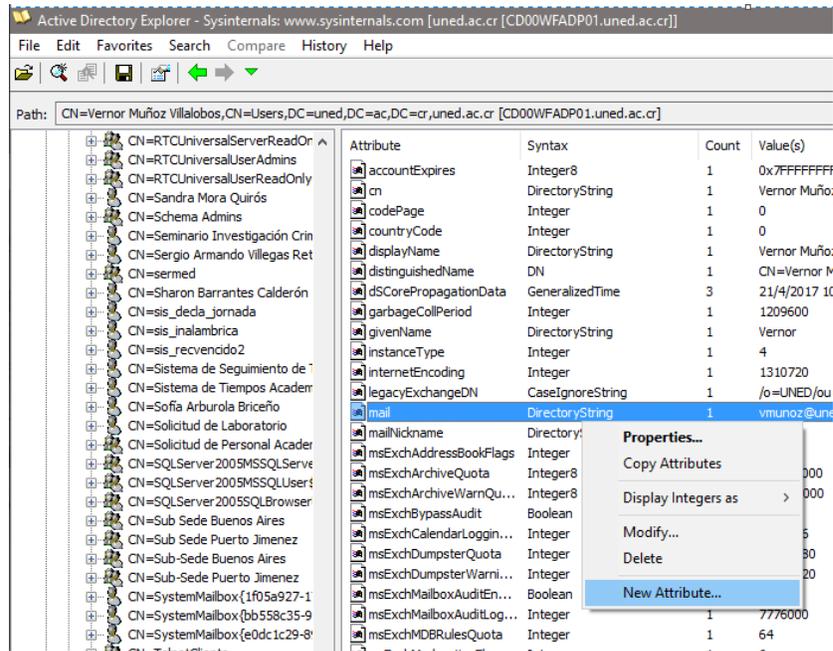
 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

16. En la venta de “**Search Container**” debe seleccionar la **Class “--Common classes--”**, y **agregar (Add)** el **atributo (attribute) sAMAccountName** con el **Valor (Value)** nombre de usuario del funcionario. Dar clic al botón **Search** de la ventana “**Search Container**”.



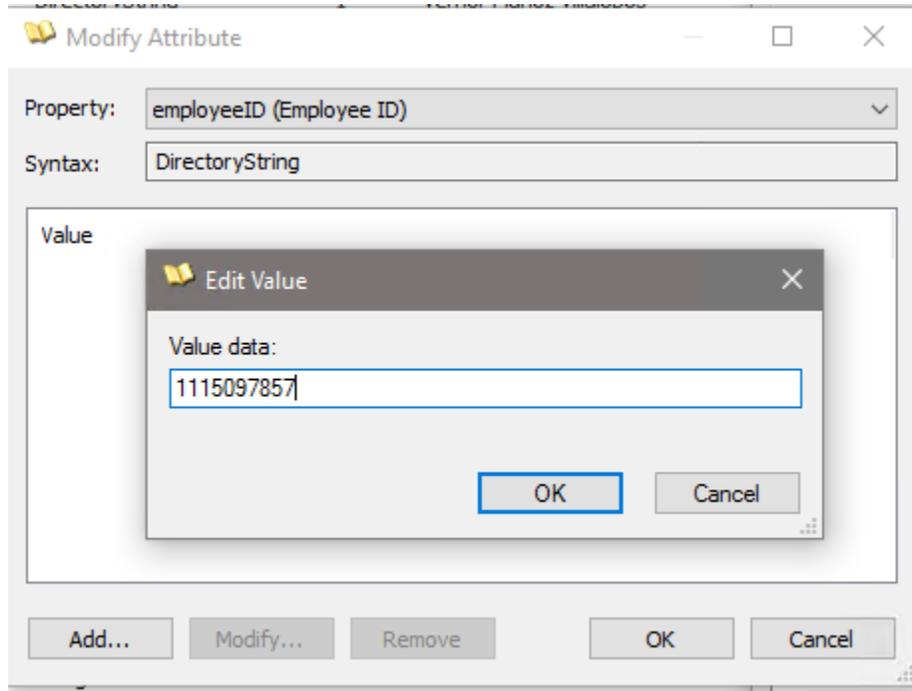
 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

17. Al dar clic al botón **“Search”** de la ventana **“SearchContainer”** se ubica al usuario nuevo, se debe posicionar sobre las propiedades, dar clic derecho y seleccionar nuevo atributo **“New Attribute”**”.



18. Se debe agregar como nuevo atributo **“employeeID (EmployeeID)”** y el valor correspondiente es la cedula del funcionario. Se da clic al botón **OK**.

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06



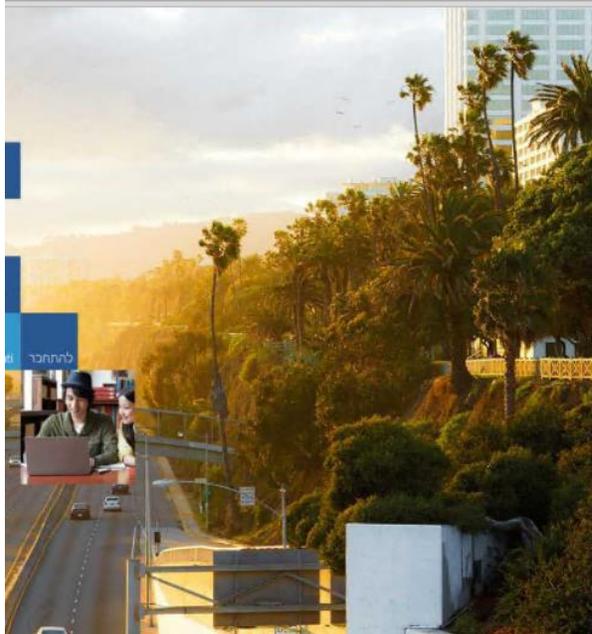
19. El nuevo atributo queda con el valor (cedula) asignado.

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFF
cn	DirectoryString	1	Vernor Muñoz Villalobos
codePage	Integer	1	0
countryCode	Integer	1	0
displayName	DirectoryString	1	Vernor Muñoz Villalobos
distinguishedName	DN	1	CN=Vernor Muñoz Villalobos,CN=L
dSCorePropagationData	GeneralizedTime	3	21/4/2017 10:43:30 a. m.;21/4/20
<b>employeeID</b>	<b>DirectoryString</b>	<b>1</b>	<b>1115097857</b>
garbageCollPeriod	Integer	1	1209600
givenName	DirectoryString	1	Vernor

20. Después de agregar el atributo de **“employeeID” (Employee ID)** y asignar el valor de numero de cedula del funcionario, se debe habilitar las licencias de correo electrónico del nuevo usuario en el Administrador de Exchange de Office 365. Se ingresa al Administrador de Exchange de Office 365, donde una vez ingresado las credenciales debe dar clic al botón de **“Iniciar sesión”**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

https://login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1492790146&rver=6.7.6640.0&wp=MCMBI&wreply=https%3a%2f%2fwww.uned.ac.cr



Cuenta profesional o educativa



ust\_soporte3@uned.ac.cr

Contraseña

Mantener la sesión iniciada

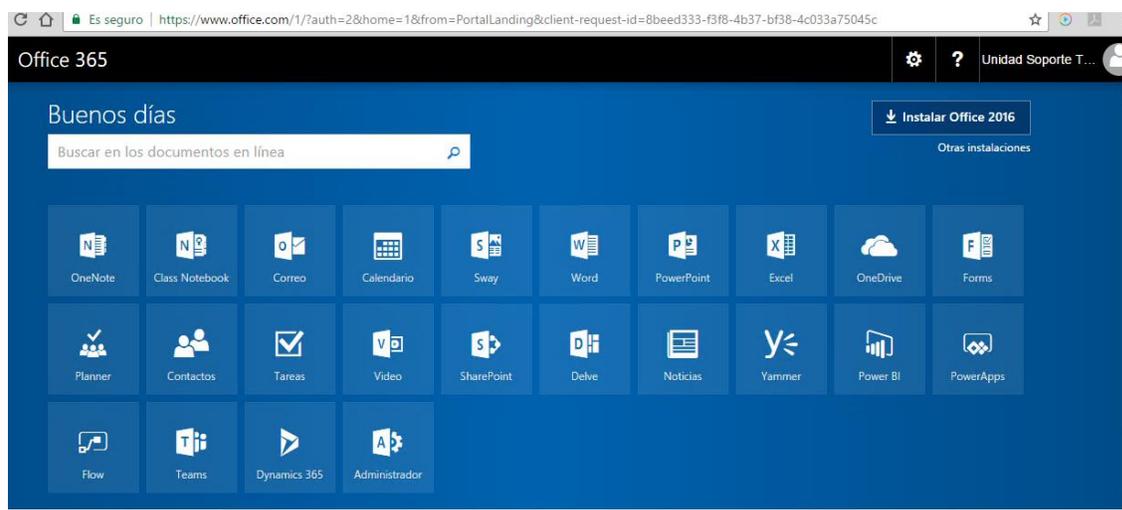
Iniciar sesión

Atrás

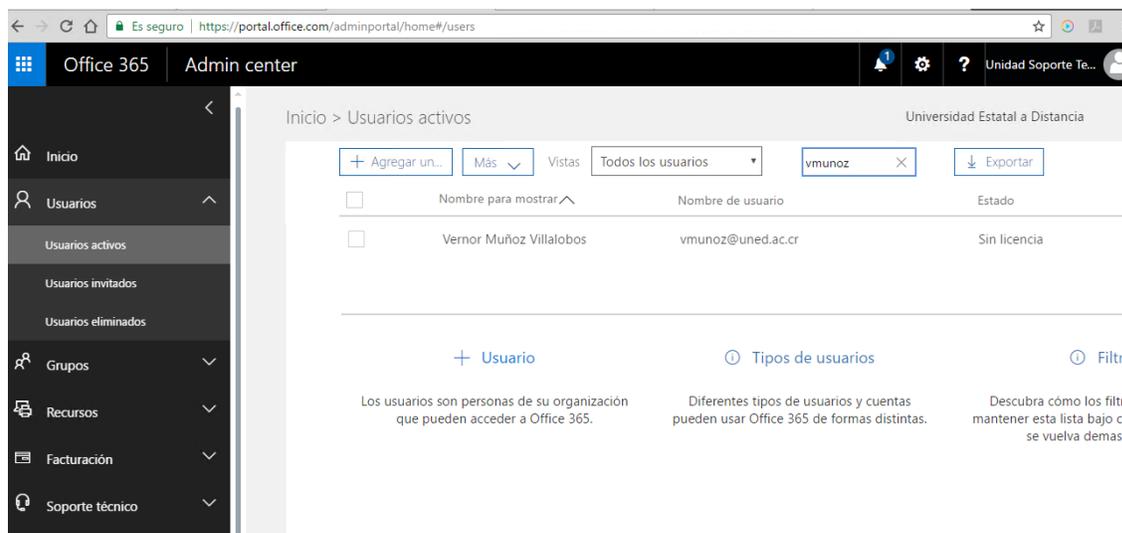
[¿No puede acceder a su cuenta?](#)

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

21. En la pantalla de “Administración de Office 365 de la UNED”, debe dar clic en la opción de “Administrador”.



22. En la pantalla de Administrador “Admin center”, debe seleccionar la opción “Usuarios” del menú vertical y posicionarse en la opción “Usuarios activos”. Ubicado en esta pantalla debe digitar el usuario y presionar el botón de “Enter” con el fin de filtrar la lista de usuarios. Una vez ubicado, debe dar doble clic sobre el nombre del usuario.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

23. Al dar doble clic sobre el nombre se carga las propiedades de Office 365 del usuario nuevo. Debe dar clic al enlace “Editar” de la opción “Licencias de productos”.

Vernor Muñoz Villalobos  
vmunoz@uned.ac.cr

↻ ✕

🔍 Restablecer contraseña

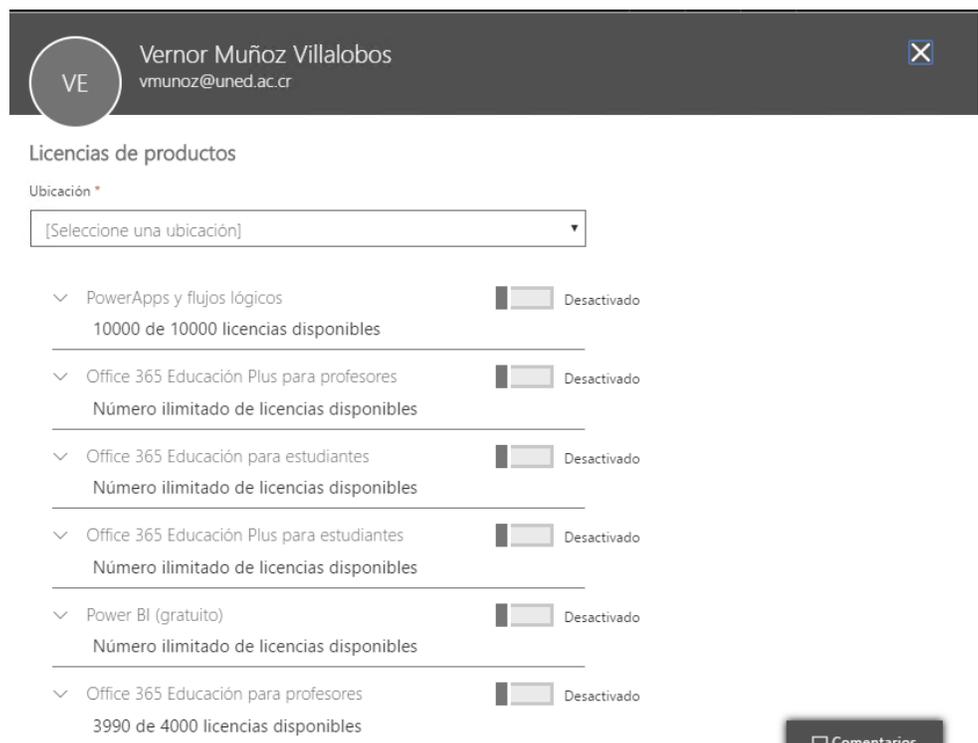
🗑 Eliminar usuario

Nombre de usuario	vmunoz@uned.ac.cr	<a href="#">Editar</a>
Licencias de productos	No se han asignado productos	<a href="#">Editar</a>
Pertenencia a grupos (0)	No hay grupos para el usuario. Haga clic en editar para cambiar la pertenencia al grupo.	<a href="#">Editar</a>
Estado de inicio de sesión	Inicio de sesión permitido	<a href="#">Editar</a>
Nombre para mostrar	Vernor Muñoz Villalobos	<a href="#">Editar</a>
Teléfono de la oficina		

Cerrar

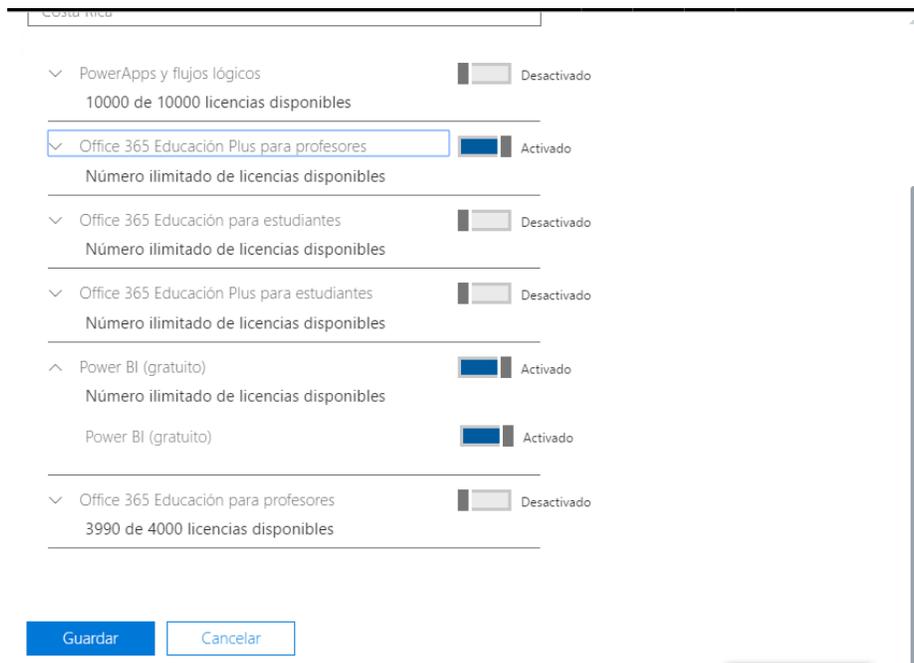
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

24. En la pantalla de “Licencias de productos”, debe activar las licencias “Office 365 Educación Plus para profesores” y “Power BI (gratuito)”.



25. La pantalla de “Licencias de productos” debe quedar de la siguiente forma. Posteriormente debe dar clic al botón “Guardar”.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



26. Una ventana le indicara que los productos fueron asignados. Debe dar clic al botón “Cerrar”.



27. La ventana de propiedades del usuario nuevo debe quedar de la siguiente forma.



**Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia**

Dependencia	Dirección de Tecnología, información Y comunicaciones
Fecha Aprobación	26/06/2017
Fecha revisión	26/06/2019
Código	MEGAC-PEGAC.03-PR-06

**VE** Vernor Muñoz Villalobos  
vmunoz@uned.ac.cr

[Restablecer contraseña](#) [Eliminar usuario](#)

Nombre de usuario	vmunoz@uned.ac.cr	<a href="#">Editar</a>
Licencias de productos	Office 365 Educación Plus para profesores Power BI (gratuito)	<a href="#">Editar</a>
Pertenencia a grupos (0)	No hay grupos para el usuario. Haga clic en editar para cambiar la pertenencia al grupo.	<a href="#">Editar</a>
Estado de inicio de sesión	Inicio de sesión permitido	<a href="#">Editar</a>
Instalaciones de Office	Ver y administrar los dispositivos en los que este usuario tiene instaladas aplicaciones de Office.	<a href="#">Editar</a>
Nombre para mostrar	Vernor Muñoz Villalobos	<a href="#">Editar</a>
Teléfono de la oficina		
Más opciones de configuración	Editar propiedades de Skype Empresarial	

[Cerrar](#) [Comentarios](#)

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### 3. Creación de Cuentas de Correo para Usuarios ya Existentes

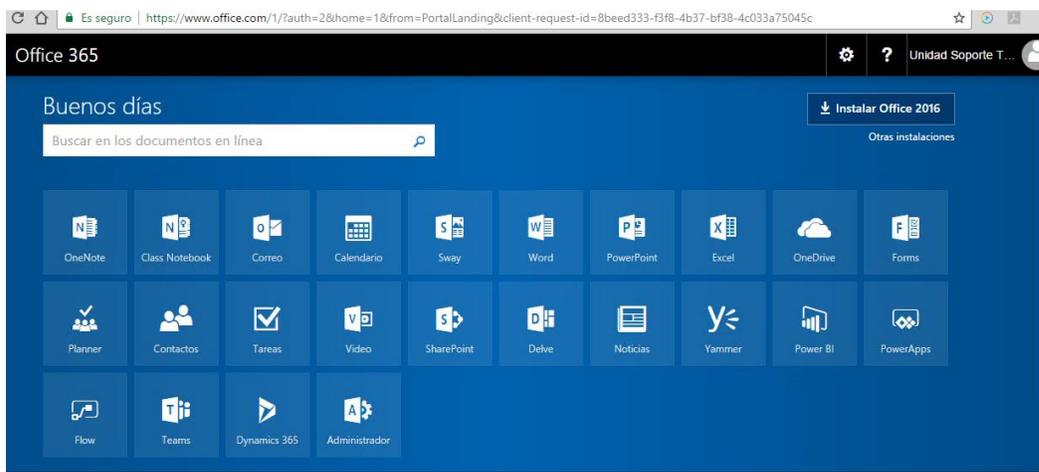
Para la creación de cuentas de correo debe venir la solicitud en el documento “**UEO-PL-002 Solicitud código de usuarios Producción**” (de ahora en adelante **UEO-PL-002**), este documento cuenta con una serie de opciones las cuales se completan según las necesidades para cada usuario, además debe venir con el visto bueno del encargado de área respectiva y firmado por el director de la Dirección de Tecnología.

1. Una vez recibida la solicitud con el visto bueno, Se ingresa al Administrador de Exchange de Office 365, donde una vez ingresado las credenciales debe dar clic al botón de “**Iniciar sesión**”.

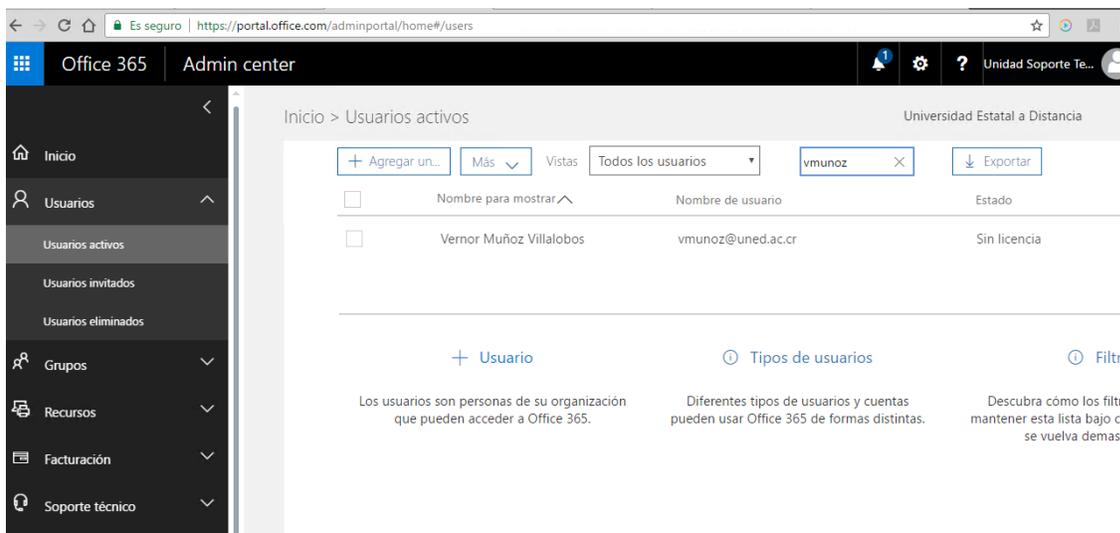


2. En la pantalla de “**Administración de Office 365 de la UNED**”, debe dar clic en la opción de “**Administrador**”.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



- En la pantalla de Administrador “**Admin center**”, debe seleccionar la opción “**Usuarios**” del menú vertical y posicionarse en la opción “**Usuarios activos**”. Ubicado en esta pantalla debe digitar el usuario y presionar el botón de “**Enter**” con el fin de filtrar la lista de usuarios. Una vez ubicado, debe dar doble clic sobre el nombre del usuario.



- Al dar doble clic sobre el nombre se carga las propiedades de Office 365 del usuario nuevo. Debe dar clic al enlace “**Editar**” de la opción “**Licencias de productos**”.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Vernor Muñoz Villalobos  
vmunoz@uned.ac.cr

Restablecer contraseña Eliminar usuario

Nombre de usuario	vmunoz@uned.ac.cr	Editar
Licencias de productos	No se han asignado productos	Editar
Pertenencia a grupos (0)	No hay grupos para el usuario. Haga clic en editar para cambiar la pertenencia al grupo.	Editar
Estado de inicio de sesión	Inicio de sesión permitido	Editar
Nombre para mostrar	Vernor Muñoz Villalobos	Editar
Teléfono de la oficina		

Cerrar

5. En la pantalla de “**Licencias de productos**”, debe activar las licencias “**Office 365 Educación Plus para profesores**” y “**Power BI (gratuito)**”.

Vernor Muñoz Villalobos  
vmunoz@uned.ac.cr

Licencias de productos

Ubicación \*

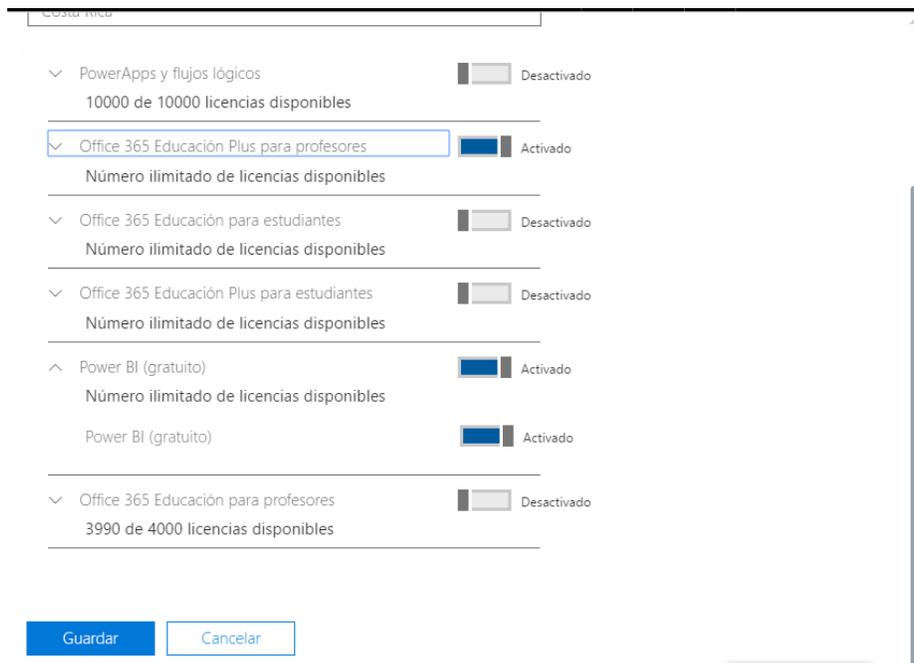
[Seleccione una ubicación]

- PowerApps y flujos lógicos 10000 de 10000 licencias disponibles  Desactivado
- Office 365 Educación Plus para profesores Número ilimitado de licencias disponibles  Desactivado
- Office 365 Educación para estudiantes Número ilimitado de licencias disponibles  Desactivado
- Office 365 Educación Plus para estudiantes Número ilimitado de licencias disponibles  Desactivado
- Power BI (gratuito) Número ilimitado de licencias disponibles  Desactivado
- Office 365 Educación para profesores 3990 de 4000 licencias disponibles  Desactivado

Comentarios

6. La pantalla de “**Licencias de productos**” debe quedar de la siguiente forma. Posteriormente debe dar clic al botón “**Guardar**”.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



7. Una ventana le indicara que los productos fueron asignados. Debe dar clic al botón **“Cerrar”**.



8. La ventana de propiedades del usuario nuevo debe quedar de la siguiente forma.



**Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia**

Dependencia

Dirección de Tecnología, información Y comunicaciones

Fecha Aprobación

26/06/2017

Fecha revisión

26/06/2019

Código

MEGAC-PEGAC.03-PR-06

 Vernor Muñoz Villalobos  
vmunoz@uned.ac.cr

[Restablecer contraseña](#) [Eliminar usuario](#)

Nombre de usuario	vmunoz@uned.ac.cr	<a href="#">Editar</a>
Licencias de productos	Office 365 Educación Plus para profesores Power BI (gratuito)	<a href="#">Editar</a>
Pertenencia a grupos (0)	No hay grupos para el usuario. Haga clic en editar para cambiar la pertenencia al grupo.	<a href="#">Editar</a>
Estado de inicio de sesión	Inicio de sesión permitido	<a href="#">Editar</a>
Instalaciones de Office	Ver y administrar los dispositivos en los que este usuario tiene instaladas aplicaciones de Office.	<a href="#">Editar</a>
Nombre para mostrar	Vernor Muñoz Villalobos	<a href="#">Editar</a>
Teléfono de la oficina		
Más opciones de configuración	Editar propiedades de Skype Empresarial	

[Cerrar](#) [Comentarios](#)

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## 1. Creación del Grupo de Distribución

- Una vez recibida la solicitud en el documento **UEO-PL-002** con su respectivo visto bueno, se deberá ingresar al Centro de Administración de Exchange.

### Centro de administración de Exchange

Dirección de correo electrónico:

Contraseña:

**iniciar sesión**

- En el Centro de Administración de Exchange se debe posicionar en la opción del Menú Vertical “**destinatarios**” dar clic en la pestaña “**grupos**”. Ubicado en esta opción se debe dar clic al botón “+” y seleccionar “**Grupo de distribución**”.

buzones **grupos** recursos contactos compartido migración

+ -     ...

	TIPO DE GRUPO	DIRECCIÓN DE CORREO ELECTRÓNICO
<ul style="list-style-type: none"> <li>Grupo de distribución</li> <li>Grupo de seguridad</li> <li>Grupo de distribución dinámico</li> </ul>	<b>Grupo de seguridad</b>	<b>vic.planificacion@uned.ac.cr</b>
Vicerrectoria Academica	Grupo de seguridad	Vicerrectoria.Ejecutiva@uned.ac.cr
vencimiento	Grupo de seguridad	Vic.academica@uned.ac.cr
Unidad Mantenimiento	Grupo de distribución	vencimiento@uned.ac.cr
Unidad Estratégica de Sistemas de Informa...	Grupo de distribución	mantenimiento@uned.ac.cr
	Grupo de distribución	dticuesi@uned.ac.cr

- Se abre la pantalla **Grupo de distribución (nuevo grupo de distribución)** donde se deberá ingresar el Nombre para mostrar, el Alias, seleccionar a Unidad Organizativa donde debe estar ubicado el grupo de

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

distribución, agregar el propietario del grupo, agregar los miembros y marcar **“Aprobación del propietario”**. Se da clic al botón **Guardar**.

The image displays two screenshots of the 'Nuevo grupo de distribución' (New distribution group) web form in Google Chrome. The URL is <https://correo.uned.ac.cr/ecp/UsersGroups/NewPlainDistribution>.

**Left Screenshot:** Shows the form fields:

- \*Nombre para mostrar: Tutores
- \*Alias: listadetutores
- Descripción: (empty text area)
- Unidad organizativa: uned.ac.cr/UNED/Centra (with 'Examinar...' button)
- \*Propietarios: Juan Perez Perez (with '+ -' controls)
- Miembros: (empty list)
- Buttons: guardar, cancelar

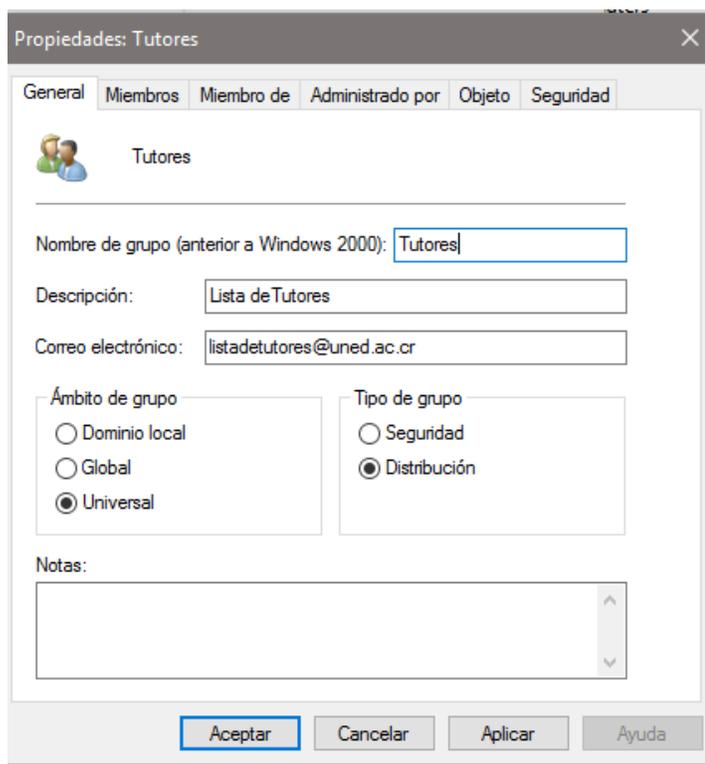
A tooltip points to the 'Propietarios' field with the text: "Los grupos deben tener al menos un propietario que debe administrar el grupo. De manera predeterminada, se le agregará como propietario del grupo que esté creando. Para agregar otros propietarios, haga clic en Agregar."

**Right Screenshot:** Shows the 'Miembros' section:

- Checkbox:  Agregar propietarios de grupo como miembros
- + - controls
- Member list: Erick López Agüero, Juan Perez Perez (highlighted)
- Options for group approval:
  - Abierto: cualquiera puede unirse a este grupo sin la aprobación de los propietarios del grupo.
  - Cerrado: solo pueden agregar miembros los propietarios del grupo. Se rechazarán automáticamente todas las solicitudes para unirse.
  - Aprobación del propietario: todas las solicitudes son aprobadas o rechazadas por los propietarios del grupo.
- Options for group abandonment:
  - Abierto: cualquiera puede abandonar este grupo sin la aprobación de sus propietarios.
  - Cerrado: solamente pueden quitar miembros los propietarios del grupo. Se rechazarán automáticamente todos los pedidos para abandonar.
- Buttons: guardar, cancelar

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. En caso de ser necesario se puede agregar una descripción del Grupo de distribución a nivel de Directorio Activo (Active Directory).



## 5. Entrega del Usuario

1. Una vez finalizada la creación del usuario, se llena el documento **UEO-PL-002** con los datos:
  - a. Nombre de la persona que creó el usuario
  - b. Fecha de realización
  - c. Firma
  - d. Descripción (nombre usuario, contraseña, grupo o lista de distribución)

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Realizado por _____ (a)	(b) Fecha: _____
Nombre Completo: _____	(c) Firma: _____
Descripción de lo realizado: (d)	
Usuarios:	
Grupos:	
Listas de distribución:	
Observaciones: _____	
_____	

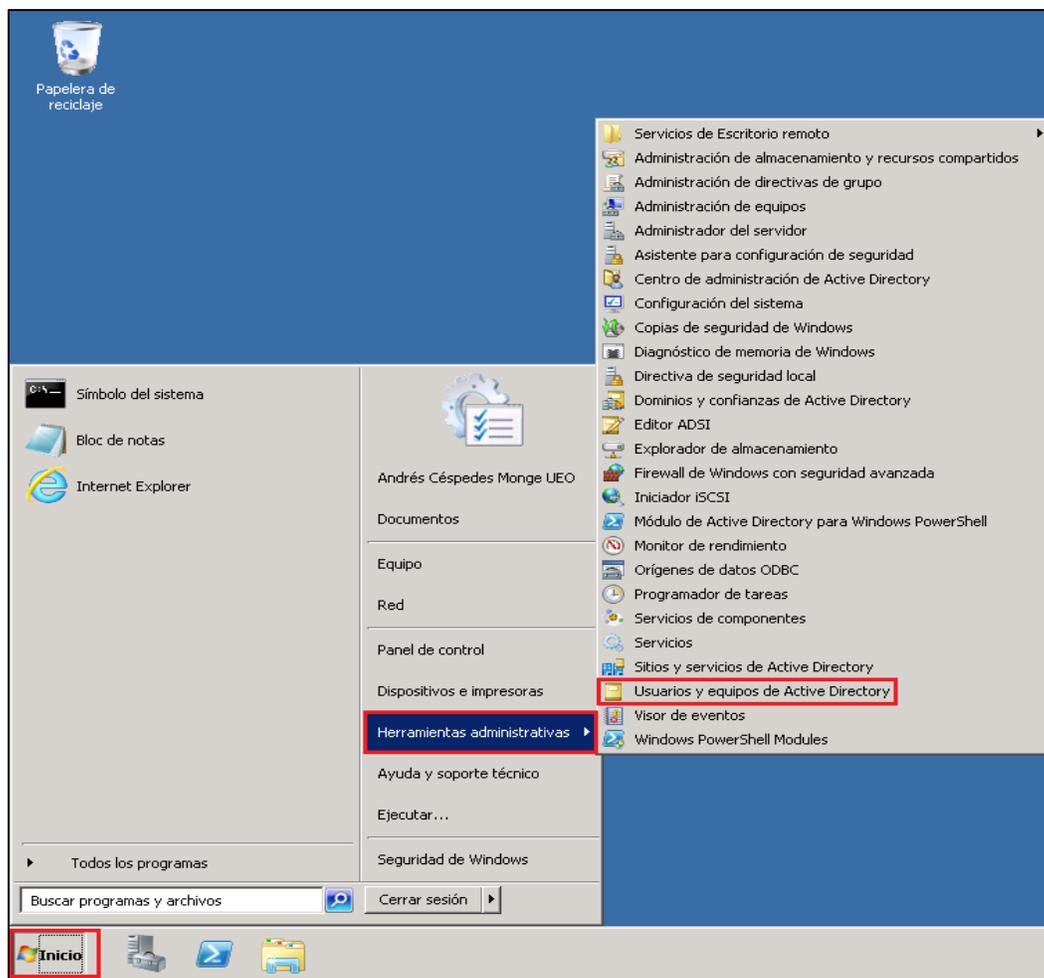
2. Se entregará la boleta al responsable de creación de usuarios, quién envía una copia en digital al coordinador de la *Unidad de Seguridad*, esto con el fin de que pueda verificar la realización de la solicitud de forma correcta.
3. El responsable de creación de usuarios, comunica a los usuarios que deben retirar la información en la Dirección de Tecnología, con su respectiva cedula, para la entrega de su usuario y contraseña.
4. El responsable de creación de usuarios entrega la boleta al encargado de recepción para archivo.

## 6. Inhabilitar cuentas de usuario

Para proceder a deshabilitar cuentas de usuarios se debe contar con un documento oficial (cese de funciones, defunción, jubilación) de Recursos Humanos o un comunicado por correo electrónico del jefe del área que solicite.

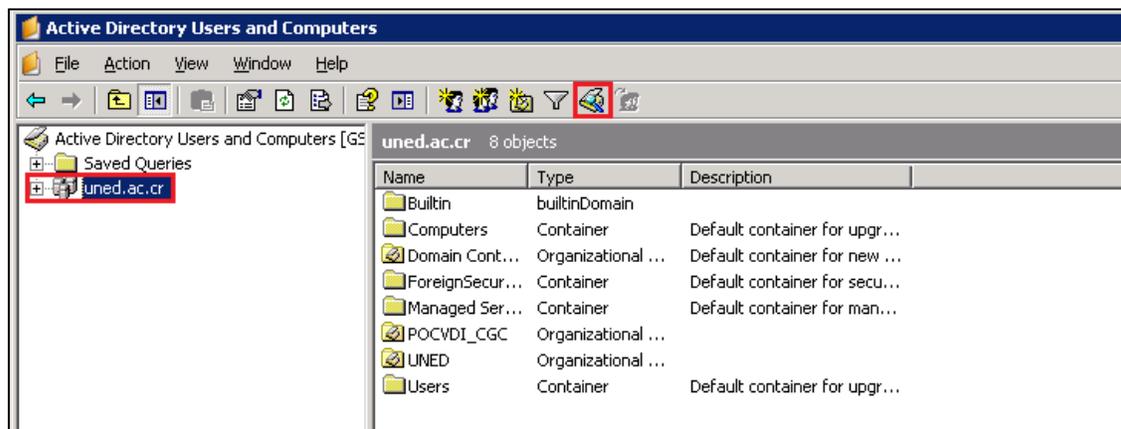
1. Una vez recibida la solicitud con su respectivo visto bueno, se deberá ingresar al servidor que tenga el rol de Active Directory instalado, ya en el equipo se debe presionar el botón de **Inicio**. buscar la opción **Herramientas Administrativas** y en **Usuarios y Equipos de Active Directory**, dar Click.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

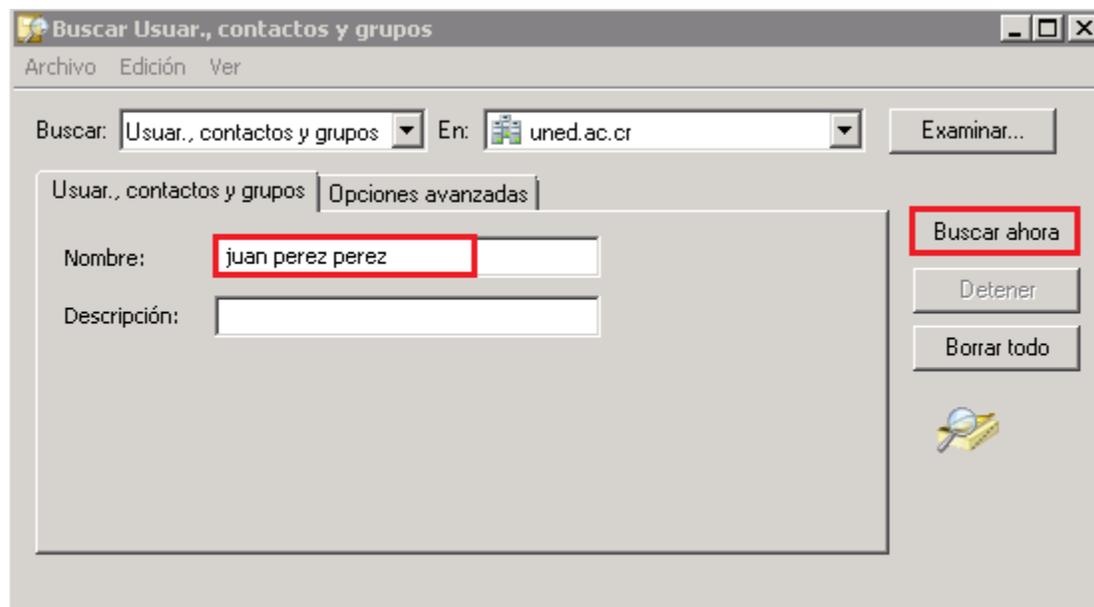


 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

Se abre la pantalla **Active Directory Users and Computers** donde se selecciona el dominio “**uned.ac.cr**”, luego presionamos la opción de buscar usuarios.

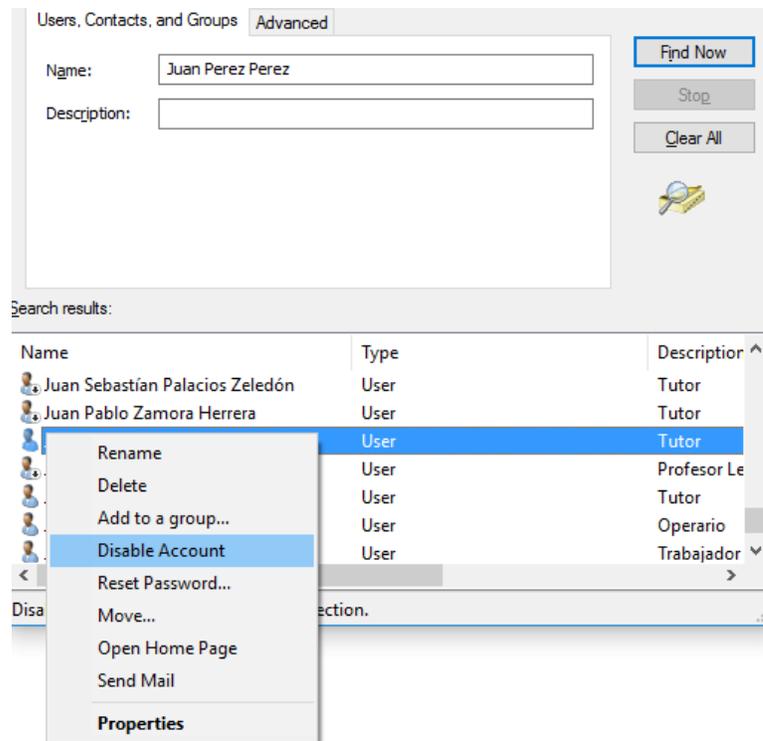


2. En la ventana **Buscar Usuar., contactos y grupos** se ingresa el usuario nombre al cual se cancela el buzón de correo y se presiona la opción de **buscar ahora**.

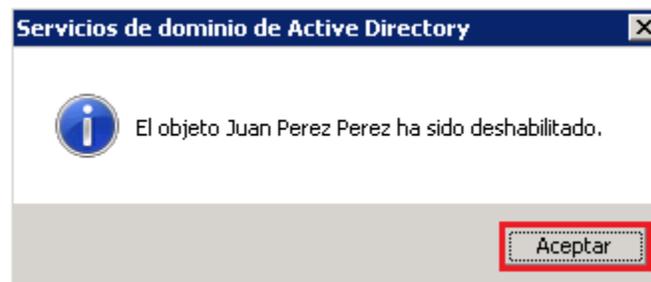


	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- Sobre esa pantalla aparecerá el usuario que se está buscando y sobre el usuario se presiona click derecho para que aparezcan las opciones de usuario, se selecciona **“Deshabilitar Cuenta (Disable Account)”**,

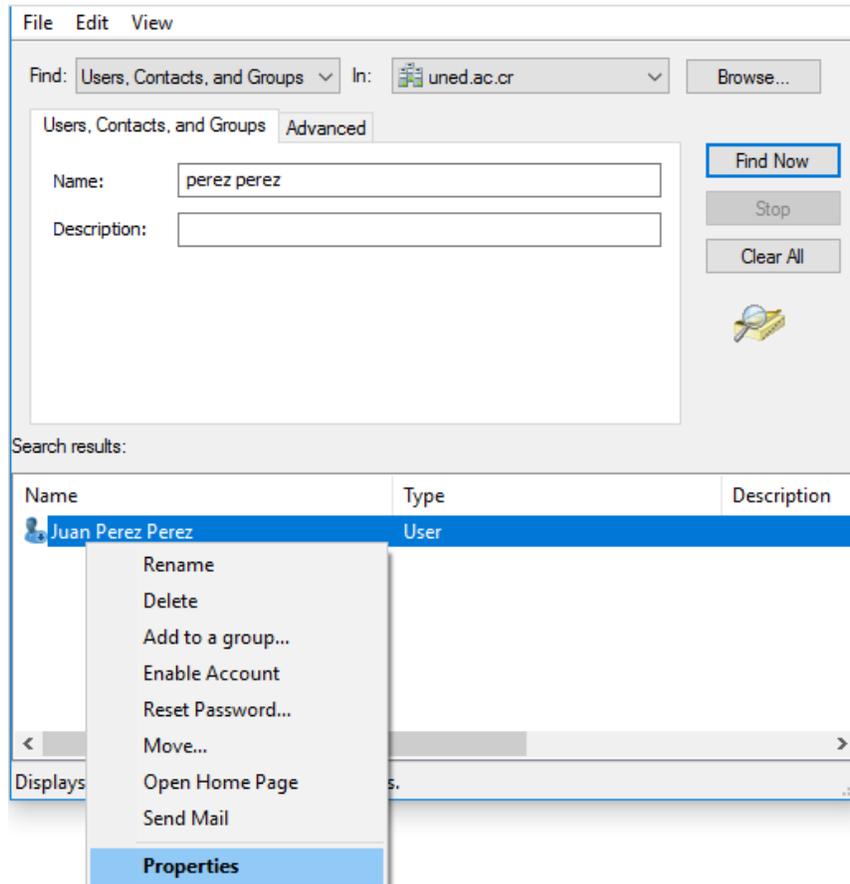


- Luego de esto saldrá un mensaje comunicando que la cuenta se desactivo y se presiona Aceptar.



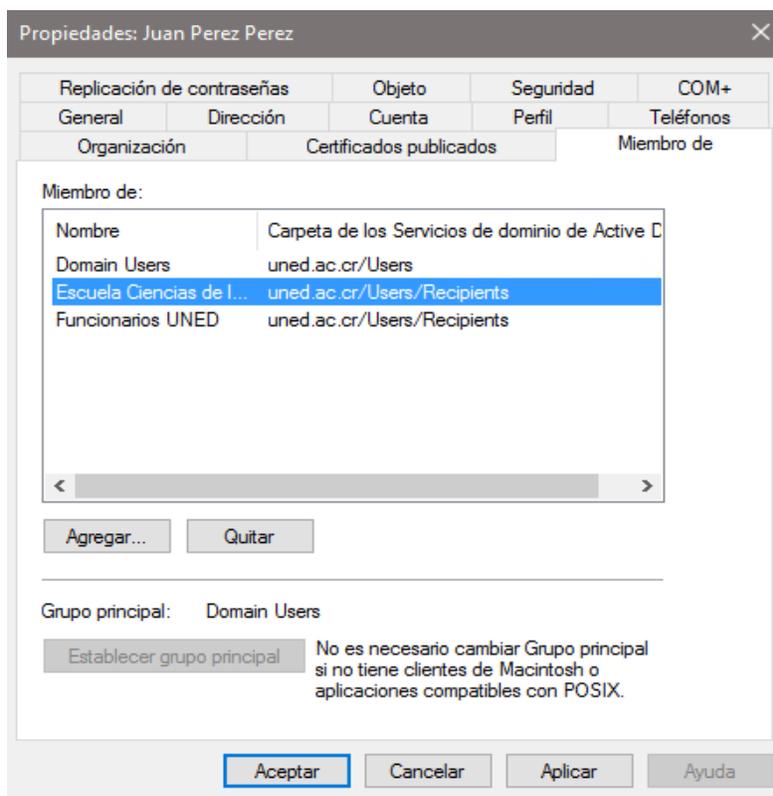
 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

5. Una vez deshabilitada la cuenta, debe dar clic derecho nuevamente sobre el usuario y seleccionar “Propiedades (Properties)”.



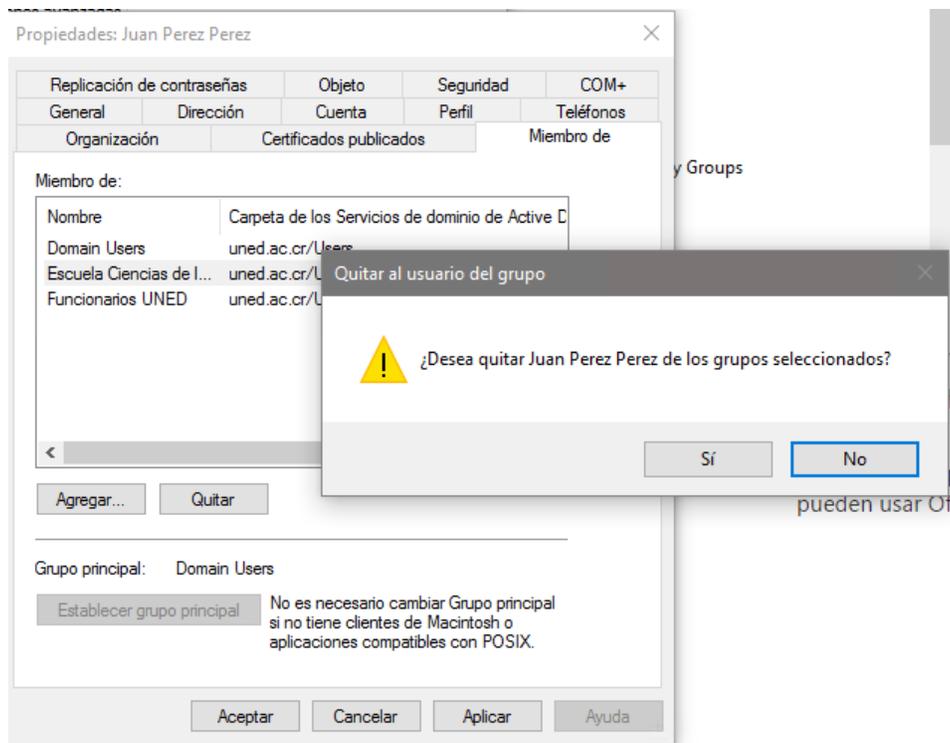
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

6. Sobre esa pantalla aparecerá las propiedades del usuario y debe dar clic sobre la pestaña “**Miembro de**”.



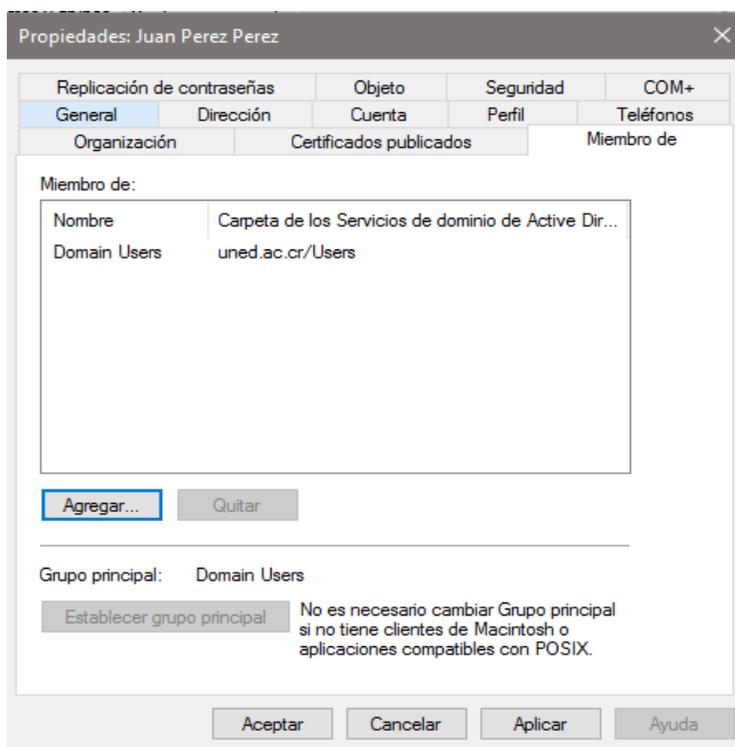
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

7. Ubicado en la pestaña “**Miembro de**” debe seleccionar cada uno de los grupos y dar clic al botón “**Quitar**”, el sistema le consultará si desea quitar al usuario de los grupos seleccionados, para lo cual debe dar clic al botón “**Sí**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

8. En la pestaña “Miembro de” debe asegurarse que el usuario deshabilitado solo quede incluido en el grupo de “**Domain Users**”. Posteriormente se da clic al botón **Aceptar**.



9. Una vez deshabilitado el usuario y excluido de los grupos al cual pertenecía, se procede a quitar el usuario de la **lista de direcciones**. Se debe ingresar al Centro de Administración de Exchange: <https://correo.uned.ac.cr/ecp/>.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Centro de administración de Exchange

Dirección de correo electrónico:

Contraseña:

[➔ iniciar sesión](#)

- En la opción del Menú **“destinatarios”** debe digitar el usuario deshabilitado, y presionar el botón de **“Enter”**, esto con el fin de filtrar la lista de destinatarios. Debe dar doble clic sobre el nombre del funcionario deshabilitado.

Centro de administración de Exchange

destinatarios | buzones | grupos | recursos | contactos | compartido | migración

permisos  
administración de cumplimiento  
organización  
protección  
flujo de correo  
móvil  
carpetas públicas  
mensajería unificada

NOMBRE PARA MOSTRAR	TIPO DE BUZÓN	DIRECCIÓN DE CORREO ELECTRÓNICO
Erick López Agüero	Office 365	elopez@uned.ac.cr

Erick López Agüero

Buzón del usuario remoto  
elopez@uned.ac.cr

Tratamiento: AUXILIAR ADMINISTRATIVO  
Oficina: DIR. TECNOLOGIA INF. Y COM  
Teléfono del trabajo: 2234-3236 ext 3695

Archivo local  
Archivado: Deshabilitado  
[Habilitar](#)

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

Al dar doble clic sobre el nombre del funcionario deshabilitado, se abre una pantalla con propiedades del usuario, debe deseleccionar la opción **“Ocultar de las listas de direcciones”**. Después debe presionar el botón **“guardar”**.

Buzón de Office 365 - Google Chrome

Es seguro | <https://correo.uned.ac.cr/ecp/UsersGroups/EditRemoteMailbox.aspx?pwmcid=4&ReturnObjectTy>

Erick López Agüero Ayuda

► **General**

Información de contacto organización

Dirección de correo electrónico

Configuración del flujo de correo

Miembro de

Sugerencia de correo electrónico

Nombre: Erick

Iniciales:

Apellidos: López Agüero

\*Nombre: Erick López Agüero

\*Nombre para mostrar: Erick López Agüero

\*Nombre de inicio de sesión del usuario: elopez @ uned.ac.cr

Pedir el cambio de contraseña en el siguiente inicio de sesión

**Ocultar de las listas de direcciones**

[Más opciones...](#)

guardar cancelar

Si seleccionas esta opción, el usuario no aparecerá en la libreta de direcciones de tu organización ni en otras listas de direcciones, pero seguirá recibiendo el correo enviado a él.

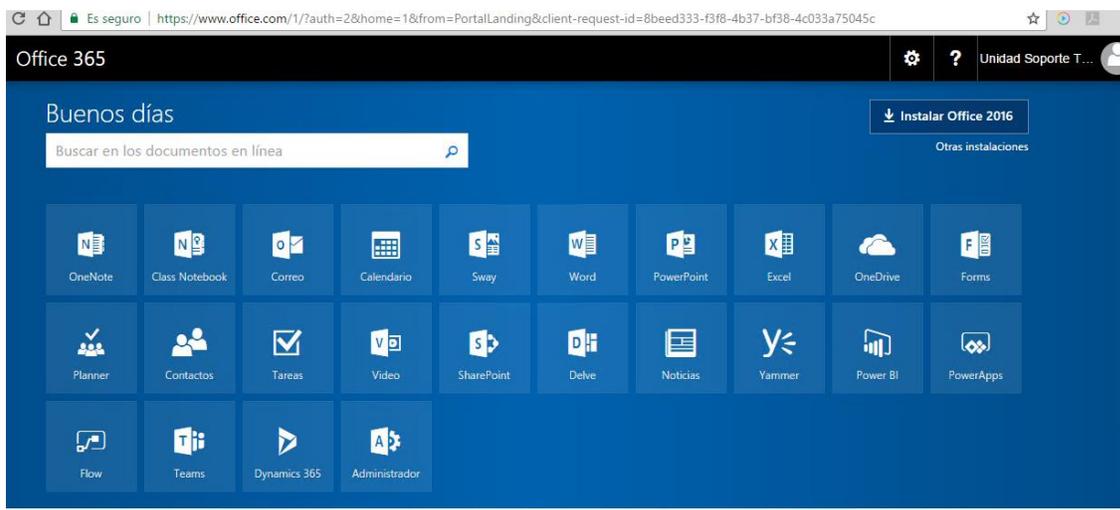
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

11. Como último paso se debe desactivar la licencia de Office 365, para lo cual se debe ingresar al área de **“Administración de Office 365 de la UNED”**. Una vez ingresado las credenciales debe dar clic al botón de **“Iniciar sesión”**.

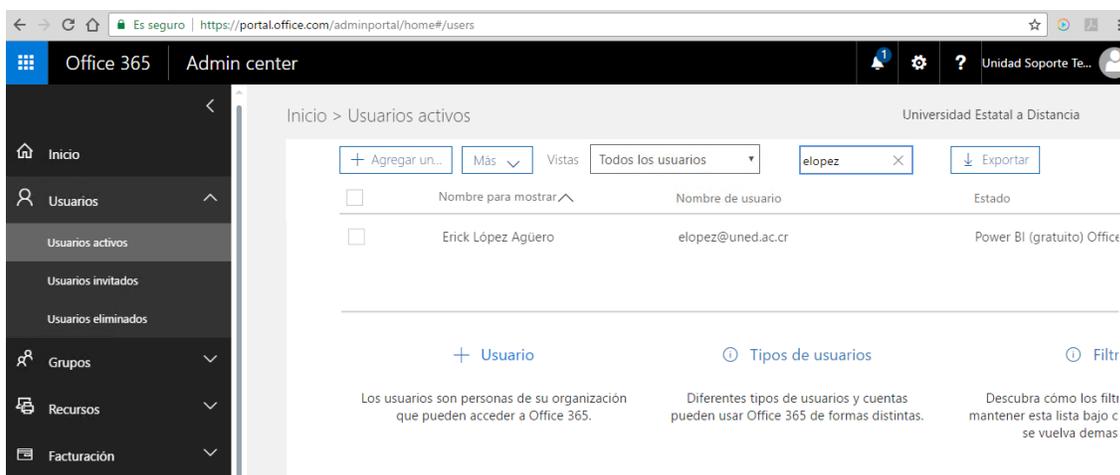


12. En la pantalla de **“Administración de Office 365 de la UNED”**, debe dar clic en la opción de **“Administrador”**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

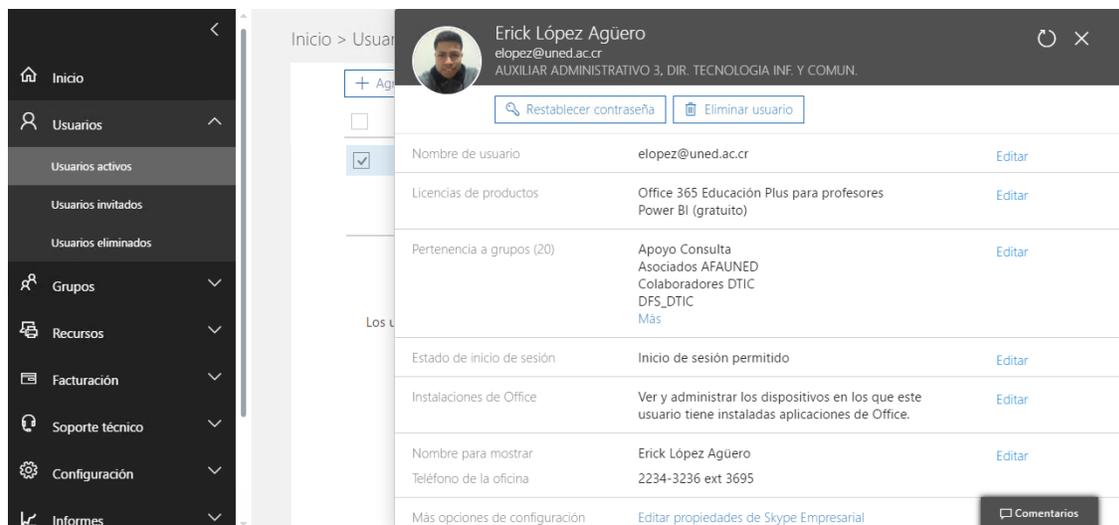


13. En la pantalla de Administrador “**Admin center**”, debe seleccionar la opción “**Usuarios**” del menú vertical y posicionarse en la opción “**Usuarios activos**”. Ubicado en esta pantalla debe digitar el usuario deshabilitado y presionar el botón de “**Enter**” con el fin de filtrar la lista de usuarios. Una vez ubicado, debe dar doble clic sobre el nombre del usuario.



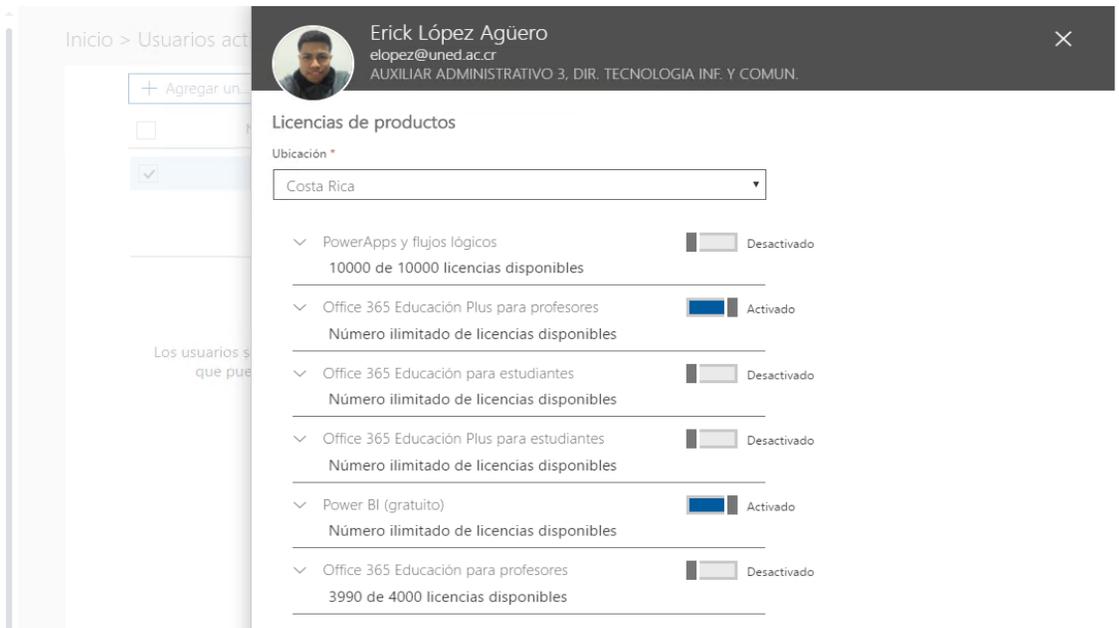
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

14. Al dar doble clic sobre el nombre se carga las propiedades de Office 365 del usuario deshabilitado. Debe dar clic al enlace **“Editar”** de la opción **“Licencias de productos”**.

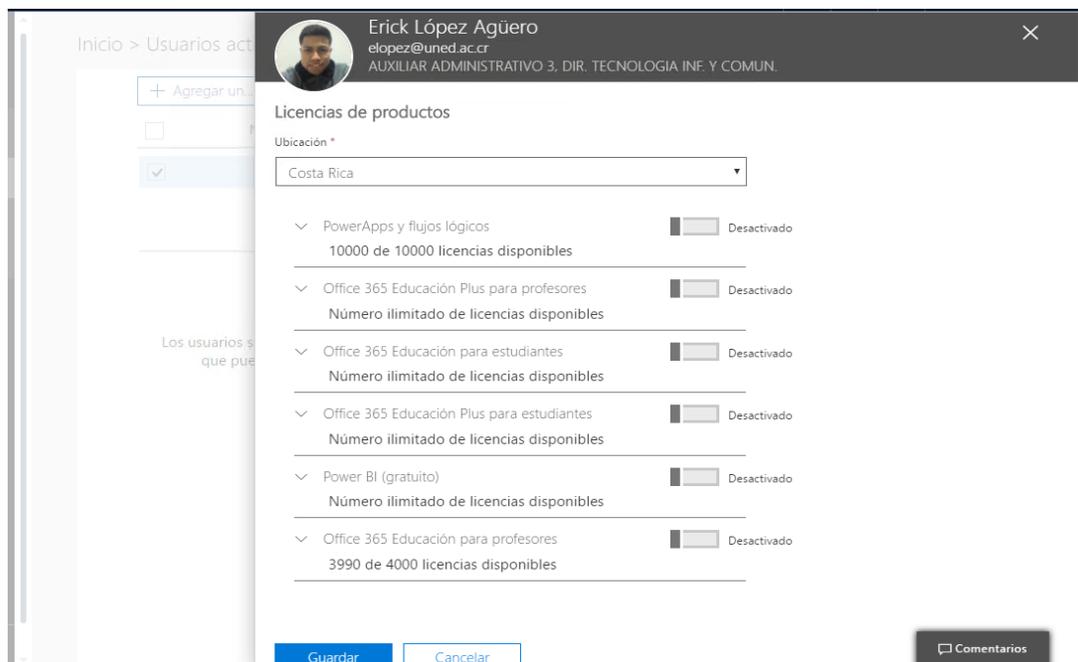


15. En la pantalla de **“Licencias de productos”**, debe desactivar las licencias **“Office 365 Educación Plus para profesores”** y **“Power BI (gratuito)”**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



16. La pantalla de “**Licencias de productos**” debe quedar de la siguiente forma. Posteriormente debe dar clic al botón “**Guardar**”.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para la Administración de Usuarios, roles y privilegios en ORACLE

### ¿En qué consisten los roles y privilegios de ORACLE?

Es el conjunto de privilegios que se pueden otorgar a un usuario o a otro Rol, utilizados para conectarse y realizar diferentes operaciones en una Base de Datos ORACLE, utilizando de por medio un **nombre de usuario**, el cual el motor de Base de Datos autentifique que es válido y autorizado.

### Conceptos

- **Base de datos:** es un “almacén” que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.
- **ORACLE:** Sistema de gestión de base de datos de tipo objeto-relacional desarrollado por la Corporación Oracle.
- **Roles de base de datos:** Los roles son una forma de simplificar el proceso de gestión de privilegios sobre objetos de Base de Datos.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

1. El usuario debe estar **asignado a una Base de Datos** y dentro de ella estar **asociado a un tablespace por defecto y a uno temporal, y al menos a un rol de Base de Datos**, por medio del cual se le otorgan o deniegan los **permisos** (*select, insert, delete, update, execute, etc.*), sobre los diferentes **objetos de Base de Datos** (*tablas, vistas, procedimientos almacenados, funciones, etc.*) y cumplir con ciertas características que se detallan más adelante.
2. ORACLE provee tres **métodos de autenticación** para cada cuenta de usuario:
  - a. Autenticación de contraseña
  - b. Autenticación de sistema operativo
  - c. Autenticación global de usuario

### Autenticación mediante contraseña:

1. Cuando un usuario conecta con una base de datos verifica que este usuario y la contraseña introducida almacenada en la base de datos, sea correcta. Las contraseñas se guardan encriptadas en la base de datos (en el Diccionario de Datos).

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

### Autenticación externa o sistema operativo:

1. Al conectarse el usuario con la Base de Datos, se verifica que el nombre de usuario es el mismo que el nombre de usuario del sistema operativo para permitir la validación.
2. No se almacenan las cuentas en la Base de Datos de ninguna forma. Estas cuentas están siempre referidas con **OPSS**

### Autenticación global:

1. Al realizar la conexión el usuario con la Base de Datos, se verifica globalmente cuando la información pasa por una opción avanzada de seguridad (**ADVANCED SECURITY OPTION**) para la autenticación, tal como **Kerberos, RADIUS ....**
2. Para las cuentas globales no se almacena tampoco nada en la Base de Datos.

### En cuanto a la Relación de los roles de las bases de datos

1. Se pueden crear cuantos roles sean necesarios para una aplicación o sistema, y ser asignados a los usuarios existentes.
2. De esta forma, cuando se desee revocar un privilegio para un usuario, solamente se debe de revocar la asignación del rol al usuario, en vez de revocar cada privilegio de forma individual.

### En cuanto a otorgar privilegios a Rol de Base de Datos en ORACLE

1. Una vez creados los usuarios y que estos hayan sido asignados a roles de Base de Datos, es necesario dotarlos de privilegios para que puedan realizar operaciones específicas en la Base de Datos.
2. Los privilegios a otorgar suelen clasificarse en:
  - a. **Privilegios del sistema** (*permiten al usuario realizar algún tipo de operación que afecte a todo el sistema manejador de Base de Datos*), y
  - b. **Privilegios de objetos** (*permiten al usuario realizar operaciones específicas sobre objetos específicos como tablas, vistas, procedimientos, etc.*)
3. Los privilegios de sistema por lo general son aquellos que ejecutan una sentencia del tipo **CREATE, DROP, ALTER**, mientras que los privilegios de objeto están

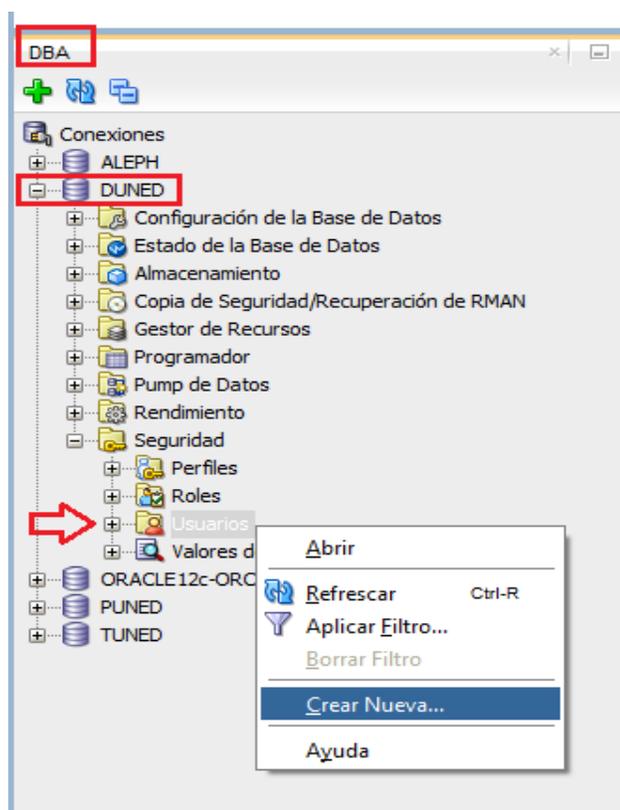
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

relacionados a la ejecución de sentencias como **SELECT, INSERT, DELETE, UPDATE, EXECUTE.**

## Actividades para realizar el trámite de Usuarios, roles y privilegios

### (1) Creación de usuarios en Oracle

1. Conéctese a la Base de Datos por medio de la herramienta de **SQL Developer** con un usuario con privilegios de **Administrador.**
2. En la vista del DBA seleccione y expanda la **Base de Datos** donde creará el usuario. Luego seleccione y expanda la carpeta de **Seguridad.**
3. Sobre la carpeta de **Usuarios** de click derecho del mouse y seleccione la opción **Crear Nuevo.**



4. En el cuadro de propiedades para Crear Usuario se debe indicar:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- a. **Usuario:** un nombre de usuario que guarde relación con el sistema al que pertenece.
- b. **Contraseña Nueva:** escriba una contraseña para el nuevo usuario que esté compuesta como mínimo de diez caracteres, donde se combinen letras mayúsculas-minúsculas, valores numéricos y caracteres especiales.
- c. **Confirmar Contraseña:** repita la misma contraseña ingresada en el punto anterior. En caso de que no coincidan se producirá un error.
- d. Adicionalmente hay otras opciones que se pueden activar para el usuario como:
  - i. **Vencimiento de la contraseña** que obliga al usuario a cambiarla la siguiente ocasión que intente conectarse.
  - ii. **Usuario de Sistema Operativo:** al conectarse el usuario con la Base de Datos, se verifica que el nombre de usuario es el mismo que el nombre de usuario del sistema operativo para permitir la validación.
  - iii. **Bloqueo de cuenta:** se crea la cuenta de usuario, pero ésta queda bloqueada de forma automática.
  - iv. **Edición Activada**

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- e. **Tablespace por Defecto:**indicar el tablespace que tendrá por defecto el usuario. El estándar seguido en la DTIC indica que los usuarios tendrán **USERS** como tablespace por defecto.
- f. <sup>26</sup>**Tablespace Temporal:** indicar el tablespace que tendrá de forma temporal el usuario. El estándar seguido en la DTIC indica que los usuarios tendrán **TEMP** como tablespace temporal.
- g. **Roles Otorgados:** para que un usuario pueda realizar al menos la conexión con la Base de datos, se le debe asignar el rol llamado **SESSION**, pero para poder interactuar con los objetos de Base de datos propios del sistema al cual estará asignado, se le deberán indicar los Roles respectivos. Este tema se trata en detalle en la sección de Roles de Base de Datos.

<sup>26</sup>Un tablespace temporal se utiliza para almacenar “segmentos” temporales que son creados durante operaciones como ORDER BY,SELECT DISTINCT, MERGE JOIN o CREATE INDEX. A veces a los usuarios se les asocia un tablespace temporal para realizar este tipo de operaciones, cuando estas operaciones finalizan este segmento temporal que se ha creado exclusivamente para la operación desaparece.



**Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia**

Dependencia

Dirección de Tecnología, información Y comunicaciones

Fecha Aprobación

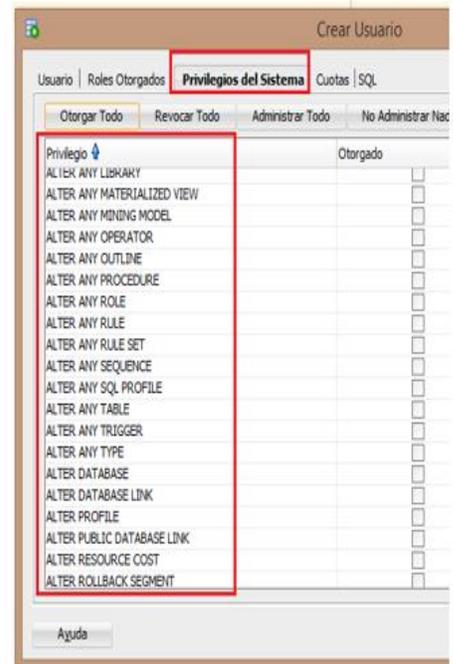
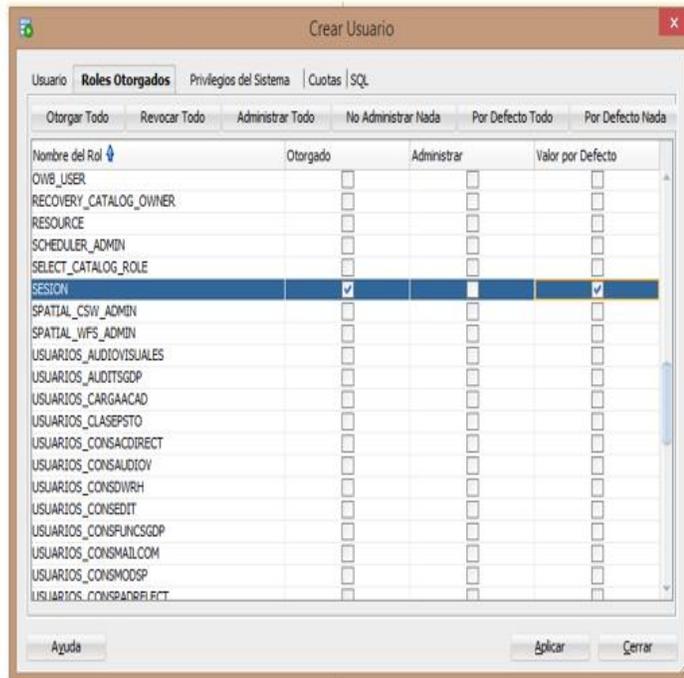
26/06/2017

Fecha revisión

26/06/2019

Código

MEGAC-PEGAC.03-PR-06

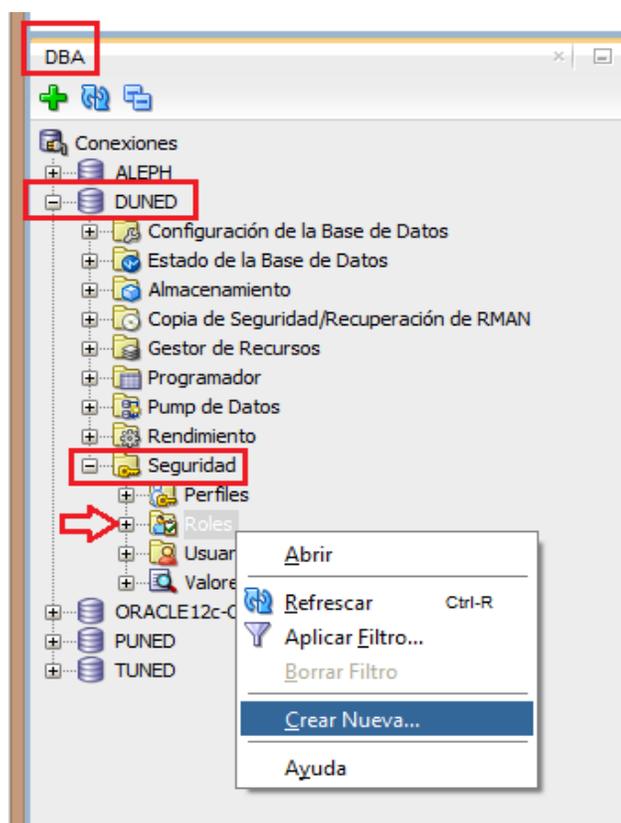


h. **Privilegios del Sistema:** si el usuario por sus funciones requiere de algún privilegio especial que sobrepasen los permisos a nivel de datos (Insert, delete, update, select) o la ejecución de algún procedimiento almacenado o función, se debe de elegir de la lista de privilegios disponibles.

## (2) Para crear Roles de base de datos en ORACLE

1. Conéctese a la Base de Datos por medio de la herramienta de **SQL Developer** con un usuario con privilegios de **Administrador**.
2. En la vista del DBA seleccione y expanda la **Base de Datos** donde creará el usuario. Luego seleccione y expanda la carpeta de **Seguridad**.
3. Sobre la carpeta de **Roles** de click derecho del mouse y seleccione la opción **Crear Nuevo**.

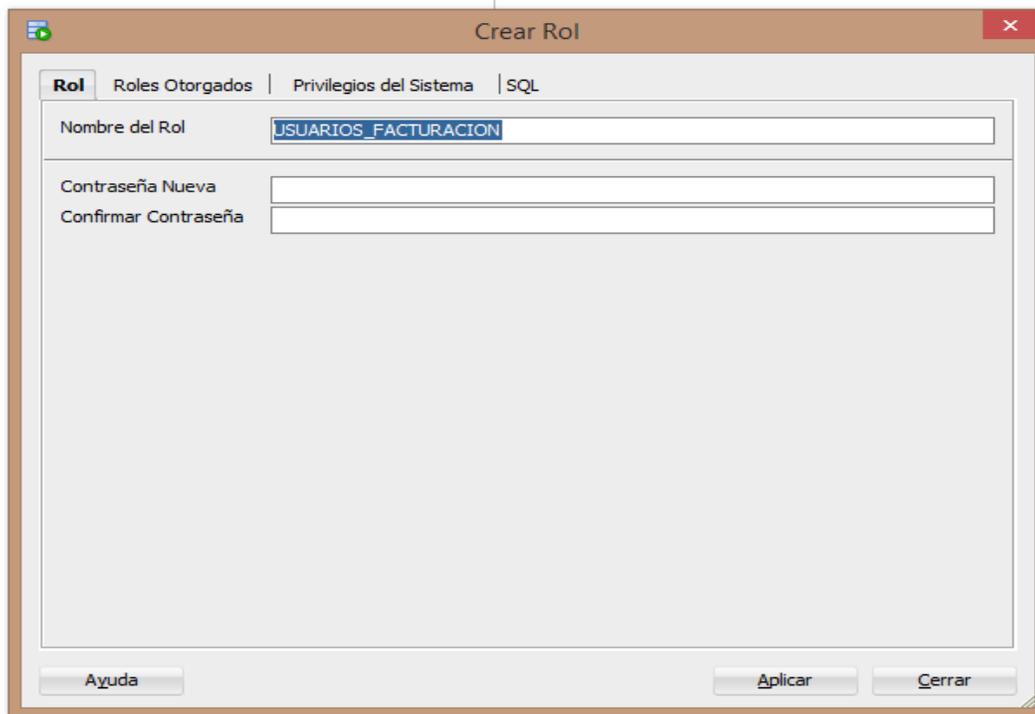
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



4. En el cuadro de propiedades para Crear Roles se debe indicar:
- Nombre del Rol:** un nombre que identifique al Rol de tal forma que sea representativo de la función que cumplirá.
  - Contraseña Nueva:** escriba una contraseña para el nuevo rol que esté compuesta como mínimo de diez caracteres, donde se combinen letras mayúsculas-minúsculas, valores numéricos y caracteres especiales. Esta característica aplica si el nivel de seguridad de la aplicación así lo requiere.
  - Confirmar Contraseña:** repita la misma contraseña ingresada en el punto anterior. En caso de que no coincidan se producirá un error.
  - Adicionalmente hay otras opciones que se pueden activar para el Rol como:
    - Roles Otorgados:** opción para asignarle al Rol otros Roles existentes.
    - Privilegios del Sistema:** si el usuario por sus funciones requiere de algún privilegio especial que sobrepasen los permisos a nivel

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

de datos (Insert, delete, update, select) o la ejecución de algún procedimiento almacenado o función, se debe de elegir de la lista de privilegios disponibles.



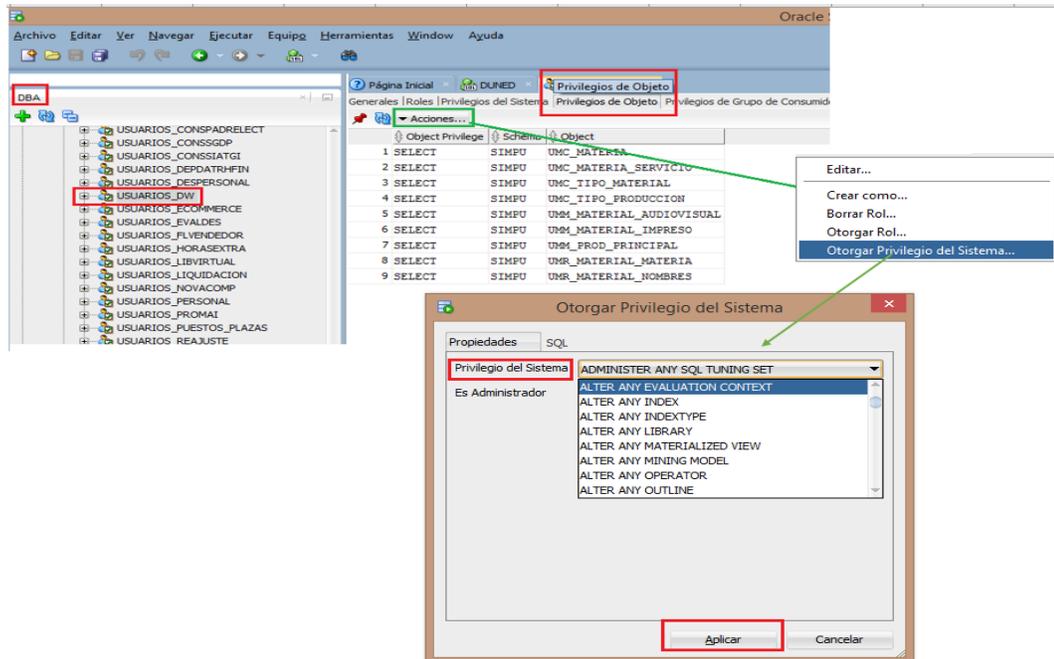
### (3) Asignación de privilegios a roles de base de datos en ORACLE

Para agregar / denegar privilegios a un Rol de Base de Datos, se puede hacer de dos formas: a) de forma gráfica, b) por medio de sentencias SQL.

#### De forma gráfica

1. Conéctese a la Base de Datos por medio de la herramienta de **SQL Developer** con un usuario con privilegios de **Administrador**.
2. En la vista del DBA seleccione y expanda la **Base de Datos** donde está el Rol al cuál le otorgará el privilegio de objeto. Luego seleccione y expanda la carpeta de **Seguridad**.
3. Selecciones y expanda la carpeta de **Roles**, y selecciones el nombre del Rol de Base de Datos. De click derecho del mouse sobre él y en la pantalla que se despliega al lado derecho seleccione el tab **Privilegios de Objeto / Privilegios de Sistema**.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

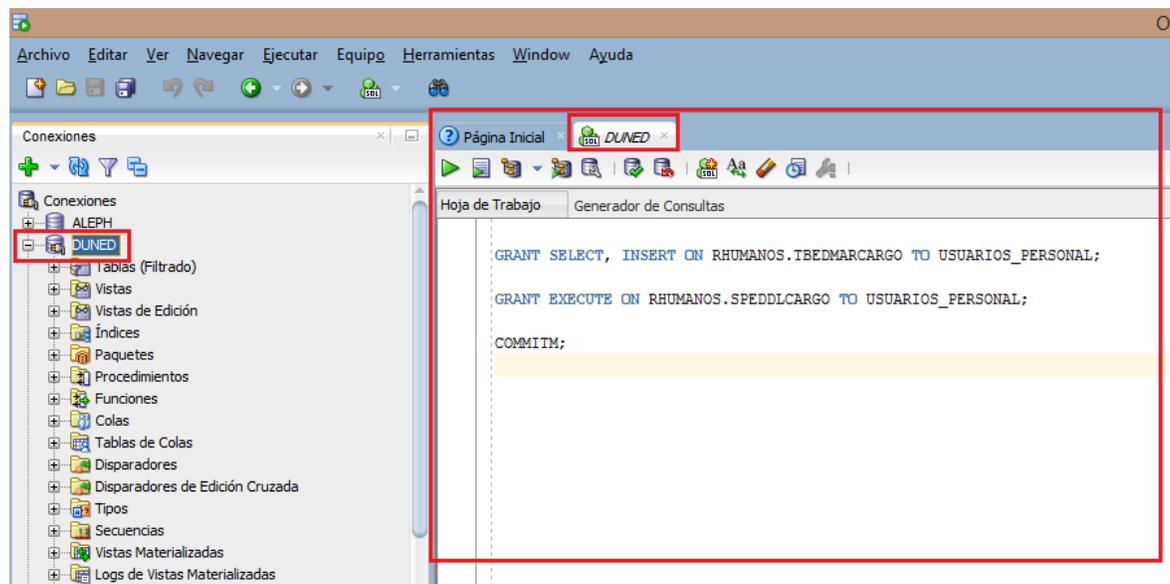


4. Seleccione el privilegio a otorgar de la lista disponible, y de click sobre el botón Aplicar.

### Por medio de sentencias SQL

1. Conéctese a la Base de Datos por medio de la herramienta de **SQL Developer** con el usuario dueño de los objetos (Tablas, vistas, procedimientos, etc.) sobre lo que otorgará privilegios al Rol.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



2. En la **hoja de trabajo** que se habilita al lado derecho, escriba las sentencias SQL para otorgar los privilegios necesarios al Rol de Base de Datos.
3. Una vez que ejecute las sentencias SQL con éxito, ejecute el comando **COMMIT** para guardar de forma permanente el cambio en la Base de Datos.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

## Instructivo para la Administración de Usuarios, roles y privilegios de SQL Server

### ¿En qué consisten el Inicio de Sesión, los roles y privilegios de SQL Server?

Para conectarse a una instancia en el motor de Base de Datos de SQL Server, debe existir un usuario que inicie sesión, ya sea basado en una entidad de **seguridad de Windows** (*usuario de dominio o grupo de dominio*) o bien como un **inicio de sesión de SQL Server**. Para realizar lo anterior, el motor de Base de Datos deberá estar configurado para utilizar el **modo de autenticación mixto**.

Adicionalmente, para conectarse a una Base de Datos específica el usuario además de iniciar una sesión, debe estar **asignado a una Base de Datos** y dentro de ella estar **asociado al menos a un rol de Base de Datos**, por medio del cual se le otorgan o deniegan los permisos (*select, insert, delete, update, execute, etc.*), sobre los diferentes objetos de Base de Datos (*tablas, vistas, procedimientos almacenados, funciones, etc.*) y cumplir con ciertas características que se detallan más adelante.

### Conceptos

- **Base de datos:** es un “almacén” que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.
- **SQL Server:** Sistema de gestión de base de datos relacionales empresarial desarrollado por la Corporación Microsoft.
- **Roles de una base de datos:** Los roles son una forma de simplificar el proceso de gestión de privilegios sobre objetos de Base de Datos.

### Para la ejecución de las actividades se debe tener en cuenta lo siguiente

1. Para efectos de la creación de un inicio de sesión para los Sistemas de la UNED, este instructivo se concentrará en las opciones **Asignación de usuarios (UserMapping)** y **Estado (Status)**.
2. Se pueden crear cuantos roles sean necesarios para una aplicación o sistema, y ser asignados a los usuarios existentes y que forma parte éste.

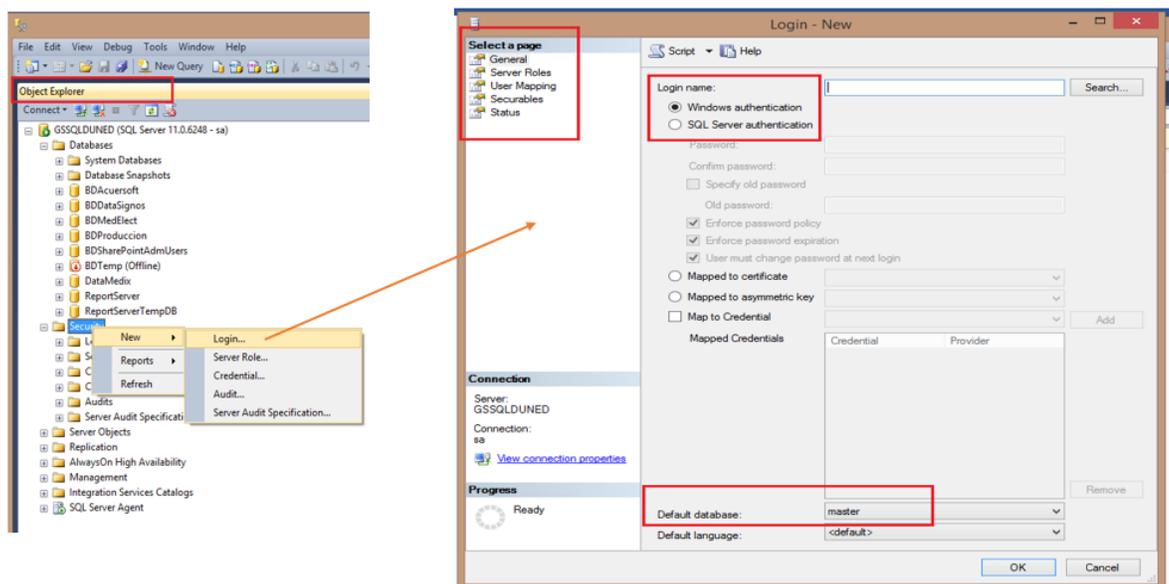
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- De esta forma, cuando se desee revocar un privilegio para un usuario, solamente se debe de revocar la asignación del rol al usuario, en vez de revocar cada privilegio de forma individual.
- Los privilegios a otorgar suelen clasificarse en **privilegios del sistema** (*permiten al usuario realizar algún tipo de operación que afecte a todo el sistema manejador de Base de Datos*), y **privilegios de objetos** (*permiten al usuario realizar operaciones específicas sobre objetos específicos como tablas, vistas, procedimientos, etc.*)
- Los privilegios de sistema por lo general son aquellos que ejecutan una sentencia del tipo **CREATE, DROP, ALTER**, mientras que los privilegios de objeto están relacionados a la ejecución de sentencias como **SELECT, INSERT, DELETE, UPDATE, EXECUTE**.

## Actividades para realizar el trámite de Configuración del Inicio de Sesión de los Usuarios

### (1) Pasos para crear un Inicios de sesión en SQL Server

- En el Explorador de objetos, expanda la carpeta de la instancia de servidor en la que desea crear el nuevo inicio de sesión o Login.
- Haga clic con el botón secundario en la carpeta **Seguridad (Security)**, seleccione **Nuevo (New)** y, a continuación, seleccione **Inicio de sesión o Login**.



	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

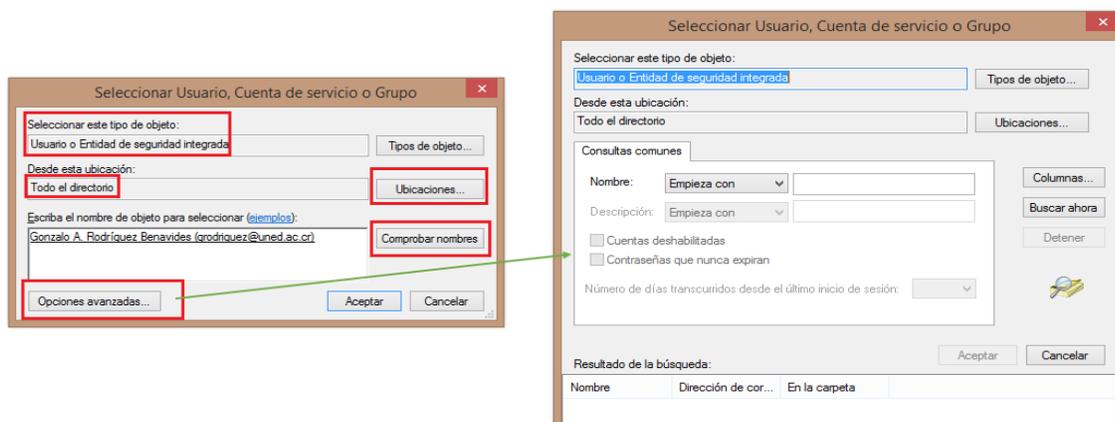
3. En el cuadro de diálogo **Inicio de sesión (Login) - Nuevo**, en la página **General**, escriba el nombre de un usuario en el cuadro **Nombre de inicio de sesión (LoginName)**.

3.1 Si el usuario iniciará sesión por medio de una entidad de seguridad de Windows haga clic en **Buscar (Search)** para abrir el cuadro de diálogo **Seleccionar usuarios o grupos**.

Si hace clic en **Buscar**:

- a. En **Seleccionar este tipo de objeto**, haga clic en **Tipos de objeto** para abrir el cuadro de diálogo **Tipos de objeto** y seleccione alguna o todas las opciones siguientes: **Entidades de seguridad integradas, Grupos y Usuarios**. Las opciones **Entidades de seguridad integradas y Usuarios** están seleccionadas de forma predeterminada. Cuando termine, haga clic en **Aceptar**.
- b. En **Desde esta ubicación**, haga clic en **Ubicaciones** para abrir el cuadro de diálogo **Ubicaciones** y seleccione una de las ubicaciones de servidor disponibles (local o todo el directorio). Cuando termine, haga clic en **Aceptar**.
- c. En **Escribir los nombres de objeto para seleccionar (ejemplos)**, escriba el usuario o el nombre de grupo que desea buscar. Si eligió en ubicación Todo el directorio, el usuario escrito será validado ante el Servidor de Active Directory, sino la validación se realizará ante el Servidor Local.
- d. Adicionalmente podrá hacer clic sobre el botón de **Opciones Avanzadas** para obtener más opciones de búsqueda.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



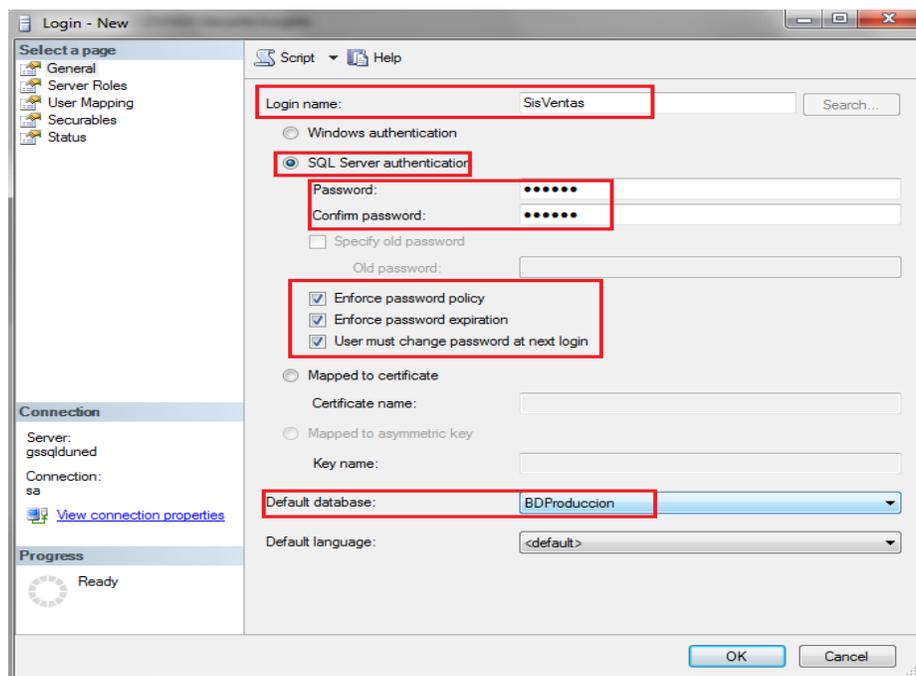
e. Haga clic en **Aceptar** cuando haya ingresado toda la información necesaria para el inicio de sesión.

3.2 Si el usuario iniciará sesión basado en la autenticación de SQL Server, deberá seleccionar la opción **SQL Server authentication** y seguir los siguientes pasos:

- a. En el cuadro **Contraseña (Password)**, escriba una contraseña para el nuevo usuario que esté compuesta como mínimo de diez caracteres, donde se combinen letras mayúsculas-minúsculas, valores numéricos y caracteres especiales. Vuelva a escribir la contraseña en el cuadro **Confirmar contraseña (ConfirmPassword)**.
- b. Al cambiar una contraseña existente, seleccione **Especificar contraseña anterior (Specify Old Password)** y escriba la contraseña anterior en el cuadro **Contraseña anterior (Old Password)**.
- c. Para aplicar las opciones de la directiva de contraseñas a efectos de complejidad y exigencia, puede seleccionar **Exigir directivas de contraseñas (EnforcePasswordPolicy)**. Esta es una opción predeterminada cuando se selecciona **Autenticación de SQL Server**.
- d. Para aplicar las opciones de la directiva de contraseñas a efectos de expiración, seleccione **Exigir expiración de contraseña (EnforcePasswordExpiration)**. Debe seleccionar la opción **Exigir directivas de contraseñas** para habilitar esta casilla. Esta es una opción predeterminada cuando se selecciona **Autenticación de SQL Server**.
- e. Para obligar al usuario a crear una nueva contraseña después de utilizarse el inicio de sesión por primera vez, seleccione **El usuario debe**

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

**cambiar la contraseña en el siguiente inicio de sesión (Usermustchange password at next login).** Debe seleccionar la opción **Exigir expiración de contraseña** para habilitar esta casilla. Esta es una opción predeterminada cuando se selecciona **Autenticación de SQL Server**.



- f. Adicionalmente, para asociar el inicio de sesión a un certificado de seguridad independiente, seleccione **Asignado a certificado (Mapped to certificate)** y seleccione el nombre de un certificado existente de la lista.
- g. Para asociar el inicio de sesión a una clave asimétrica independiente, seleccione **Asignado a clave asimétrica (Mapped to asymmetric key)** y seleccione el nombre de una clave existente de la lista.
- h. Para asociar el inicio de sesión a una credencial de seguridad, active la casilla de **Asignado a credencial** y seleccione una credencial existente de la lista o haga clic en Agregar para crear una nueva credencial. Para quitar una asignación a una credencial de seguridad del inicio de sesión, seleccione la credencial en Credenciales asignadas y haga clic en **Quitar**.

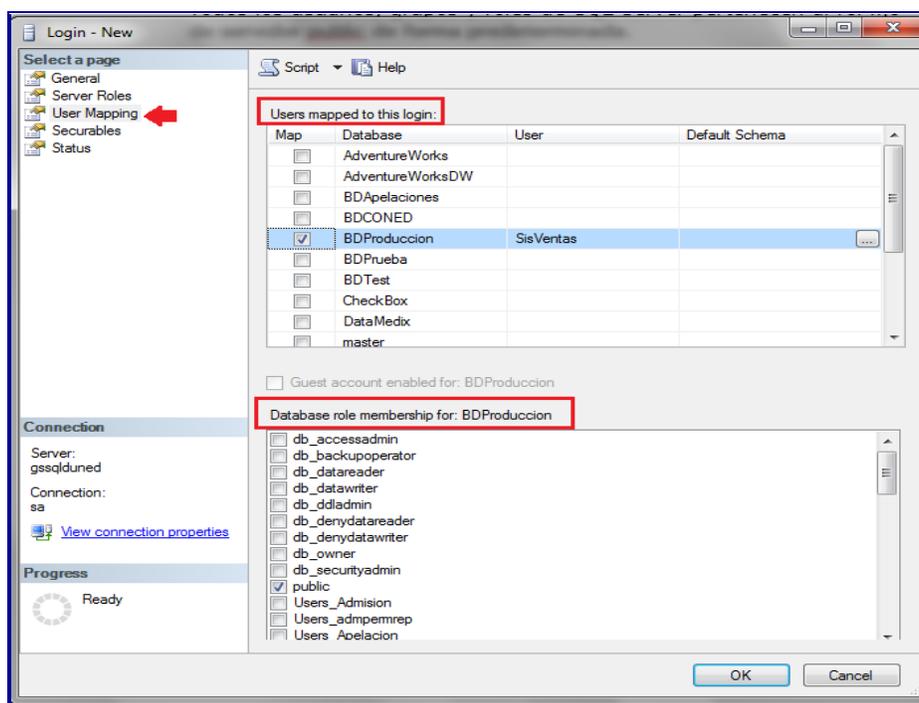
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

4. En la lista **Base de Datos predeterminada (Default Database)**, seleccione una Base de Datos predeterminada para el inicio de sesión.
5. En la lista **Idioma predeterminado (Default language)**, seleccione un idioma predeterminado para el inicio de sesión.
6. Haga clic en Aceptar (OK) cuando haya ingresado toda la información necesaria.
7. Opciones adicionales: El cuadro de diálogo Inicio de sesión - Nuevo también proporciona otras opciones adicionales que están presentes en las páginas disponibles del cuadro de diálogo, que se podrán asignar a un inicio de sesión cuando lo amerite.
  - a. Roles del servidor (Server Roles).
  - b. Asignación de usuarios (UserMapping).
  - c. Elementos protegibles (Securables).
  - d. Estado (Status).

### 7.1 Asignación de usuarios (UserMapping)

La página Asignación de usuarios enumera **todas las Bases de Datos posibles y las pertenencias al rol de Base de Datos** en esas Bases de Datos que se pueden aplicar al inicio de sesión. Las Bases de Datos seleccionadas determinan las pertenencias a roles disponibles para el inicio de sesión. En esta página están disponibles las opciones siguientes:

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



- **Usuarios asignados a este inicio de sesión (Usersmapped to thislogin):** Seleccione las Bases de Datos a las que se puede obtener acceso con este inicio de sesión. Cuando se seleccione una Base de Datos, sus roles válidos se mostrarán en el panel **Miembros del rol de base de datos para: database\_name (Database role membershipfor:)**.
- **Mapa (Map):** Permite que el inicio de sesión obtenga acceso a las Bases de Datos que se muestran a continuación. Para seleccionar una, solamente debe de hacer clic sobre ella.
- **Base de Datos (Database):** Muestra las Bases de Datos disponibles en el servidor.
- **Usuario (User):** Especifica el usuario de <sup>27</sup>Base de Datos que se va a asignar al inicio de sesión.
- **Esquema predeterminado (Default Schema):** Especifica el <sup>28</sup>esquema predeterminado del usuario. Cuando se crea un usuario por primera vez, el

<sup>27</sup>De forma predeterminada, el nombre del usuario de Base de Datos coincide con el inicio de sesión.

<sup>28</sup>No puede especificar un esquema predeterminado para un usuario asignado a un grupo, un certificado o una clave asimétrica de Windows.

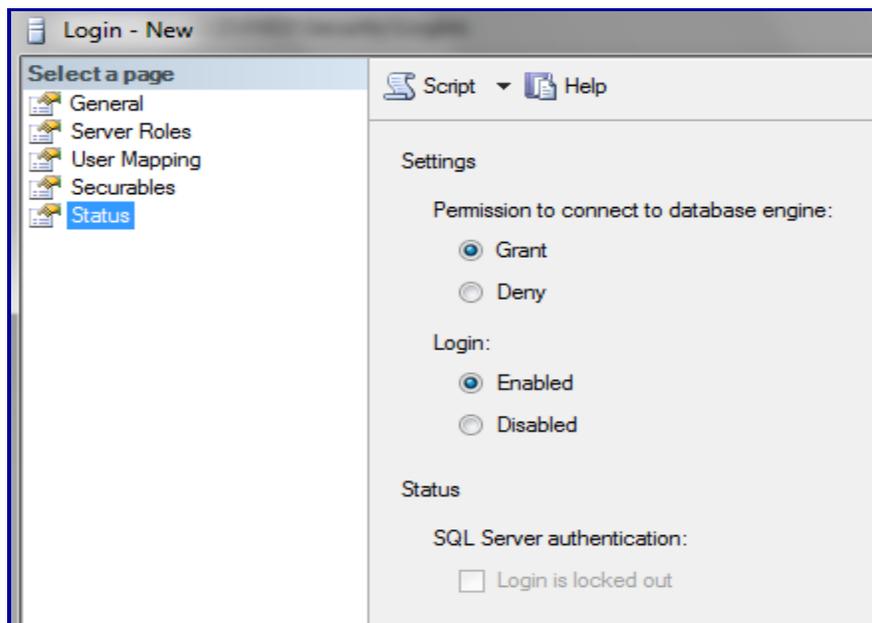
 <p>UNED UNIVERSIDAD ESTADAL CUBANA Instituto Superior de la Educación y la Cultura</p>	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

esquema predeterminado es **dbo**. Es posible especificar un esquema predeterminado que aún no existe.

- **Cuenta de invitado habilitada para: database\_name**  
Atributo de solo lectura que indica si la cuenta de invitado está habilitada en la Base de Datos seleccionada. Utilice la página Estado del cuadro de diálogo **Propiedades de inicio de sesión** de la cuenta de invitado para habilitarla o deshabilitarla.
- **Miembros del rol de Base de Datos para: database\_name(Guestaccountenabledfor):** Selecciona los roles para el usuario en la Base de Datos especificada. Todos los usuarios son miembros del **rol public** de todas las Bases de Datos, y no pueden eliminarse. En la Sección de Creación y Asignación de Roles de Base de Datos se explica en detalle este tema.

## 7.2 Estado (Status)

La página Estado enumera algunas de las opciones de autenticación y autorización que se deben configurar en el inicio de sesión de SQL Server seleccionado y que se describen a continuación:



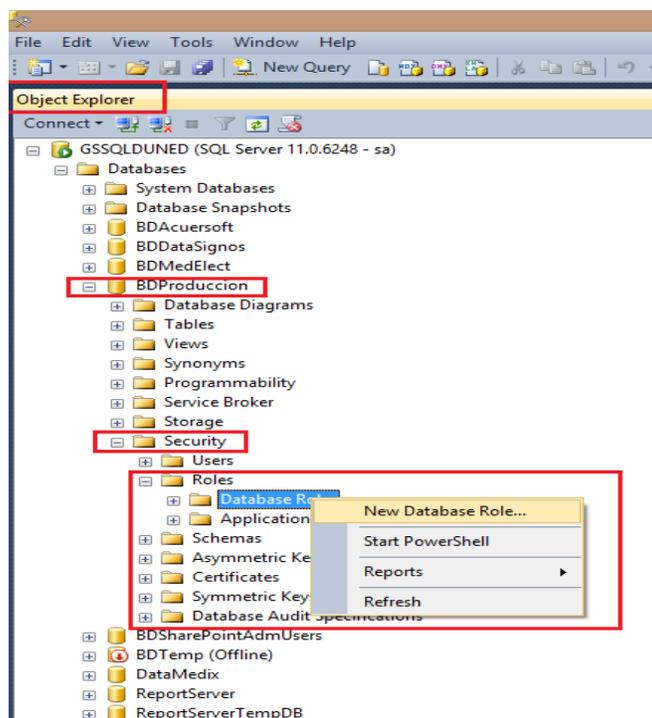
	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

- **Permiso para conectarse al motor de la Base de Datos:** Mediante esta opción se le otorga (Grant) o Deniega (Deny) el permiso de conexión al motor de Base de Datos. Cuando trabaje con esta configuración, debe pensar en el inicio de sesión seleccionado como una entidad de seguridad a la que se le puede otorgar o denegar un permiso para un elemento protegible. Seleccione **Conceder (Grant)** para conceder el permiso CONNECT SQL al inicio de sesión. Seleccione **Denegar (Deny)** para denegar el permiso CONNECT SQL al inicio de sesión.
  - **Inicio de sesión (Login):** Un inicio de sesión que se ha deshabilitado sigue existiendo en el registro del motor de Base de Datos, pero si intenta conectarse a SQL Server, el inicio de sesión no se autenticará. Seleccione esta opción para **habilitar (Enabled) o deshabilitar (Disabled)** este inicio de sesión. Esta opción utiliza la instrucción ALTER LOGIN con las opciones ENABLE o DISABLE.
  - **Status-Authenticación de SQL Server:**La casilla Inicio de sesión bloqueado (Loginislockedout) solo estará disponible si el inicio de sesión seleccionado se conecta usando la autenticación de SQL Server y el inicio de sesión está bloqueado. Este valor es de solo lectura. Para desbloquear un inicio de sesión que está bloqueado, ejecute ALTER LOGIN con la opción UNLOCK, o utilizando las opciones Grant-Deny / Enabled-Disabled descritas anteriormente.
8. Después de crear un inicio de sesión, este puede conectarse a SQL Server, pero no necesariamente tiene permisos suficientes para realizar ningún trabajo útil en una Base de datos.
  9. Para acceder a una Base de Datos y poder ejecutar sentencias DML debe de combinar el inicio de sesión con un usuario de Base de datos y un rol de Base de Datos

## (2) Pasos para crear un Roles de base de datos en SQL Server

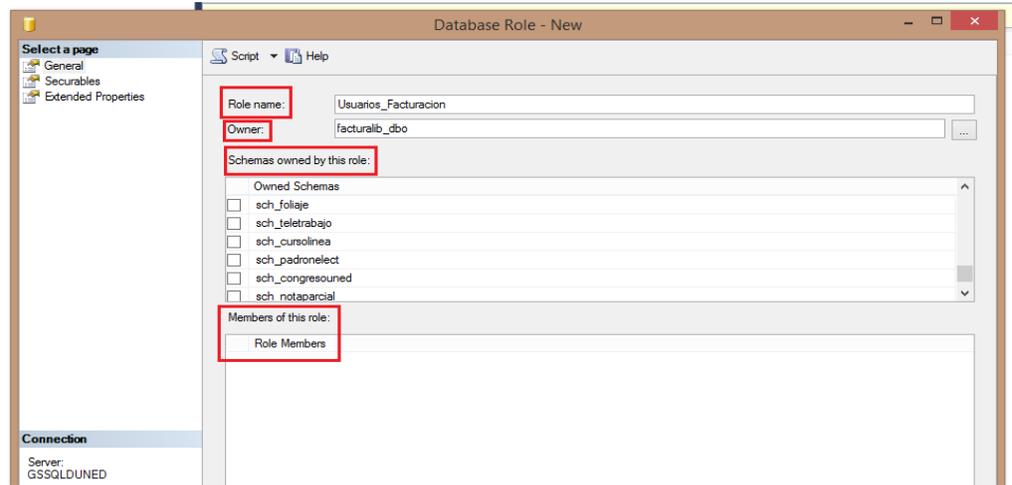
1. En el Explorador de objetos, seleccione y expanda la Base de Datos donde creará el rol, seleccione y expanda la carpeta de Seguridad (Security), seleccione y expanda la carpeta de Roles, y haga click derecho sobre la carpeta Roles de Base de Datos (Database Roles).

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06

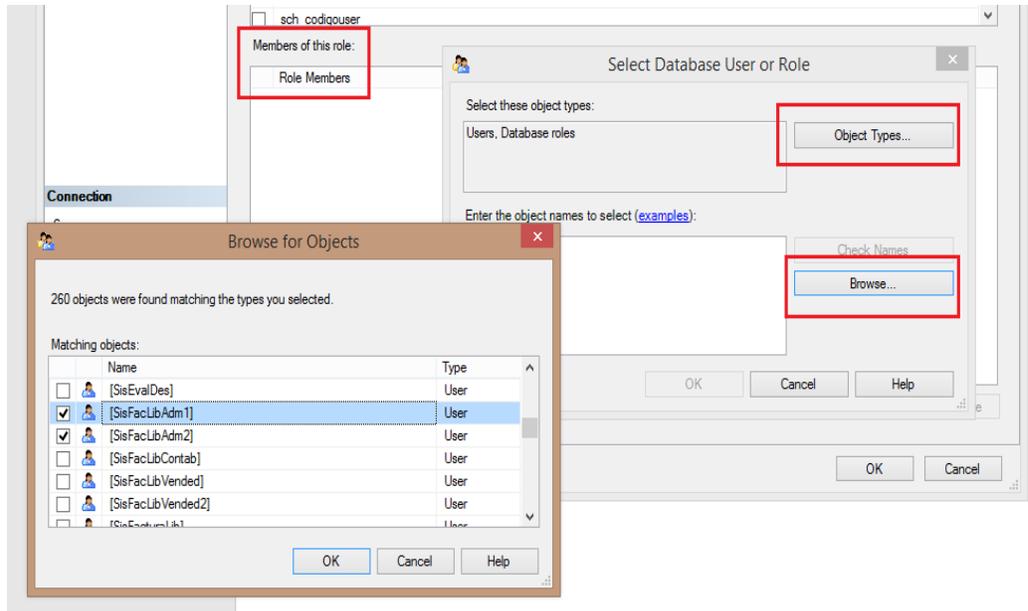


2. Seleccione la opción **Nuevo Rol de Base de Datos (New Database Role)** y proporcione la siguiente información:
  - a. **Nombre del Rol (Rol name):** un nombre que identifique al Rol y que sea representativo de la aplicación y función que cumplirán los usuarios que pertenezcan a él.
  - b. **Propietario del Rol (owner):** indicar el usuario de la Base de Datos quien es propietario de este Rol.
  - c. **Esquema(s) propiedad del Rol (Schemasownedbythis role):** si aplica esta opción, se deberá indicar el esquema donde están creados los objetos de Base de Datos, y quien son propiedad del Rol.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06



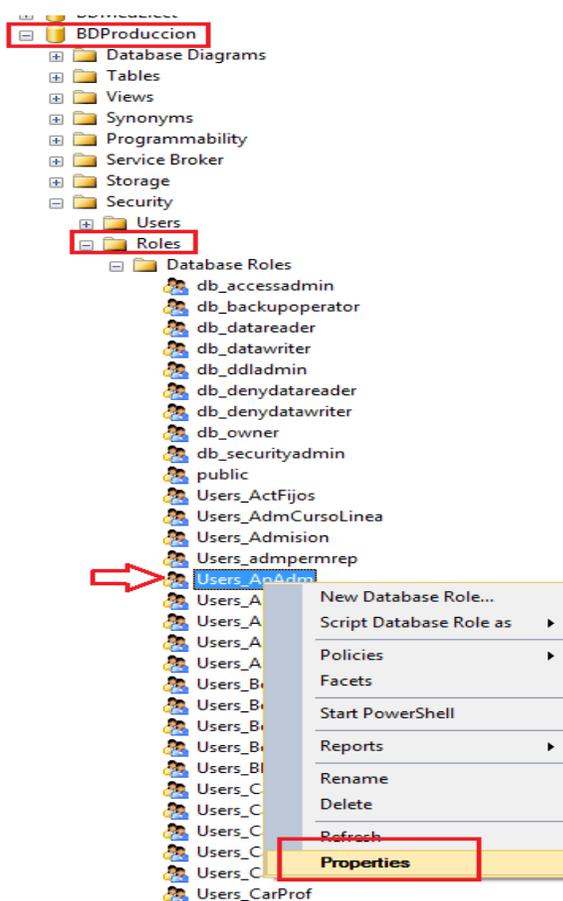
- d. **Miembros de este Rol (Members of this role):** adicionalmente se deben indicar los usuarios que son parte del rol que se está creando. En el botón Agregar (Add) se podrán elegir los usuarios disponibles en la Base de Datos.



 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

### (3) Pasos para otorgar privilegios a roles de base de datos en SQL Server

- Una vez creados los usuarios y que estos hayan sido asignados a roles de Base de Datos, es necesario dotarlos de privilegios para que puedan realizar operaciones específicas en la Base de Datos.
- En el Explorador de objetos, seleccione y expanda la Base de Datos donde creará el rol, seleccione y expanda la carpeta de **Seguridad (Security)**, seleccione y expanda la carpeta de Roles, y haga click derecho sobre la carpeta **Roles de Base de Datos (Database Roles)**.
- Seleccione el nombre del Rol al que desea otorgarle privilegios, y de click derecho del mouse sobre él. Elija la opción de **Propiedades (Properties)**



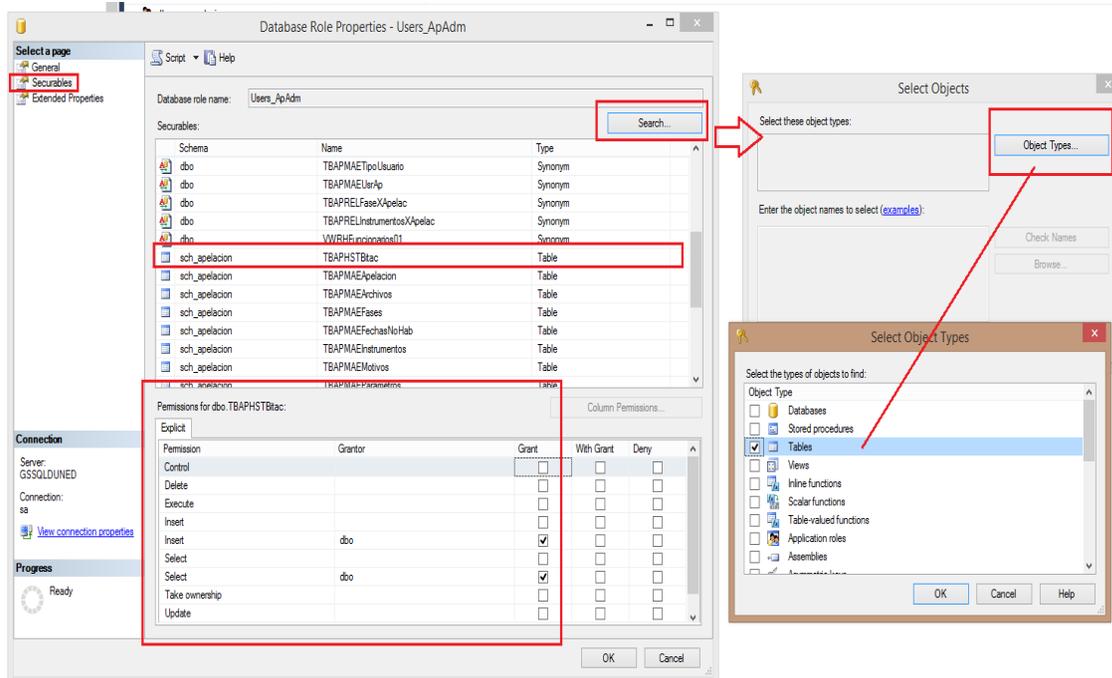
- En el cuadro de diálogo de propiedades de **Roles de Base de Datos (Database Role Properties)**, seleccione la página **Securables**. En ésta página se

 <p><b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b></p>	Dependencia	Dirección de Tecnología, información Y comunicaciones
	Fecha Aprobación	26/06/2017
	Fecha revisión	26/06/2019
	Código	MEGAC-PEGAC.03-PR-06

desplegarán/agregarán los objetos de Base de Datos sobre los cuáles se agregarán los privilegios de objeto.

- Para agregar un objeto a la lista, haga clic sobre el botón **buscar (Search)**, indique el tipo de objeto (*Vista, Tabla, Procedimiento, función, etc.*), el nombre del objeto y agréguelo a la lista de objetos asegurables. Luego indique el privilegio a otorgar.

Dependiendo del tipo de objeto que haya seleccionado, las opciones de privilegios a otorgar puede que varíen.



- Una vez que haya indicado toda la información necesaria (*objetos y privilegios*), de click sobre el botón **Aceptar (OK)** para finalizar.

	<b>Manual de Procedimientos para la Seguridad de Tecnologías de Información y Comunicaciones del Proceso específico de la Gestión de tecnologías de información y comunicación de la Universidad Estatal a Distancia</b>	Dependencia	Dirección de Tecnología, información Y comunicaciones
		Fecha Aprobación	26/06/2017
		Fecha revisión	26/06/2019
		Código	MEGAC-PEGAC.03-PR-06