Universidad Estatal a Distancia
Vicerrectoría de Planificación
Centro de Planificación y Programación Institucional

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.2104-2020, celebrada el 10 de agosto del 2020.

2020

TABLA DE CONTENIDO **Pág.**

Aprobación

Manual aprobado por Consejo de Rectoría en sesión 2104-2020, Artículo IV, inciso 1), celebrada el 10 de agosto del 2020.

Elaboración y Revisión

Funcionario	Puesto	Dependencia
María Luisa Molina Mendez	Gestora de Cumplimiento de Planes TI	Dirección de Tecnologías de Información y Comunicación
Alejandro Sánchez Rivera,	Coordinador de la Unidad Soporte Técnico	Dirección de Tecnologías de Información y Comunicación
Esteban Artavia Herrera.	Funcionario de la Unidad de Infraestructura Tecnológica	Dirección de Tecnologías de Información y Comunicación
Jose Pablo Chávez Sanchez.	Coordinador de la Unidad de Sistemas de Información	Dirección de Tecnologías de Información y Comunicación
Rolando Rojas Coto,	Coordinador de la Unidad de Infraestructura Tecnológica	Dirección de Tecnologías de Información y Comunicación
Francisco Duran Montoya.	Director de la Dirección de Tecnología de Información y Comunicaciones	Dirección de Tecnologías de Información y Comunicación

Revisión relacionada a las modificaciones de la versión 02 por parte de la Ing. Loretta Sánchez Herrera, funcionaria del Centro de Planificación y Programación Institucional.

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.

Marco [1]Normativo

Como resultado de la recopilación de leyes, normativa interna, acuerdos, pronunciamientos, contratos, resoluciones y directrices; entre otras, y en cumplimiento a la norma Nº 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, Nº R-CO- 26-2007 del 7 de junio del 2007.

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

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 Nº 464, Artículo VI, acuerdo Nº 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 Nº 058-2000 del 30 de mayo del 2000, publicado en la Gaceta Nº 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 Nª 6683 de Derechos de Autor y Derechos Conexos, publicada en la Gaceta Nº 212 del 04 de noviembre del 1982.
- Ley Nª 7202 del Sistema Nacional De Archivos, publicada en la Gaceta Nº 225 del 27 de noviembre del 1990.
- Ley Nª 7600 de Igualdad de Oportunidades para las Personas con Discapacidad, publicada en la Gaceta Nº 102, del 29 de mayo de 1996.
- Ley Nª 8292 General de Control Interno, publicada en la Gaceta Nº 169, del 04 de setiembre del 2002.
- Ley Nª 8422 Contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública, publicada en la Gaceta Nº 212 del 29 de octubre del 2004.
- Ley Nª 8454 de Certificados, Firmas y Documentos Electrónicos, publicada en la Gaceta Nº 197, del 13 de octubre del 2005.
- Ley Nª 8642 General de Telecomunicaciones, publicada en la Gaceta Nº 125, del 30 de junio del 2008.

- Ley Nª 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, publicada en la Gaceta Nº 170, del 05 de setiembre del 2011.
- Ley Nª 9048 de Delitos Informáticos y Conexos, publicada en la Gaceta Nº 214 del 06 de noviembre del 2012.
- Normas del Control Interno en el Sector Publico (N-2-2009-CO-DFOE), publicado en la Gaceta Nº 26 del 06 de febrero del 2009.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, N-2-2007CO-DFOE, publicado en la Gaceta Nº 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 Nª 2401-2015, Articulo III, inciso 1-a), del 05 de febrero del 2015.
- Reforma al Reglamento a la Ley Nº 7494 de Contratación Administrativa, publicado en la Gaceta Nº 93, del 16 de mayo del 2007, Decreto Nº 33758-H.
- Reglamento a la Ley Nº 6683 de Derechos de Autor y Derechos Conexos, publicado en la Gaceta Nº 201, del 24 de octubre del 1995, Decreto Nº 24611-J.
- Reglamento a la Ley Nº 7202 del Sistema Nacional De Archivos, publicado en la Gaceta Nº 47, del 7 de marzo del 1995, Decreto Nº 24023-C.
- Reglamento a la Ley Nº 7494 de Contratación Administrativa, publicada en la Gaceta Nº 210, del 02 de noviembre de 2006, Decreto Nº 33411-H.
- Reglamento a la Ley Nº 7600 de Igualdad de Oportunidades para las Personas con Discapacidad, publicado en la Gaceta Nº 75, del 20 de abril del 1998, Decreto Nº 26831-MP.
- Reglamento a la Ley Nº 8422 Contra la Corrupción y el Enriquecimiento Ilícito en la Función Pública. Publicado en la Gaceta Nº 82, del 09 de abril del 2005, Decreto Nº 32333MP-J.
- Reglamento a la Ley Nº 8454 de Certificados, Firmas y Documentos Electrónicos, publicado en la Gaceta Nº 77, del 21 de abril del 2006, Decreto Nº 33018.

- Reglamento a la Ley Nº 8642 General de Telecomunicaciones, publicado en la Gaceta Nº 186, del 26 de setiembre del 2008, Decreto Nº 34765-MINAET.
- Reglamento a la Ley Nº 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales, publicado en la Gaceta Nº 45, del 05 de marzo del 2013, Decreto Nº 37554-JP.
- Reglamento General Estudiantil, aprobado por el Consejo Universitario en sesión Nº 2145, Art. IV, I. -a) del 15 de marzo del 2012. Acuerdo analizado posteriormente en sesión Nº 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 Nº 204, del 24 de noviembre del 2005, Decreto Nº 32717-h.
- 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) 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 Nº 2336, Art. II, inciso 2- a) de 15 de mayo del 2014.

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 Nº 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, Articulo 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 Nº 1833-2014, Artículo V, celebrada el 22 de setiembre de 2014.
- Estructura de Riesgos UNED, Anexo Nº 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 Nº 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, Articulo 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 Nº 094-2019, artículo I, celebrada el 20 de febrero del 2015.
- 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 24332015, 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 Nº 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 Nº 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 Nº 1896-2016, Artículo VI, celebrada el 29 de febrero del 2016.

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.

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. [2]Servicios de TI institucionales

Servicio Académico	Tipo de Servicio
Información y comunicación	
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
Transacción interna	
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

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

Servicio Académico	Tipo de Servicio
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

Servicio Académico	Tipo de Servicio
Información y comunicación	
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
Transacción Externa Estudiante	
SAE – Matriweb	Servicio Académico
SAE – Admisión y Empadronamiento	Servicio Académico
SAE – Reconocimientos	Servicio Académico
Entorno de Estudiantes	Servicio Académico
Encuestas en línea	Servicio Académico
Transacción externa público	
Eventos	Servicio Académico
Servicio administrativo	
Información y comunicación	
Telefonía IP	Servicio administrativo
Transacción interna	
AS – 400 – Activos fijos	Servicio administrativo

Servicio Académico	Tipo de Servicio
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
Servicio Académico	**Tipo de Servicio**
Información y comunicación	
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.

Clasificación de Recursos de TI	
Nombre	**Tipificación**
Aplicaciones	Sistema Financiero Contable
	Sistema de Matricula
	Sistema de Transportes
	Procedimientos Manuales
	Otros
Información(datos)	Archivos
	Base de datos
	Cintas de Respaldo

Clasificación de Recursos de TI	
Nombre	**Tipificación**
	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

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

Clasificación de la Información	
Nombre	**Tipificación**
Clasificación de la Información	
Nombre	**Tipificación**
	Normativa Universitaria
	Información de Carreras
	Información Científica
	Informes finales de Auditoría Interna

Normas de Aplicación

Monitoreo [3]preventivo y solicitud de estudios necesarios sobre el uso de la red institucional, equipos tecnológicos y las aplicaciones

La Dirección de Tecnología de 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 (Reglamento para el Uso de Equipo de Cómputo e Internet), 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 una herramienta para la gestión y análisis de eventos de red institucional o cualquier otro dispositivo que la DTIC considere necesario.
2. El monitoreo y el diagnóstico se realizará de forma periódica seleccionando una o varias dependencias de la universidad. Esta puede variar según la situación laboral del

[3] 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.

momento, de las condiciones de los equipos de comunicaciones y seguridad de las dependencias, el licenciamiento, la disponibilidad de personal y equipos para analizar el tráfico de la universidad, cambios en prioridades de la UNED, de la DTIC, entre otros factores.

3. Para el caso del monitoreo y diagnóstico de la red institucional se va contar con al menos los siguientes reportes:
    a. Uso de ancho de banda y aplicaciones
    b. Uso de actividad web
    c. Amenazas informáticas
4. El monitoreo y diagnóstico va tener la duración de al menos 15 días y producto del mismo se realizará un análisis de los datos que este genere.
5. 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.

6. Los reportes generados y el correspondiente informe se almacenarán en las siguientes ubicaciones:

a) Nube privada de la UNED. Espacio creado por la DTIC el cual forma parte del ciclo de respaldos principal de la universidad. Este forma parte de los “Respaldos Servidores Plataformas Windows y Linux”, citado en el Instructivo para respaldo de Información del centro de datos principal, denominado “UNED-Instructivo de Respaldos centro de Datos”, aprobado por el Consejo de Rectoría, en sesión 2064-2020, Artículo IV, inciso 5), celebrada el 20 de enero del 2020.

b) OneDrive de la Unidad de Seguridad Digital. Espacio que tendrá como función ser una segunda copia de respaldo.

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 una herramienta para la gestión y análisis de eventos de red institucional o cualquier otro dispositivo que la DTIC considere necesario.
3. De ser necesario, se solicitará la participación y asesoramiento de la Oficina Jurídica, así como de cualquier oficina que requiera ser involucrada (Auditoría Interna, Control Interno, entre otros.).
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, entre otros, 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, en caso que se requiera levantar un acta de todo lo realizado en la visita.
    d. Uno o varios funcionarios de la DTIC, quienes realizarán 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:
        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 informará 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.
7. Se almacenará la solicitud realizada, los reportes generados y el correspondiente informe en las siguientes ubicaciones:

   a) Nube privada de la UNED. Espacio creado por la DTIC el cual forma parte del ciclo de respaldo principal institucional. Este forma parte de los "Respaldos Servidores Plataformas Windows y Linux", citado en el Instructivo para respaldo de Información del centro de datos principal, denominado "UNED-Instructivo de Respaldos centro de Datos", aprobado por el Consejo de Rectoría, en sesión 2064-2020, Artículo IV, inciso 5), celebrada el 20 de enero del 2020.

   b) OneDrive de la Unidad de Seguridad Digital. Espacio que tendrá como función ser una segunda copia de respaldo.

En cuanto a la [4]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.

[4] 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."

2. Definición de una [5]configuración base de Hardware y software.
3. Identificación de las aplicaciones de uso institucional por perfil de funcionario, entendiéndose [6]como:
    a. Perfil: la actividad que desarrolla una persona en su puesto de trabajo.
    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 [7]actividades que cumplen los funcionarios de la universidad,

---

[5] La cual contiene la lista de software que será instalada en todo equipo de cómputo con activo de la UNED. [6]De esta manera se logró identificar los programas que se deben instalar en un computador dependiendo del funcionario que vaya hacer uso del mismo.

6 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.

[7] 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.

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 [8]software que se utilice en los equipos de cómputo de la Universidad deben tener licencia propietaria o GPL.
2. Los perfiles de [9]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.

[8] 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 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.

[9] 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. **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.

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 [10]hardware a nivel institucional:

   - Perfil de Hardware para computadores portátiles “PASCAL”
   - Perfil de Hardware para computadores portátiles “KELVIN”
   - Perfil de Hardware para computadores portátiles “KEPLER”
   - Perfil de Hardware para computadores portátiles MAC “CURIE”
   - Perfil de Hardware para computadores portátiles MAC “DAVINCI”
   - Perfil de Hardware para computadores escritorio “PASCAL”
   - Perfil de Hardware para computadores escritorio “KELVIN”
   - Perfil de Hardware para computadores escritorio “KEPLER”
   - Perfil de Hardware para computadores escritorio MAC “CURIE”
   - Perfil de Hardware para computadores escritorio MAC “DAVINCI”
   - Perfil de Hardware para computadores escritorio PC “DAVINCI”

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.

[10] 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 los 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.

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.

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
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

Localización

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

Identi ficador	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 Da tos 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
HP UX	H

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
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

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
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. 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

[11] 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.

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.)

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
	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.
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.
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.

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.

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

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, 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.

Administración de Contraseñas de Usuario

La asignación de contraseñas se administración siguiendo los siguientes criterios:

1. Los usuarios completan y firmen el respectivo[12]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

[12] 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.

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.

Administración de Contraseñas Críticas

1. En los diferentes ambientes de procesamiento existen [13]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.

[13] 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.

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.
    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.

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.
    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 Titulo, 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.

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.
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:
    - Perdidas 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.

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

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 registras 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
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) Articulo 8 Capitulo 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

        i. Es definido y proporcionado por la UNED, tal y como lo estable en la Configuración base para los equipos de cómputo institucional, el cual es un documento en respuesta al inciso d) Articulo 5 Capitulo 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 los estipulado 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.
7. En caso de anomalías o fallos relacionados con el [14]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:

[14] Una vez instalado en las estaciones de trabajo o máquinas portátiles.

- 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.
- 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.
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:
    a. 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).
    b. Los documentos que contienen macros maliciosas.

c. Los archivos cuyo contenido está protegido con una contraseña.

d. Los archivos protegidos por contraseña que contengan un archivo.

e. 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[15] 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:
    a. Almacenamiento total de los correos (Bandeja de entrada, Bandeja de salida, Elementos enviados, Borradores y Elementos Eliminados).
    b. 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.

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:

[15] 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.

- ✓ 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.

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 autentificación 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.
- **Confiabilidad 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.

  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 Tabletas, 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.

  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.

- ✓ 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 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 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, 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.
- **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

Actores y Responsabilidades

ACTOR	RESPONSABILIDADES
Coordinación de la Unidad de Seguridad Digital de la Dirección de Tecnología de Información y Comunicaciones	• Elaborar el Estudio de incidentes y/o anomalías de Seguridad en TI. • Coordinar con las instancias y/o funcionarios que se considere necesario para elaborar el estudio de incidentes y/o anomalías de Seguridad en TI. • Implementar las acciones que se consideren necesarias para eliminar el riesgo o mitigar los daños en la seguridad en TI. • Elaborar el informe en Seguridad en TIC, para ser trasladado a la Oficina de Recursos Humanos y a la jefatura correspondiente.
Director (a) de la Dirección de Tecnología de Información y Comunicaciones	• 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.
Solicitante	• Solicitar ante la Dirección de Tecnología de Información y Comunicaciones, la elaboración del Estudio de incidentes y/o anomalías de Seguridad en TI. • Implementar las medidas o acciones necesarias de conformidad con los hallazgos del Estudio de incidentes y/o anomalías de Seguridad en TI.
Dependencia (s) y/o Funcionario (a) (s)	• Colaborar y facilitar lo que sea necesario para la elaboración del Estudio de incidentes y/o anomalías de Seguridad en TI.

Matriz Descriptiva de los Procedimientos

PR-06-01 Procedimiento para la atención de estudios, incidentes y/o anomalías de Seguridad Informática.

Orden	Descripción actividades	Responsable	Paso
01.01	Presenta la necesidad de realizar un estudio sobre el uso de equipo de cómputo e internet. En caso de ser derivado del [16]monitoreo, **Pasa al orden 1.3** 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.	**01.02**
01.02	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	**01.03**
01.03	Recibe analiza y coordina con las instancias y/o funcionario(a)s respectivas lo necesario para realizar el estudio	C.USD.DTIC	**01.04**
01.04	Recibe y facilita los respectivo para la realización del estudio	Dep./Func.	**01.05**
01.05	Realiza estudio. En caso de no detectar incidentes o anomalías **pasa al orden 1.7** En caso de detectar anomalías **pasa al orden 1.7** En caso de detectar incidentes	C.USD.DTIC	**01.06**
01.06	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	**01.07**
01.07	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	**01.08**
01.08	Recibe, analiza y tramita lo [17]correspondiente de conformidad con los hallazgos del Informe sobre la seguridad en TIC.	[18]Solic.	**FIN**

[16] El monitoreo es acción exclusiva de la Unidad de seguridad digital de la DTIC.

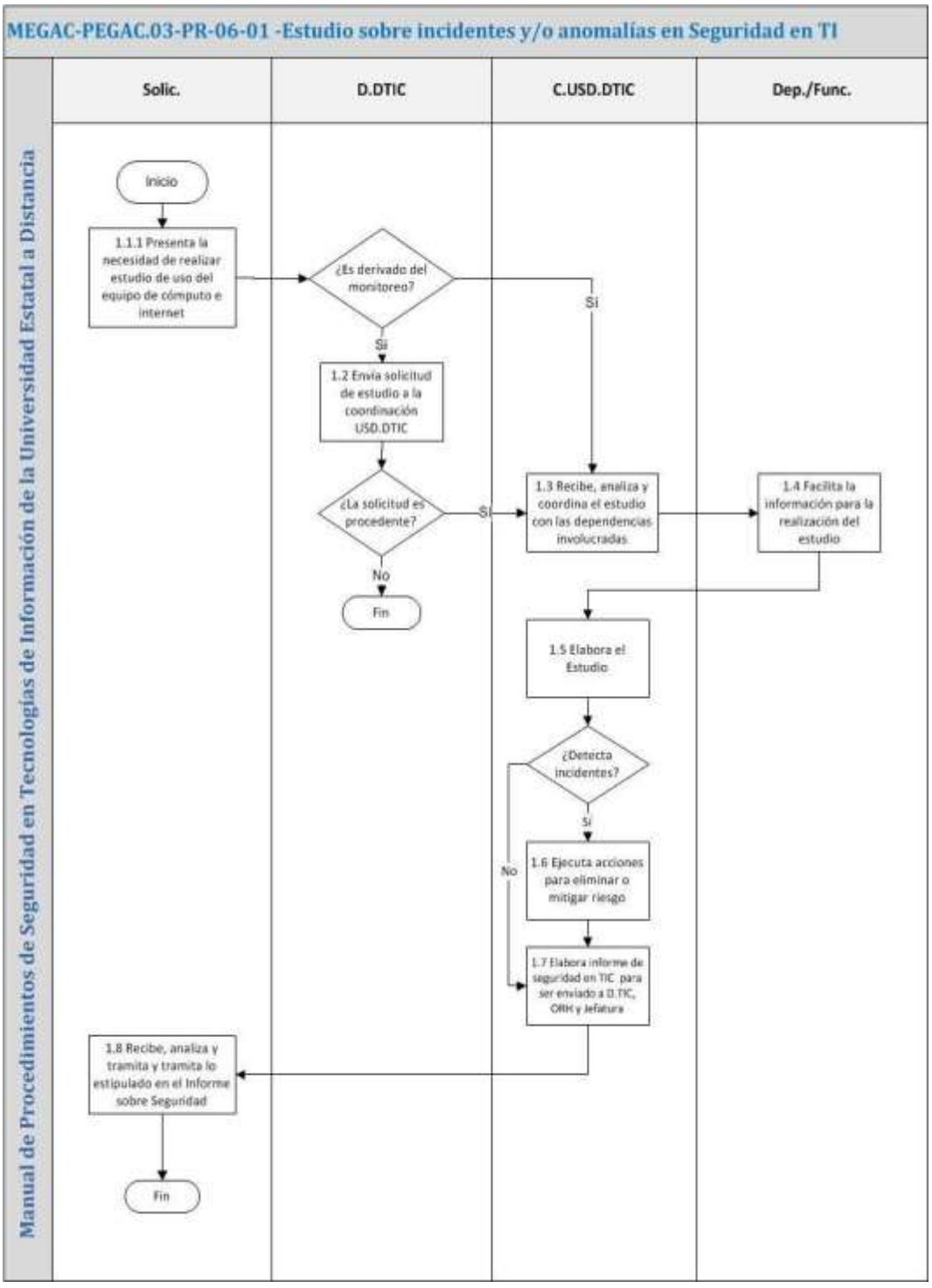
[17] En caso de que se detectara una anomalía o incidente, deberá el/la solicitante aplicar los correspondiente establecido en el Estatuto de personal y el Estatuto orgánico.

[18] En caso de la aplicación de sanciones, la C.USD.DTIC, únicamente suministra los hallazgos en el Informe sobre seguridad en TIC.

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		
N°	**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.

Diagrama o Mapa del Procedimiento



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[19] 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.

[19] 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.

Comunicación

Los mecanismos de comunicación y/o divulgación serán:

1. [20]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.

[20] 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.

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
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

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	• Debe velar por el seguimiento de los procedimientos aquí establecidos, de modo que controle la necesidad de realizar un análisis sobre los mismos. • Debe realizar la/las actualizaciones a este manual y solicitar de ser necesario el acompañamiento al CPPI. • 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. • Cumplir con las demás responsabilidades establecidas en este manual. • Deberá velar por la divulgación del documento y la publicación en la página web de la UNED.
Centro de Panificación y Programación Institucional	• Brindará el acompañamiento necesario de ser solicitado. • Como dependencia competente de considerarlo necesario comunicará cualquier cambio para ser implementado previo consenso con las partes. • Realiza por medio de la jefatura la pre-aprobación según criterio técnico correspondiente.
Otras Dependencias de los Procedimientos de este manual	• Deberán de acatar el cumplimiento de las responsabilidades asignadas en el procedimiento. • 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.

Anexos:

- Directriz en cuanto al acceso a las instalaciones de la DTIC y DATACENTER por parte de terceros
- Directriz sobre el Uso de Redes Privadas Virtuales (VPN) UNED
- Acuerdo de Rectoría CR.2016.124
- Disposiciones de la Ley de Control Interno en cuanto a la Identificación y Valoración de Riesgos de TI
- Responsabilidades de las áreas usuarias de la DTIC https://www.uned.ac.cr/dtic/images/documentos/ResponsabilidadesAreasUsuariasDTIC2.0.pdf
- 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 https://www.uned.ac.cr/dtic/images/documentos/manuales/gestion_usuarios.pdf

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.

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:

Acceso permanente

a. 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.
b. 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.
c. 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

a. 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.
b. Solo la Unidad de Infraestructura Tecnológica podrá entregar autorizaciones de acceso al Centro de Datos.
c. 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.
d. 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

a. Las tarjetas de proximidad solo se entregarán a funcionarios de la DTIC con autorización de acceso permanente aprobado por la UIT.

b. 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.

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).
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 Coordinar de la UIT. Por ejemplo, el ingreso de Cámaras fotográficas o Video de parte de personal del Instituto Nacional de Seguros, cuando realizan inspecciones.

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:

- 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 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.

Acuerdo de Rectoría CR.2016.124

CONSEJO DE RECTORÍA

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

UNED
UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

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:

CONSEJO DE RECTORÍA

TELS: 2224 1689 • 2527-2503 • FAX 2253 4990

CORREO: tmena@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

CONSEJO DE RECTORÍA

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

UNED
UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

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

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 Publico (N-2-2009-CO-DFOE), publicado en la Gaceta Nº 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[21]."*

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

[21] Actualmente PROCI.

proceso. Al ser identificados riesgos de TI estos son analizados en cuanto a su 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[22].

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 [23] 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

[22] Actualmente PROCI.
[23] Entendiéndose proyectos tecnológicos de trascendencia institucional, todos aquellos proyectos que sean aprobados por la Comisión Estratégica de Tecnologías de Información y Comunicaciones.

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
    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.

Responsabilidades de las áreas usuarias de la DTIC

https://www.uned.ac.cr/dtic/images/documentos/ResponsabilidadesAreasUsuariasDTIC2.0.pdf

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

https://www.uned.ac.cr/dtic/images/documentos/manuales/gestion_usuarios.pdf