



POLÍTICAS GENERALES INTERNAS DE SEGURIDAD DE LA INFORMACIÓN, UNIVERSIDAD POLITÉCNICA TERRITORIAL DEL OESTE DE SUCRE "CLODOSBALDO RUSSIÁN"



Cumaná, Mayo año 2026



REPÚBLICA BOLIVARIANA DE VENEZUELA
MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN UNIVERSITARIA
UNIVERSIDAD POLITÉCNICA TERRITORIAL DEL OESTE DE SUCRE
"CLODOSBALDO RUSSIÁN"
RESOLUCIÓN DE CONSEJO UNIVERSITARIO N° 13-04-ORD-2026

CUMANÁ, 01 de Julio de 2026

En el uso de las atribuciones que le confiere el Decreto de creación de la Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián" No. 8.804 publicado en la Gaceta Oficial de la República Bolivariana de Venezuela No 39.902 de fecha 13 de Abril de 2012, mediante el cual se crea la Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián", y en conformidad con lo previsto en los artículos 1 y 43 de la Ley Orgánica de Educación y Gaceta Oficial del a República Bolivariana de Venezuela N° 41.214, Resolución 59 de fecha 15 de agosto de 2017, donde se decreta el Reglamento de Organización y Funcionamiento de la Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián";

POR CUANTO

La organización y funcionamiento de la Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián" debe estar determinada a partir del encargo social de la institución de educación universitaria, a fin de coadyuvar en la organización del espacio geográfico nacional en ejes estratégicos de desarrollo territorial, y tomando las actuales y futuras formas de organización geopolítica-nacional, que sean determinadas por el Ejecutivo Nacional, todo ello en virtud de crear modelos de gestión, formación, generación y socialización de conocimientos estrechamente vinculados a las comunidades y su área de influencia territorial, para facilitar el trabajo cooperativo, solidario y articulado con otras instituciones,

POR CUANTO

Dada la importancia que los activos de información y por ende de la Plataforma Tecnológica de la Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián" (UPTOSCR), del Ministerio del Poder Popular para la Educación Universitaria (MPPEU) a través de la Oficina de Tecnologías de Información y Comunicación (OTIC) de conformidad con el marco legal vigente en materia de seguridad de los activos de información,

DICTA LAS SIGUIENTES:
POLÍTICAS GENERALES INTERNAS DE SEGURIDAD DE LA INFORMACIÓN
UNIVERSIDAD POLITÉCNICA TERRITORIAL DEL OESTE DE SUCRE
"CLODOSBALDO RUSSIÁN"

Realizado por: Lcda. Luisana Parejo, Coordinadora de Gestión Curricular de PNF y PNFA
Revisado por: Ofic. Planificación y Presupuesto / Unid. Organización y Sistemas

Version: 1.0

IVARIAN
PODER POPULAR
ON UNIVERSITARIA

GANIZACION
SISTEMAS

IBBALDO RUSSIÁN
TERRITORIAL DEL OESTE DE

Pág. 3/27



Índice de contenido

CAPÍTULO I. DISPOSICIONES GENERALES.....	8
Del Objetivo.....	8
Ámbito de Aplicación y Alcance.....	8
Base Legal y Documental.....	8
CAPÍTULO II. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN.....	9
Sección I. Clasificación de los Activos de Información.....	9
De la Clasificación.....	9
Sección II. Identificación de los Activos de Información.....	9
De la Identificación.....	9
Sección III. Responsabilidad de Seguridad de la Información.....	9
De los Responsables.....	9
Del Reporte de Incidentes de los Activos de Información.....	10
Medidas de Protección para el manejo de activos de información.....	10
Atención de incidentes.....	10
Sección IV. Responsabilidad de los Custodios de Activos de Información.....	10
Custodios de Activos de Información.....	10
Sección V. Acuerdos de Confidencialidad.....	10
De los Acuerdos.....	10
Sección VI. Responsabilidad del Administrador de Plataforma Tecnológica.....	10
De Responsables.....	10
Del Suministro de Información.....	11
Sección VII. Estándares para el Manejo y uso de los Documentos Electrónicos Internos y Externos.....	11
Manejo y uso de documentación Editable.....	11
Manejo y uso de documentación Portable.....	11
Documentación especializada.....	11
Distribución segura de documentos.....	11
CAPÍTULO III. CONTROL DE ACCESO.....	11
Sección I. Gestión de Contraseñas.....	11
Actualización de Contraseñas.....	11
Protección de Contraseñas.....	11
Responsabilidad del usuario en el manejo de Contraseñas.....	11
Sección II. Gestión de acceso a usuarios.....	12
Responsabilidad del usuario.....	12
Autorización de acceso.....	12
Deshabilitación de acceso.....	12
Control de acceso.....	12
Sección III. Control de Acceso a la Red de Datos.....	12
Monitorización de la red de datos.....	12
Uso de la red de datos.....	12
Seguridad de la información Oficial.....	12
Acceso remoto a la red de datos.....	12
Sección IV. Servicio de Internet.....	13



Gobierno Bolivariano
de Venezuela

Ministerio del poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russián"



Acceso al Servicio de Internet.....	13
Autorización de Acceso a Internet.....	13
Seguridad de la información Institucional.....	13
Descarga de Software.....	13
Daños a Activos de Información de Terceros.....	13
Uso Inadecuado del Internet.....	13
Control a los Recursos de Internet.....	13
Monitorización de Sitios Web.....	13
Restricción de Acceso a Internet.....	13
CAPÍTULO IV. REPORTE DE INCIDENTES, FALLAS Y EVENTOS.....	13
Sección I. Gestión de Reportes.....	13
Reporte de Incidentes, Fallas y Eventos de Seguridad de la Información.....	13
Actuación del Usuario ante un Incidente.....	14
Suministro de Información ante un Incidente.....	14
Gestión del Incidente, Falla o Evento.....	14
Suministro de Información a los Organismos de Seguridad del Estado.....	14
Seguridad de la Información ante un Incidente.....	14
CAPÍTULO V. GESTIÓN DE COMUNICACIONES Y OPERACIONES TÉCNICAS.....	14
Sección I. Gestión de Cambios y Responsabilidades de Procedimientos Técnicos	
Operativos.....	14
Cambios en la Plataforma Tecnológica.....	14
Gestión de Cambios.....	14
Cambios Tecnológicos de Alto Impacto.....	14
Seguridad de la Información ante un Incidente.....	14
Protección contra Código Malicioso y Descargable.....	14
Protección de la Plataforma Tecnológica.....	15
Sección II. Control de la Red de Datos.....	15
Medidas de Seguridad a la Red de Datos.....	15
Control de la Red de Datos.....	15
Mensaje de Advertencia.....	15
Sección III. Servicio del Correo Electrónico.....	15
Intercambio de Información a través del Correo Electrónico Institucional.....	15
Propiedad de la información en el servicio de Correo Electrónico.....	15
Valor jurídico de los mensajes de datos a través del Correo Electrónico Institucional.....	15
Auditoría a los mensajes de buzones.....	15
Seguridad en la administración de contratos.....	15
Incumplimiento de Políticas del servicio de correo electrónico institucional.....	16
Manejo seguro de evidencias.....	16
Monitorización de envío y recepción de mensajes a través del Correo Electrónico Institucional.....	16
Intercambio seguro de Información entre la UPTOSCR y otras instituciones.....	16
Restricción de dominios libres de la Internet.....	16
Mensaje Institucional a través del correo electrónico institucional.....	16
Mensajes prohibidos a través del correo electrónico institucional.....	16
Integridad de mensajes del correo electrónico institucional.....	16
Recepción de mensajes de dudosa procedencia.....	16
Imagen de la Institución a través del correo electrónico.....	17
Afiliación de cuentas del correo electrónico institucional.....	17
Protección del servicio del correo electrónico institucional.....	17

Realizado por: Lcda. Luisana Parejo, Coordinadora de Gestión Curricular de PNF y PNFA
Revisado por: Ofic. Planificación y Presupuesto / Unid. Organización y Sistemas
Versión: 1.0

Sección IV. Gestión de Respaldo.....	17
Respallos periódicos.....	17
Protección de activos de información electrónica.....	17
Resguardo de activos de información de la UPTOSCR.....	17
CAPÍTULO VI. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	17
Sección I. Adquisición y Desarrollo de Sistemas.....	17
Adquisición de aplicaciones.....	17
Evaluación de riesgo de las aplicaciones.....	18
Medidas de seguridad en las aplicaciones.....	18
Mantenimiento de las aplicaciones.....	18
Sección II. Controles Criptográficos.....	18
Controles Criptográficos.....	18
Control de acceso a archivos encriptados.....	18
Sección III. Seguridad de los Procesos de Desarrollo y Soporte.....	18
Control de cambios en desarrollo de aplicaciones.....	18
Documentación de cambios en desarrollo de aplicaciones.....	18
Responsabilidad de cambio bajo Estándares de Calidad.....	18
Sección IV. Seguridad Base de los Sistemas Operativos.....	18
Seguridad de los archivos del sistema.....	18
CAPÍTULO VII. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	19
Sección I. Plan de Continuidad.....	19
Efectividad de los planes de atención de eventualidad.....	19
Actualización de planes para el manejo de eventualidades.....	19
Documentación de planes para el manejo de eventualidades.....	19
Activación de los planes para la continuidad de las operaciones.....	19
Manejo de eventualidades para la continuidad de las operaciones.....	19
Efectividad de los planes para la continuidad de las operaciones.....	19
Sección II. Recuperación de las Operaciones.....	19
Pruebas y simulacros para la recuperación de las operaciones.....	19
Tiempo de recuperación ante eventualidades.....	19
Redundancia en los sistemas de la UPTOSCR.....	20
Mantenimiento de la plataforma tecnológica de la UPTOSCR.....	20
CAPÍTULO VIII. SEGURIDAD FÍSICA Y AMBIENTAL.....	20
Sección I. Centro de Almacenamiento y Procesamiento de Datos (CAPD).....	20
Seguridad en la administración de los datos de la UPTOSCR.....	20
Efectividad del Sistema Contra Incendio.....	20
Efectividad del Sistema de Alimentación de Energía.....	20
Efectividad de los Servicios Auxiliares.....	20
Estructuración del cableado de la red de dato.....	20
Seguridad en los CAPD.....	20
Almacenamiento y procesamiento de datos por terceros.....	20
Sección II. Seguridad de los Equipos.....	21
Correctivos y actualizaciones de los equipos.....	21
Conexión de equipos tecnológicos ajenos a la institución.....	21
Gestión de información dentro de la red de datos de la UPTOSCR.....	21
Uso adecuado de los equipos tecnológicos de la UPTOSCR.....	21
Prohibición de instalación de programas.....	21



Gobierno Bolivariano
de Venezuela

Ministerio del poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russián"



Uso adecuado de los equipos que procesan información.....	21
Seguridad, Higiene y Ambiente de los equipos tecnológicos.....	21
Manejo de incidente de equipos tecnológicos.....	21
Sobre la movilización de Equipos.....	21
CAPÍTULO IX. CÓDIGO DE ÉTICA PARA EL DESARROLLO Y APLICACIÓN RESPONSABLE DE LA	
INTELIGENCIA ARTIFICIAL EN UPTOS.....	22
Sección I. Principios Generales.....	22
Sección II. Desarrollo y Adquisición de Sistemas con IA.....	22
Sección III. Operación y Gobernanza de la IA.....	23
Sección IV. Capacitación y Difusión.....	23
CAPÍTULO X. GLOSARIO Y SIGLAS.....	23
Sección I. Glosario.....	23
Sección II. Siglas.....	27



Gobierno Bolivariano
de Venezuela

Ministerio del Poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russián"



CAPÍTULO I. DISPOSICIONES GENERALES

Del Objetivo

ARTÍCULO 1. La presente tiene por objeto establecer las directrices sobre el cual toda trabajadora, trabajador y demás personas que intervienen en los servicios informáticos de la Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián" (UPTOS "CR"), deben regirse para tratar y proteger los activos de información considerados "Estrictamente Confidencial" y "Confidencial" de la Institución.

Ámbito de Aplicación y Alcance

ARTÍCULO 2. Estas Políticas Generales Internas aplican para todas las trabajadoras, trabajadores y comunidad en general que participan en la prestación de los servicios que brinda la UPTOS "CR", así como el Núcleo Ribero, Extensión Montes, Extensión Bolívar y Extensión Cruz Salmerón Acosta.

Base Legal y Documental

ARTÍCULO 3. Las presentes Políticas Generales Internas basarán su funcionamiento en los siguientes instrumentos jurídicos y documentales:

- a) Constitución de la República Bolivariana de Venezuela, con la Enmienda N° 1 aprobada el 15/02/2009, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Extraordinario No. 5.908, de fecha 19/02/2009.
- b) Ley Orgánica de la Administración Pública. Gaceta Oficial N° 37.305 de fecha 17 de octubre del 2001.
- c) Ley Orgánica de Ciencia Tecnología e Innovación. Gaceta Oficial N° 39.575 de fecha 16 diciembre del 2010.
- d) Ley Orgánica de Procedimientos Administrativos, Publicada en la Gaceta Oficial de la República Bolivariana de Venezuela, N° 2.818 Extraordinaria del 1° de julio de 1981.
- e) Ley del Trabajo, de las Trabajadoras y los Trabajadores, Decreto N° 8.938, 30 de abril de 2012, publicado en la Gaceta Oficial N° 6.076 Extraordinario del 7 de mayo de 2012.
- f) Ley Especial contra Delitos Informáticos. Publicada en Gaceta Oficial N°37.313 de fecha 30 de octubre de 2001.
- g) Ley de Infogobierno. Gaceta Oficial N° 40.274 de fecha 17 de octubre de 2013.
- h) Ley del Estatuto de la Función Pública, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela, Extraordinario N° 5556, en fecha 13/11/2001.
- i) Resoluciones Nro(s) 005 y 006 de la Gaceta Oficial de la República Bolivariana de Venezuela N°39.109 de fecha 29.01.2009.
- j) Providencia Administrativa de la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), adscrita al Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias, N° 009-10, de fecha 22/10/2010, publicada en Gaceta Oficial de la República Bolivariana de Venezuela N° 39.578, de fecha 21/12/2010.
- k) Norma Internacional de Estándares de Seguridad de la Información ISO 17999 / 27001 / 27002.
- l) Norma Técnica ISO/IEC 26300:2006: Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0.
- m) Norma ISO 32000-1:2008 Document management -- Portable document format-- Part 1: PDF 1.7.
- n) Recomendación sobre la ética de la Inteligencias Artificial, UNESCO 2022.
- o) Código de Ética para el Desarrollo y Aplicación Responsable de la IA, MPPCT. Enero 2026.
- p) Convención Colectiva Única de Trabajadoras y Trabajadores Universitarios vigente.
- q) Las demás que señale el ordenamiento jurídico vigente.

CAPÍTULO II. GESTIÓN DE LOS ACTIVOS DE INFORMACIÓN

Sección I. Clasificación de los Activos de Información

De la Clasificación

ARTÍCULO 4. Todo Activo de Información en cualquiera de sus formas (impresa, manuscrita, oral, electrónica o visual) perteneciente a, o bajo la custodia de la UPTOS "CR", sus dependencias, Núcleo Ribero y Extensiones, debe ser clasificado y tomando en consideración bajo los siguientes criterios establecidos:

- **Estrictamente Confidencial:** Activo de Información valioso, relacionado con la dirección operacional o estratégica, cuyo conocimiento, divulgación o modificación por parte de personas no autorizadas, causen graves daños a la universidad.
- **Confidencial:** Activo de Información sensible, relacionado con el personal, clientes, información técnica y administrativa, cuya divulgación a personas no autorizadas causen daños a la Universidad o a sus propietarios.
- **De Uso Interno:** Activos de Información que no requieran medidas de protección especiales, y cuyo acceso, manipulación y divulgación, se realice en base al cumplimiento de las funciones propias de la Universidad.
- **De Uso Público:** Activos de la Información que no requieren de ninguna medida de protección, su acceso y manipulación pueden ser realizados de forma libre a través de todo medio disponible en la Institución. Su conocimiento no afecta función alguna.

Sección II. Identificación de los Activos de Información

De la Identificación

ARTÍCULO 5. Todo Activo de Información perteneciente a, o bajo la custodia de la UPTOS "CR", sus dependencias, Núcleo Principal y Extensiones, debe ser rotulado de acuerdo a la tabla N° 1, de manera que todos los usuarios puedan tener conocimiento acerca de su clasificación.

Color	Fig. Geométrica	Clasificación
ROJO	Círculo	Estrictamente Confidencial
NARANJA	Rombo	Confidencial
AZUL	Cuadrado	De Uso Interno
VERDE	Triángulo	De Uso Público

Tabla N° 1. Nomenclatura de Identificación Visual de los Activos de Información.

PARÁGRAFO ÚNICO. Todo Activo de Información generado o creado debe considerarse en el Documento de Identificación de Activos, ser rotulados utilizando sellos con la identificación del UPTOS "CR", la clasificación respectiva y la dependencia organizativa propietaria. (Ver Anexo N°1).

Sección III. Responsabilidad de Seguridad de la Información

De los Responsables

ARTÍCULO 6. Los responsables de Seguridad de la Información de la UPTOS "CR", debe supervisar la



correcta identificación de los activos de la información, administrada por el Propietario o Custodio a fin de garantizar su confidencialidad, integridad y disponibilidad.

PARÁGRAFO ÚNICO. Todo Activo de Información debe ser protegido, custodiado y resguardado de acuerdo a los niveles de clasificación aquí establecidos.

Del Reporte de Incidentes de los Activos de Información

ARTÍCULO 7. Tanto el Propietario como los Custodios de la información, deben reportar la pérdida, robo, hurto, sabotaje, divulgación o destrucción no autorizada de los activos de información, al responsable de la Seguridad de la Información de la UPTOSCR, a fin de levantar investigaciones y establecer las responsabilidades pertinentes al caso, de acuerdo a lo establecido en el marco legal vigente.

Medidas de Protección para el manejo de activos de información

ARTÍCULO 8. Los responsables de Seguridad de la Información de la UPTOSCR, deben emitir las medidas para almacenar, manejar, proteger y destruir adecuadamente los Activos de Información clasificados como "Estrictamente Confidencial" o "Confidencial" en cualquiera de sus formas.

Atención de incidentes

ARTÍCULO 9. Los responsables de Seguridad de la Información de la UPTOSCR, deben solicitar toda la información necesaria (registros de auditoría (Logs), así como registros de errores y fallas de aplicaciones), entre otros, al responsable de la Administración de la Plataforma Tecnológica, a fin de atender incidentes relacionados con la pérdida, robo, hurto, sabotaje, ingeniería social, divulgación o destrucción no autorizada de los activos de información.

Sección IV. Responsabilidad de los Custodios de Activos de Información

Custodios de Activos de Información

ARTÍCULO 10. La responsabilidad de protección, resguardo y custodia sobre cada Activo de Información, debe ser asignada a los Directores Generales, Coordinadores de área, Líderes o Jefes de grupo de la UPTOSCR y de cada Núcleo y/o dependencia adscrita, de acuerdo a su estructura organizativa. Sin embargo, es importante recalcar que, toda trabajadora y trabajador es co-responsable en la custodia de la información que maneje.

Sección V. Acuerdos de Confidencialidad

De los Acuerdos

ARTÍCULO 11. La UPTOSCR y cada Núcleo y/o dependencia adscrita, a través de la Oficina de Gestión Humana, y la Oficina de Tecnologías de Información y Comunicación (OTIC) de la Universidad, deben implementar una Declaración de Confidencialidad para los trabajadoras y trabajadores y otra para terceros en la cual, se establezca los términos y condiciones, bajo las cuales, se debe manejar y resguardar la información clasificada como Estrictamente Confidencial o Confidencial. Se entiende por trabajadoras y trabajadores: empleados directos o fijos, contratados directos, pasantes, comisión de servicio y por terceros: contratistas, consultores, personal temporal, cooperativas, voluntarios.

Sección VI. Responsabilidad del Administrador de Plataforma Tecnológica

De Responsables

ARTÍCULO 12. Los responsables de la administración de la Plataforma Tecnológica, deben implementar los mecanismos de resguardo y protección de los Activos de Información emitidos por los responsables de Seguridad de la Información de la UPTOSCR y de cada Núcleo.



Del Suministro de Información

ARTÍCULO 13. Los responsables de la administración de la Plataforma Tecnológica, deben suministrar toda la información necesaria (registros de auditoría, así como el registro de errores y fallas de aplicaciones, entre otros) a los responsables de Seguridad de la Información de la UPTOSCR, a fin de atender incidentes relacionados con la pérdida, robo, hurto, sabotaje, ingeniería social, divulgación o destrucción no autorizada de los activos de información.

Sección VII. Estándares para el Manejo y uso de los Documentos Electrónicos Internos y Externos

Manejo y uso de documentación Editable

ARTÍCULO 14. Toda información que se maneje en la UPTOSCR, debe cumplir con los estándares establecidos en la Ley de Infogobierno, las resoluciones Nro (s) 005 y 006 y Norma Técnica ISO/IEC 26300:2006: Information technology -- Open Document Format for Office Applications (OpenDocument) v1.0.

Manejo y uso de documentación Portable

ARTÍCULO 15. La UPTOSCR, cada Núcleo y/o dependencia adscrita, que generen, procesen o almacenen documentos electrónicos ofimáticos, en lo que se requiera preservar la capacidad de modificación de la información, deben aplicar y usar el Formato Abierto de Documentos (ODF), siendo la herramienta a utilizar para la edición de documentos en cualquier herramienta de software libre que cumpla con los estándares antes mencionados. De acuerdo a la Norma ISO 32000-1:2008 Document management -- Portable document format -- Part 1: PDF 1.7.

Documentación especializada

ARTÍCULO 16. La UPTOSCR, cada Núcleo y/o dependencia adscrita, que generen, procesen o almacenen documentos electrónicos con características especializadas, utilizarán herramientas para la edición y publicación en Software Libre.

Distribución segura de documentos

ARTÍCULO 17. La UPTOSCR y de cada Núcleo y/o dependencia adscrita, que generen, procesen o almacenen documentos electrónicos que no tengan por finalidad ser editados, o distribuidos a terceros, conservando la integridad de su aspecto gráfico y su contenido, deben aplicar el Formato de Documentos Portátil (PDF), de acuerdo a la Norma ISO 32000-1:2008 Document management -- Portable document format -- Part 1: PDF 1.7.

CAPÍTULO III. CONTROL DE ACCESO

Sección I. Gestión de Contraseñas

Actualización de Contraseñas

ARTÍCULO 18. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben implementar medidas que permitan la actualización de las contraseñas de forma periódica.

Protección de Contraseñas

ARTÍCULO 19. Los responsables de la administración de la Plataforma Tecnológica de la UPTOSCR, deben ajustar las contraseñas de sistemas, a los criterios de seguridad establecidos y autorizados por los responsables de Seguridad de la Información de la UPTOSCR.

Responsabilidad del usuario en el manejo de Contraseñas

ARTÍCULO 20. Todas las trabajadoras y trabajadores, estudiantes y demás personas que intervienen en el intercambio de información dentro de la plataforma tecnológica de la UPTOSCR, deben resguardar la



privacidad de la contraseña y evitar el alcance de personas no autorizadas o en archivos electrónicos no protegidos.

Sección II. Gestión de acceso a usuarios

Responsabilidad del usuario

ARTÍCULO 21. Es responsabilidad única y exclusiva del usuario el uso adecuado de los accesos y privilegios otorgados, todo identificador electrónico asignado a este, debe ser único e intransferible y su clave de acceso intransferible.

PARÁGRAFO PRIMERO. Todo usuario inactivo con acceso a servicios crítico debe ser deshabilitado de manera inmediata.

PARÁGRAFO SEGUNDO. Está terminantemente prohibida la creación de cuentas genéricas para el acceso de Aplicaciones o Sistemas de Información.

Autorización de acceso

ARTÍCULO 22. Todo acceso y privilegios a la plataforma tecnológica de la Institución, debe estar formalmente autorizado y avalado por la máxima autoridad del área solicitante. Queda terminantemente prohibido el acceso sin autorización a la plataforma tecnológica.

Deshabilitación de acceso

ARTÍCULO 23. Todas las trabajadoras y trabajadores de la UPTOSCR, y Núcleos y las demás personas que intervienen y demás personas que intervengan en la prestación de servicio académico y que gestionen información "Estrictamente Confidencial" y "Confidencial", cuyas funciones sean modificadas, o terminen su relación laboral y/o contrato con la Institución, se le debe deshabilitar los accesos y privilegios a la plataforma tecnológica.

Control de acceso

ARTÍCULO 24. Todo acceso y deshabilitaciones de privilegios a la plataforma tecnológica de todas las trabajadoras y trabajadores de la UPTOSCR, y Núcleos y demás personas que intervengan en la prestación de servicio académico, debe ser restringido, registrado y auditado.

Sección III. Control de Acceso a la Red de Datos

Monitorización de la red de datos

ARTÍCULO 25. Todo acceso a la red de datos, debe estar registrado por los servicios, monitoreado por el administrador de la misma y auditado por los responsables de Seguridad de la Información.

Uso de la red de datos

ARTÍCULO 26. La red de datos debe utilizarse para transmitir información de interés de la Institución.

Seguridad de la información Oficial

ARTÍCULO 27. La transmisión vía red de datos de información oficial "Estrictamente Confidencial" y "Confidencial" y su almacenamiento en cualquier sistema, debe garantizar su integridad, confiabilidad y disponibilidad.

Acceso remoto a la red de datos

ARTÍCULO 28. Todo acceso a la red datos vía remota, debe ser asignado por tiempo determinado.



Gobierno Bolivariano
de Venezuela

Ministerio del poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russián"



Sección IV. Servicio de Internet

Acceso al Servicio de Internet

ARTÍCULO 29. Todas las trabajadoras y trabajadores de la UPTOS "CR", sus Núcleos y demás personas que intervengan en la prestación de servicio académico, deben acceder al servicio de Internet a través de conexiones autorizadas por la Institución.

Autorización de Acceso a Internet

ARTÍCULO 30. El acceso a Internet debe estar autorizado por la máxima autoridad del área solicitante, de acuerdo a las funciones inherentes al cargo.

Seguridad de la información Institucional

ARTÍCULO 31. Los responsable de la administración del servicio de Internet, deben implementar mecanismos y herramientas para proteger la información de la UPTOSCR y sus Núcleos, mientras se transmita por la red de Internet.

Descarga de Software

ARTÍCULO 32. Prohibido descargar, software no autorizado por la Institución. Solo para uso académico y de investigación se realizará la evaluación de permisos para el acceso requerido a través de Oficina de Tecnologías de Información y Comunicación (OTIC).

Daños a Activos de Información de Terceros

ARTÍCULO 33. Los daños sobre activos y conflictos con terceros, derivados del uso no autorizado de Internet no será responsabilidad de la UPTOSCR y sus Núcleos. El responsable será sancionado de acuerdo a las leyes vigentes en el país.

Uso Inadecuado del Internet

ARTÍCULO 34. Prohibido el acceso a Internet para asuntos personales, material obsceno o pornográfico, material que conlleve a actividades ilegales, que inciten a la violencia o promuevan la discriminación o terrorismo.

Control a los Recursos de Internet

ARTÍCULO 35. Todo acceso a los recursos de Internet, debe ser registrado y monitoreado como acción preventiva por los responsables de la plataforma tecnológica.

Monitorización de Sitios Web

ARTÍCULO 36. Los responsables de Seguridad de la Información de la UPTOSCR, se reserva el derecho de auditar los registros de acceso a los sitios web por los usuarios; así como monitorear el cumplimiento de las normas y políticas establecida para ello.

Restricción de Acceso a Internet

ARTÍCULO 37. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben utilizar Internet, como herramienta de interés público para las ciencias, la tecnología, la innovación y demás servicios de información relacionados con su trabajo. La Institución se reserva el derecho de restringir su acceso de acuerdo a las funciones que desempeñe.

CAPÍTULO IV. REPORTE DE INCIDENTES, FALLAS Y EVENTOS

Sección I. Gestión de Reportes

Reporte de Incidentes, Fallas y Eventos de Seguridad de la Información

ARTÍCULO 38. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, que detecte un incidente, falla o evento en materia de seguridad de los activos de información, debe reportarlo de inmediato por los canales establecidos (a través de un escrito por correo o en reunión) a los responsables de Seguridad de la Información de la UPTOSCR.

Actuación del Usuario ante un Incidente

ARTÍCULO 39. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben garantizar la no manipulación del dispositivo involucrado en el incidente, falla o evento hasta que los responsables de las dependencias responsables hagan acto de presencia para iniciar la investigación.

Suministro de Información ante un Incidente

ARTÍCULO 40. Todas las trabajadoras y trabajadores de la UPTOSCR, sus Núcleos y demás personas que intervengan en la prestación de servicio académico, deben suministrar información veraz y oportuna.

Gestión del Incidente, Falla o Evento

ARTÍCULO 41. Los responsables de Seguridad de la Información de la UPTOSCR, son los encargados de gestionar el incidente, falla o evento de forma inmediata, por lo tanto debe contar con los accesos a las herramientas y equipos involucrados para llevar a cabo la investigación.

Suministro de Información a los Organismos de Seguridad del Estado

ARTÍCULO 42. De acuerdo al impacto del incidente, falla o evento, los responsables de Seguridad de la Información de la UPTOSCR, informarán a los Organismos de Seguridad del Estado, dependencias organizativas del MPPECT y demás personas que intervienen en la prestación del Servicio Público Académico Universitario de la cual se requiera su participación en la investigación.

Seguridad de la Información ante un Incidente

ARTÍCULO 43. Todos los datos e información que maneje el equipo de investigación antes, durante y posterior a su desarrollo, debe ser de carácter "Estrictamente Confidencial". Esta condición es de obligatorio cumplimiento para todos los integrantes y la violación a la misma devengará las sanciones que la ley establece en materia de seguridad de la información y las establecidas por los procesos internos de la UPTOSCR.

CAPÍTULO V. GESTIÓN DE COMUNICACIONES Y OPERACIONES TÉCNICAS**Sección I. Gestión de Cambios y Responsabilidades de Procedimientos Técnicos Operativos****Cambios en la Plataforma Tecnológica**

ARTÍCULO 44. Los administradores responsables de las plataforma tecnológica de la UPTOSCR, deben evaluar el impacto potencial de los futuros cambios.

Gestión de Cambios

ARTÍCULO 45. Todo cambio en la plataforma tecnológica de la UPTOSCR, debe registrarse por un procedimiento formal de control de cambios.

Cambios Tecnológicos de Alto Impacto

ARTÍCULO 46. Todo cambio en la plataforma tecnológica de alto impacto, debe ser evaluado y autorizado por los responsables de Seguridad de la Información de la UPTOSCR, con el correspondiente informe de riesgos y mitigación.

Seguridad de la Información ante un Incidente

ARTÍCULO 47. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben recuperar la condición inicial de los servicios y reservar los cambios no exitosos de las operaciones.

Protección contra Código Malicioso y Descargable

ARTÍCULO 48. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben monitorear y proteger los sistemas de información para que se detecte, aísle y remueva cualquier código



malicioso de los mismos.

Protección de la Plataforma Tecnológica

ARTÍCULO 49. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben realizar de forma periódica las actualizaciones de la misma, para atender y prevenir los códigos maliciosos que atenten contra la continuidad de las operaciones de la Institución.

Sección II. Control de la Red de Datos

Medidas de Seguridad a la Red de Datos

ARTÍCULO 50. Los responsables de Seguridad de la Información de la UPTOSCR, debe dictar las medidas de seguridad para proteger la integridad, confiabilidad y disponibilidad de los datos en la red, contra accesos no autorizados a los servicios.

Control de la Red de Datos

ARTÍCULO 51. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben implementar los controles dictados por los responsables de Seguridad de la Información de la UPTOSCR.

Mensaje de Advertencia

ARTÍCULO 52. Toda conexión inicial de los usuarios a la red de datos institucional, debe advertir a través de un mensaje, lo siguiente: "Los recursos de procesamiento de la información son propiedad y de uso exclusivo de la UPTOSCR, el acceso no autorizado está prohibido, toda actividad estará siendo monitoreada".

Sección III. Servicio del Correo Electrónico

Intercambio de Información a través del Correo Electrónico Institucional

ARTÍCULO 53. Las cuentas de las todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio de gestión académica y/o administrativa, deben usarse sólo para propósitos relacionados con las actividades laborales e institucionales, así como cualquier información de interés de la máxima autoridad.

Propiedad de la información en el servicio de Correo Electrónico

ARTÍCULO 54. Los mensajes que se envíen a través del correo electrónico son propiedad de la UPTOSCR "Clodosbaldo Russián".

Valor jurídico de los mensajes de datos a través del Correo Electrónico Institucional

ARTÍCULO 55. El responsable de Seguridad de la Información de la UPTOSCR, debe evaluar políticas de certificación electrónica para su implementación, en conformidad con la ley vigente venezolana que rige esta materia, para otorgarle un valor jurídico a los mensajes de datos y a todos activos de información intangible en formato electrónico de la Institución y dar cumplimiento a las normativas emanadas desde el MPPCT en materia de certificación electrónica a las Autoridades de la UPTOSCR.

Auditoría a los mensajes de buzones

ARTÍCULO 56. Los responsables de Seguridad de la Información de la UPTOSCR, son los únicos que deben hacer auditoría a los mensajes en los buzones de los empleados cuando exista una necesidad legítima que afecte la operativa de la Institución o requiera un motivo disciplinario, previa solicitud de la Dependencia afectada y autorización de la máxima autoridad de la Institución.

Seguridad en la administración de contratos

ARTÍCULO 57. Todo contrato entre la UPTOSCR, Núcleos y demás personas que intervengan en la prestación del Servicio Académico, deben contemplar cláusulas que protejan la información, específicamente si se establece que la comunicación es por vía de correo electrónico.

Incumplimiento de Políticas del servicio de correo electrónico institucional

ARTÍCULO 58. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, que tenga conocimiento de algún empleado que incumpla estas políticas, debe notificarlo de manera inmediata a los responsables de Seguridad de la Información de la UPTOSCR para su evaluación y revisión, así como al custodio de la información.

Manejo seguro de evidencias

ARTÍCULO 59. Los responsables de la administración del servicio de correo electrónico institucional de la UPTOSCR, deben emitir evidencias condicionadas a las políticas y lineamientos implementado que respalden la información requerida por los responsables de Seguridad de la Información.

Monitorización de envío y recepción de mensajes a través del Correo Electrónico Institucional

ARTÍCULO 60. Los responsables de la Plataforma Tecnológica de la UPTOSCR, deben garantizar el monitoreo del origen y destino de los mensajes de correo por las trabajadoras y trabajadores, de acuerdo a lo suscrito a estas políticas. Dicho monitoreo permitirá revisiones y auditorias de los mensajes por los responsables de la Seguridad de la Información cuando sea necesario.

Intercambio seguro de Información entre la UPTOSCR y otras instituciones

ARTÍCULO 61. Todo intercambio de información entre la UPTOSCR y otras instituciones del Estado, vía correo electrónico, debe regirse por el ente certificador del país de origen.

Restricción de dominios libres de la Internet

ARTÍCULO 62. Prohibido el envío y recepción de toda información institucional, a través de cuentas de correo electrónico de dominios libres no administrado por el Estado venezolano.

Mensaje Institucional a través del correo electrónico institucional

ARTÍCULO 63. Todo mensaje electrónico que se envíe desde las cuentas de correo electrónico de la UPTOSCR hacia usuarios externos, debe salir con la siguiente información (en los idiomas: español e inglés) a pie del mensaje: "Esta nota puede contener información de interés sólo para la UPTOSCR. Está permitido sólo su copia, distribución o uso a personas autorizadas. Si recibió esta nota por error, por favor destrúyala y notifique al remitente o a contacto@uptos.edu.ve".

Mensajes prohibidos a través del correo electrónico institucional

ARTÍCULO 64. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben evitar la transmisión de información electrónica de naturaleza fraudulenta, contenido sexual explícito, obsceno, intimidatorio, difamatorio, ilícito, intolerantes hacia tendencias culturales, políticas y creencias religiosas, expresados a través de videos, sonidos, imágenes o texto entre otros.

Integridad de mensajes del correo electrónico institucional

ARTÍCULO 65. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben evitar leer, borrar, copiar o modificar mensajes de correos electrónicos que no le pertenezcan, al menos que esté explícitamente justificado y aprobado por el autor del mismo.

Recepción de mensajes de dudosa procedencia

ARTÍCULO 66. Todas las trabajadoras y trabajadores de la UPTOSCR, sus Núcleos y demás personas que intervengan en la prestación de servicio académico, deben evitar abrir mensajes con asunto o remitentes de dudosa procedencia, los cuales serán catalogados como spam y/o virus.



Gobierno Bolivariano
de Venezuela

Ministerio del poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russian"



Imagen de la Institución a través del correo electrónico

ARTÍCULO 67. Todas las trabajadoras y trabajadores de la UPTOSCR, sus Núcleos y demás personas que intervengan en la prestación de servicio académico, deben evitar emplear en los mensajes del sistema de correo electrónico de la universidad, accesorios tales como adornos, caricaturas, gráficos, dibujos o fondos; que no correspondan con una imagen autorizada por la Institución.

Afiliación de cuentas del correo electrónico institucional

ARTÍCULO 68. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben evitar afiliar su cuenta de correo electrónico institucional a servicios que no sean institucionales y ajenos a los servicios inherentes a la universidad.

Protección del servicio del correo electrónico institucional

ARTÍCULO 69. Los administradores del servicio de correo electrónico, deben garantizar a través de mecanismos de seguridad la protección del sistema contra virus, gusanos, bombas de correo y otros códigos maliciosos, así como posibles intersección a los mismos.

Sección IV. Gestión de Respaldo

Respaldos periódicos

ARTÍCULO 70. Los responsables de la administración de la plataforma tecnológica, deben aplicar los procedimientos de respaldo de forma periódica y estar alineado con el plan de continuidad de las operaciones críticas, de modo que puedan ser ejecutados dentro de los tiempos requeridos por la Institución, además de tener su respectiva identificación estándar según normas internas.

Protección de activos de información electrónica

ARTÍCULO 71. Todo activo de información en forma electrónica, debe ser respaldado de acuerdo a su criticidad y sensibilidad, asegurar la frecuencia, el período de retención, la calidad del respaldo y el almacenamiento protegido, lógica, física y ambientalmente. El tiempo de preservación de estos respaldos se ajustará a lo establecido en el marco legal vigente.

Resguardo de activos de información de la UPTOSCR

ARTÍCULO 72. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben garantizar que toda información que gestionan los sistemas informáticos de la UPTOSCR, las almacenadas en los PC y portátiles, de utilidad para el trabajo de los usuarios finales, cuenten con respaldos, que garanticen las actividades bajo su responsabilidad. El respaldo de la información oficial "Estrictamente Confidencial" y "Confidencial" se realizará en medios de almacenamientos autorizados, en los lugares de acceso restringido. Así mismo, los usuarios y custodios de la información deben cumplir las normas de resguardo dictadas por los responsables de la plataforma para garantizar su almacenamiento en la Intranet universitaria.

CAPÍTULO VI. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Sección I. Adquisición y Desarrollo de Sistemas

Adquisición de aplicaciones

ARTÍCULO 73. Toda adquisición y desarrollo de sistemas de información para la gestión administrativa de la Institución deben estar desarrollados en Software Libre.



Evaluación de riesgo de las aplicaciones

ARTÍCULO 74. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben realizar la evaluación de riesgo antes de la adquisición de nuevos aplicativos tecnológicos, con la finalidad de validar los controles de seguridad.

Medidas de seguridad en las aplicaciones

ARTÍCULO 75. A toda implementación de Sistemas de Información Tecnológicos, se le deben aplicar las medidas establecidas por los responsables de Seguridad de la información de la UPTOSCR, para optimizar su implementación.

Mantenimiento de las aplicaciones

ARTÍCULO 76. Toda aplicación de la plataforma tecnológica, debe disponer de un mantenimiento periódico que contemple las actualizaciones, que permita ofrecer una alta confiabilidad, integridad, disponibilidad y flexibilidad de crecimiento, dependiendo de las necesidades que la Institución demande y reducir los riesgos en estos sistemas.

Sección II. Controles Criptográficos

Controles Criptográficos

ARTÍCULO 77. El uso de controles criptográficos dentro de las aplicaciones o sistemas se debe regir según el procedimiento o técnicas evaluadas y probadas por los responsables de Seguridad de la Información de la UPTOSCR.

Control de acceso a archivos encriptados

ARTÍCULO 78. Las claves que permitan el acceso a los archivos encriptados que contengan información "Estrictamente Confidencial" y "Confidencial" deben estar documentadas bajo la custodia del responsable del activo de Información y del responsable de seguridad de la información de la UPTOSCR.

Sección III. Seguridad de los Procesos de Desarrollo y Soporte

Control de cambios en desarrollo de aplicaciones

ARTÍCULO 79. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben crear procedimientos para la verificación técnica del cambio, revisar y probar las aplicaciones a fin de garantizar que no existan impactos en los procesos una vez implementados, validar que satisfagan las necesidades y reducir futuros riesgos.

Documentación de cambios en desarrollo de aplicaciones

ARTÍCULO 80. Los cambios deben ser documentados de manera clara para ser utilizados en caso de ser necesario en futuras actualizaciones, tomando en consideración los controles necesarios para evitar la fuga de información o instalación de códigos maliciosos dentro del código de los sistema de información.

Responsabilidad de cambio bajo Estándares de Calidad

ARTÍCULO 81. Los responsables de los sistemas deben garantizar que los desarrollos de nuevos sistemas cumplan con procedimientos técnicos que permitan la integración con la plataforma, priorizando en técnicas de seguridad en el desarrollo y dando cumplimiento a los estándares de calidad en el desarrollo de software.

Sección IV. Seguridad Base de los Sistemas Operativos

Seguridad de los archivos del sistema

ARTÍCULO 82. El manejo seguro de los archivos del sistema, debe estar enmarcado bajo las recomendaciones y procedimientos definidos por los responsables de Seguridad de la Información de la UPTOSCR, para brindar protección y reducir los riesgos en los archivos del sistema.

CAPÍTULO VII. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Sección I. Plan de Continuidad

ARTÍCULO 83. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben conjuntamente con los responsables de Seguridad de la Información de la UPTOSCR, asegurar la certificación, el desarrollo, mantenimiento y prueba de los Planes de Contingencia, Prevención y Atención de Desastres.

Efectividad de los planes de atención de eventualidad

ARTÍCULO 84. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben realizar periódicamente la actualización de los Planes de Contingencia, de Prevención y Atención de Desastres, que atiendan los riesgos a los que están expuestos, de acuerdo a su probabilidad e impacto.

Actualización de planes para el manejo de eventualidades

ARTÍCULO 85. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben documentar los Planes de Contingencia, de Prevención y Atención de Desastres, acorde a la estrategia, los objetivos y las prioridades del servicio académico y de investigación.

Documentación de planes para el manejo de eventualidades

ARTÍCULO 86. El responsable de Oficina de Tecnologías de Información y Comunicación (OTIC) conjuntamente con la máxima autoridad de la Institución, debe activar el restablecimiento de las operaciones, de acuerdo a las necesidades y prioridades del sector, para asegurar la continuidad de los procesos universitarios.

Activación de los planes para la continuidad de las operaciones

ARTÍCULO 87. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben conjuntamente con los responsables de Seguridad de la Información de la UPTOSCR, en caso de la ocurrencia de eventos que afecten la continuidad de las operaciones, enfocar la planificación del restablecimiento de los servicios prioritarios, en un período de tiempo razonable, tomando en cuenta los recursos afectados (humanos, equipos y ambiente).

Manejo de eventualidades para la continuidad de las operaciones

ARTÍCULO 88. Los responsables de los procesos informáticos de la Institución, deben tener actualizado los planes de continuidad operacional asegurándose de planificar las pruebas del plan, considerando distintos escenarios, y asignado como prioridad las personas, instalaciones y procesos. Estas pruebas se deben llevar a cabo en horarios que no interrumpan las actividades.

Efectividad de los planes para la continuidad de las operaciones

Sección II. Recuperación de las Operaciones

ARTÍCULO 89. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben contar con un plan de ensayos (Pruebas / Simulacros) debidamente documentados y ejecutados que garanticen la continuidad de las operaciones.

Pruebas y simulacros para la recuperación de las operaciones

ARTÍCULO 90. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben verificar y probar los procedimientos de restauración al menos una vez al año, para garantizar su eficacia y cumplimiento dentro del tiempo asignado a su recuperación.

Tiempo de recuperación ante eventualidades



Redundancia en los sistemas de la UPTOSCR

ARTÍCULO 91. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, que soporten sistemas para las operaciones de la Institución, deben garantizar la redundancia de los sistemas, de acuerdo al nivel estratégico establecido por la Institución.

Mantenimiento de la plataforma tecnológica de la UPTOSCR

ARTÍCULO 92. Todo mantenimiento preventivo y correctivo de los equipos que soportan las plataformas tecnológicas de la Institución, debe ser realizado considerando las normas del fabricante, períodos de mantenimiento, fallas y mejoras debidamente documentadas.

CAPÍTULO VIII. SEGURIDAD FÍSICA Y AMBIENTAL

Sección I. Centro de Almacenamiento y Procesamiento de Datos (CAPD)

Seguridad en la administración de los datos de la UPTOSCR

ARTÍCULO 93. Los responsables de la administración de los Centros de Almacenamiento y Procesamiento de Datos (CAPD), deben velar por la integridad, confiabilidad y disponibilidad de los datos e información contenido en los equipos tecnológicos ubicados en estos centros.

Efectividad del Sistema Contra Incendio

ARTÍCULO 94. Los responsables de la administración de los CAPD, deben solicitar periódicamente al área correspondiente la verificación del mantenimiento efectivo de los equipos de protección contra incendios.

Efectividad del Sistema de Alimentación de Energía

ARTÍCULO 95. Los responsables de la administración de los CAPD, deben solicitar periódicamente al área correspondiente la verificación del mantenimiento efectivo y resguardo de los equipos de alimentación como UPS, generadores diésel, tableros de distribución de energía y baterías, plantas, para velar por el funcionamiento correcto de la ejecución de los mismos.

Efectividad de los Servicios Auxiliares

ARTÍCULO 96. Los responsables de la administración de los CAPD, deben solicitar periódicamente al área correspondiente la verificación del mantenimiento efectivo de la infraestructura de telecomunicaciones que contemple los sistemas de puesta a tierra, aires acondicionados, iluminación y buen estado de limpieza de estos.

Estructuración del cableado de la red de dato

ARTÍCULO 97. Los responsables de la administración de los CAPD, deben mantener el cableado de red de forma estructurada y llevar un inventario de los equipos por las áreas responsables conectados en sus diferentes dispositivos de red, con la finalidad de mantener identificada la plataforma tecnológica.

Seguridad en los CAPD

ARTÍCULO 98. Los responsables de Seguridad de la Información de la UPTOSCR, deben realizar evaluaciones de seguridad a los CAPD, con la finalidad de detectar posibles amenazas y vulnerabilidades en los activos de información, así como generar un cronograma de reducción de riesgos.

Almacenamiento y procesamiento de datos por terceros

ARTÍCULO 99. Todo equipo destinado al procesamiento de la información fuera de las instalaciones de la UPTOSCR, debe estar autorizado a través de un medio formal, por el propietario de la información en conjunto con los responsables de la plataforma tecnológica y avalado por los responsables de los Bienes de la institución. La persona autorizada signataria al uso de este equipo es responsable de la seguridad y resguardo de la información que este contenga.



Sección II. Seguridad de los Equipos

Correctivos y actualizaciones de los equipos

ARTÍCULO 100. Los responsables de la administración de la plataforma tecnológica de la UPTOSCR, deben aplicar periódicamente los correctivos y/o actualizaciones de seguridad de los equipos.

Conexión de equipos tecnológicos ajenos a la institución

ARTÍCULO 101. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben estar autorizados por el responsable de la Dirección de Oficina de Tecnologías de Información y Comunicación (OTIC), para la conexión de equipos tecnológicos a la red de datos, ajenos a la institución.

Gestión de información dentro de la red de datos de la UPTOSCR

ARTÍCULO 102. Toda información que se almacene, ejecute o transfiera a través de los equipos de computación de la UPTOSCR, será considerada como un activo de información, y por tanto, se debe monitorear y/o auditar.

Uso adecuado de los equipos tecnológicos de la UPTOSCR

ARTÍCULO 103. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben utilizar los equipos tecnológicos de oficina, para uso exclusivo de la Institución.

Prohibición de instalación de programas

ARTÍCULO 104. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, tienen prohibido instalar o copiar programas no autorizados, de acuerdo a los lineamientos establecidos por el responsable de la administración de los servicios informáticos y telemáticos.

Uso adecuado de los equipos que procesan información

ARTÍCULO 105. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben ser responsables del equipo y de la información que generen y almacenen en el mismo.

Seguridad, Higiene y Ambiente de los equipos tecnológicos

ARTÍCULO 106. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben mantener los equipos de computación de oficina en instalaciones y condiciones adecuadas, además de dar cumplimiento a los lineamientos de seguridad, higiene y ambiente de la Institución, según las normas emanadas por la Dependencia de Seguridad Laboral de la Universidad.

Manejo de incidente de equipos tecnológicos

ARTÍCULO 107. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, que detecten que se está presentando un incidente que atente contra la integridad y seguridad de su equipo de computación de oficina y de la información contenida en él, deben notificarlo a los responsables de Seguridad de la Información de la UPTOSCR, para que inicie la investigación y tome las medidas necesarias de respuesta al incidente por escrito mediante los medios disponible de la universidad.

Sobre la movilización de Equipos

ARTÍCULO 108. Todas las trabajadoras y trabajadores de la UPTOSCR, Núcleos y demás personas que intervengan en la prestación de servicio académico, deben garantizar el uso adecuado de los equipos informáticos lo que deriva en no permitir el traslado de un equipo sin antes haber sido notificado a los responsables de Seguridad de la Información de la UPTOSCR, para que inicien el protocolo de traslado una vez evaluada la necesidad.



CAPÍTULO IX. CÓDIGO DE ÉTICA PARA EL DESARROLLO Y APLICACIÓN RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL EN UPTOS

Sección I. Principios Generales

ARTÍCULO 109. El presente Capítulo tiene por objeto establecer los principios éticos y lineamientos para el desarrollo, implementación y uso responsable de sistemas basados en Inteligencia Artificial (IA) en todos los procesos de gestión de tecnologías de información y comunicación de la UPTOS CR, sus Núcleos y Extensiones, en concordancia con la Constitución de la República Bolivariana de Venezuela, la Ley Orgánica de Ciencia, Tecnología e Innovación, y los estándares internacionales en materia de ética de IA.

ARTÍCULO 110. Los principios rectores para el uso de IA en la institución son:

- Transparencia:** Todo sistema de IA debe ser identificable como tal, y sus decisiones deben ser trazables y explicables en la medida de lo posible.
- Justicia y no discriminación:** Se prohíbe el uso de IA que perpetúe sesgos, discrimine por razones de origen, género, edad, creencias, discapacidad o cualquier otra forma de exclusión social.
- Responsabilidad:** Los desarrolladores, custodios y usuarios de IA serán responsables del comportamiento del sistema, debiendo existir supervisión humana en decisiones críticas.
- Privacidad y protección de datos:** Todo sistema de IA deberá respetar la clasificación de activos de información establecida en el Capítulo II de la presente normativa, especialmente los niveles "Estrictamente Confidencial" y "Confidencial".
- Seguridad y robustez:** Los sistemas de IA deberán ser resilientes ante ataques, manipulación o fallos, garantizando la integridad, disponibilidad y confidencialidad de la información institucional.

Sección II. Desarrollo y Adquisición de Sistemas con IA

ARTÍCULO 111. Toda adquisición, desarrollo o modificación de sistemas que incorporen algoritmos de IA deberá cumplir con los estándares de Software Libre establecidos en el Artículo 73, salvo que la naturaleza del modelo requiera justificadamente otra licencia, previa autorización expresa de la Oficina de Tecnologías de Información y Comunicación (OTIC).

ARTÍCULO 112. Previo a la implementación de cualquier solución con IA, se deberá realizar una evaluación de impacto ético y algorítmico, documentando:

- El propósito del sistema y sus posibles sesgos.
- El tipo de datos utilizados para entrenamiento y operación, asegurando su legitimidad y calidad.
- Las medidas para evitar decisiones automatizadas que afecten derechos fundamentales de trabajadores, estudiantes o terceros.
- Los mecanismos de supervisión humana y reversibilidad de decisiones automatizadas.

ARTÍCULO 113. Queda prohibido el uso de sistemas de IA para:

- Vigilancia masiva no autorizada de personal, estudiantes o visitantes.
- Evaluación automatizada de desempeño laboral sin supervisión humana y sin acceso a mecanismos de impugnación.
- Toma de decisiones disciplinarias o académicas definitivas basadas exclusivamente en procesamiento automatizado.
- Reconocimiento biométrico sin consentimiento informado y sin cumplir con la Ley de Infogobierno y demás normativas aplicables.



Sección III. Operación y Gobernanza de la IA

ARTÍCULO 114. La Oficina de Tecnologías de Información y Comunicación (OTIC), será la responsable de mantener actualizado un Registro de Sistemas con IA en operación dentro de la institución, indicando su finalidad, alcance, nivel de autonomía y medidas de control implementadas.

ARTÍCULO 115. Todo incidente relacionado con sesgos, decisiones erróneas, violación de privacidad o vulnerabilidades de seguridad en sistemas de IA deberá ser reportado conforme al Artículo 38 (Reporte de Incidentes) y será tratado con prioridad por los responsables de Seguridad de la Información.

ARTÍCULO 116. Periódicamente, y al menos una vez al año, se realizarán auditorías ético-técnicas a los sistemas de IA, verificando el cumplimiento de los principios de este capítulo, la ausencia de sesgos discriminadores y la correcta protección de los activos de información.

Sección IV. Capacitación y Difusión

ARTÍCULO 117. La UPTOS CR promoverá programas de formación y sensibilización dirigidos a todas las trabajadoras, trabajadores y colaboradores sobre:

- a) Principios éticos de la IA.
- b) Riesgos asociados al uso no responsable de algoritmos automatizados.
- c) Procedimientos para reportar incidentes éticos en sistemas de IA.

ARTÍCULO 118. El incumplimiento de lo dispuesto en este Capítulo será considerado falta grave, y dará lugar a las sanciones previstas en el régimen disciplinario aplicable, sin perjuicio de las responsabilidades civiles, administrativas o penales a que hubiere lugar según la ley venezolana, en particular la Ley Especial contra Delitos Informáticos.

CAPÍTULO X. GLOSARIO Y SIGLAS

Sección I. Glosario

ACTIVO DE INFORMACIÓN: Información en cualquiera de sus formas y modalidades: impresa, manuscrita, oral, electrónica o digital y visual que de conformidad con sus intereses, la UPTOSCR y sus Núcleos, le atribuye un valor determinado, en función de la trascendencia, criticidad y sensibilidad.

ALTO IMPACTO: Todo cambio que afecte la disponibilidad de la Plataforma Tecnológica.

AMENAZA: Elemento con el cual se puede hacer un mal a cierto sistema o parte del mismo.

BOMBAS DE CORREO: Código malicioso que puede provocar la paralización o daños en un sistema tecnológico.

CRITICIDAD: Se entiende por criticidad el nivel de impacto que se puede generar debido a la paralización total o parcial de un proceso en la Plataforma Tecnológica y los Servicios Informáticos.

CENTRO DE ALMACENAMIENTO Y PROCESAMIENTO DE DATOS (CAPD): Área donde se almacenan y procesan datos e información de forma sistematizada, a través de un conjunto de hardware y software interconectados en red.

CLASIFICACIÓN: Son las diferentes categorías que se le asignan a un Activo de Información de acuerdo a

su contenido estratégico, valor e importancia para la continuidad de los procesos universitarios y que tiene la finalidad de determinar el grado de protección requerida.

CÓDIGO MALICIOSO: Programa que se ejecuta en una o varias computadoras, para robar información, eliminar archivos o formatear discos duros, mostrar publicidad invasiva, entre otros.

CONFIDENCIALIDAD: Es la forma de mantener la discreción de la información en cualquiera de sus formas (impresa, manuscrita, oral, electrónica o digital y visual) para asegurar que solo los individuos autorizados tengan acceso.

CONMUTADORES: Dispositivo electrónico que permiten la interconexión de redes de computadoras.

CONTRASEÑAS Y/O CLAVES DE ACCESO: Secuencia alfabética, numérica o combinación de ambas, protegidas por reglas de confidencialidad, utilizadas para verificar la autenticidad de la autorización, expedida a un usuario, para acceder a la data o la información contenida en un sistema.

CONTROL: Mecanismo de seguridad utilizado para guiar la operación de una máquina, aparato, sistema o proceso.

CUSTODIO DEL ACTIVO DE INFORMACIÓN: Persona natural autorizada, que tiene bajo su responsabilidad resguardar con diligencia los Activos de Información, delegados por el Propietario de los Activos de Información de la UPTOSCR y cada uno de sus núcleos. Para efecto de esta Política, le corresponde a los responsables de cada área de gestión.

DAÑO: Delito causado de manera deliberada o involuntaria a los Activos de Información propiedad de la UPTOSCR y de cada Núcleo, que, sin ocasionar paralización de procesos medulares sobre la Plataforma Tecnológica, afectan la imagen institucional.

DAÑOS GRAVES: Acciones que causan la paralización de las operaciones medulares, de los procesos administrativos, académicos y de investigación que incurra en pérdidas financieras o de otra índole.

DATO: Es la unidad mínima que compone una información, la cual representa un atributo a través de una representación simbólica.

DESTRUCCIÓN: Proceso que procura la eliminación de Activos de Información cuando deja de generar valor para la Institución, el cual debe ser autorizado únicamente por el custodio de dichos activos de información.

DISPONIBILIDAD: Es la condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

DOCUMENTO DE IDENTIFICACIÓN DE ACTIVOS: Documento que texto donde se clasifican por categorías todos los documentos que se administran en la plataforma tecnológica de la institución.

ENTIDAD: persona, aplicación o máquina.

ESTRICTAMENTE CONFIDENCIAL: Activo de Información valioso, relacionado con la dirección operacional o estratégica, cuyo conocimiento, divulgación o modificación por parte de personas no



Gobierno Bolivariano
de Venezuela

Ministerio del poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russián"



autorizadas causen graves daños al sistema universitario.

EQUIPOS: Estaciones de trabajo, servidores, portátiles u otros equipos de almacenamiento de información.

EVENTOS: Situación que ocasiona graves consecuencias a la Institución, de índole humano, operacional y económico.

FALLA: defecto que afecta la correcta operación del sistema.

GUSANO: Un gusano informático es un código malicioso que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

HARDWARE: son todos aquellos dispositivos y componentes físicos, que realizan las tareas de entrada y salida de un sistema informático.

INCIDENTE: Situación anormal que genera un alerta en un sistema y que puede convertirse en un ataque.

INFORMACIÓN: Conjunto de datos organizados que poseen valor para la Institución.

INFORMACIÓN ELECTRÓNICA: Toda información en digital, documentos, archivos de videos, audio, presentaciones.

INFORMACIÓN IMPRESA: Toda información presentada de forma física. **INTEGRIDAD:** Atributo que garantiza que la información recibida sea exactamente igual a la información transmitida, es decir, que no haya sido dañada o alterada en forma accidental o intencional.

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN: Es aquella que se hace a través del rotulado de un escrito o documento, con el cual se indica la figura geométrica y la clasificación del Activo de Información, acompañada de otros datos tales como: la unidad organizativa custodia.

IDENTIFICADOR ELECTRÓNICO: Es el código único alfanumérico que identifica al usuario para el acceso a la plataforma tecnológica.

MONITORIZADO: Es la acción de vigilar continuamente un proceso con el fin de recabar la información a controlar.

INSTITUCIÓN: Universidad Politécnica Territorial del Oeste de Sucre "Clodosbaldo Russián"

PLAN ANUAL DE CONTROL: Plan elaborado una vez al año por la oficina de Oficina de Tecnologías de Información y Comunicación (OTIC), dicho plan contiene los días y las unidades organizativas a inspeccionar, a fin de velar por el cumplimiento de la normativa legal vigente.

PLATAFORMA TECNOLÓGICA: Conjunto de equipos y medios utilizados para procesar, almacenar y transmitir datos e información.

PROPIETARIO DE LOS ACTIVOS DE INFORMACIÓN: Toda unidad o dependencia adscrita a la institución a quien se le atribuye la generación, clasificación y transmisión de la información en cualquiera de sus



Gobierno Bolivariano
de Venezuela

Ministerio del poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodomiro Russián"



formas. Para efecto de ésta Política, le corresponde al máximo responsable, jefe o coordinador de área.

RIESGO: Combinación de la probabilidad de la ocurrencia de un evento y sus consecuencias.

SERVICIO DE AUTENTICACIÓN O AUTENTIFICACIÓN: Garantizar que una entidad comunicante (una persona o máquina) es quien dice ser.

SERVICIO DE CONTROL DE ACCESO: Evitar el uso no autorizado de los recursos de la red, las aplicaciones, bases de datos y hardware de los sistemas informáticos. Delimita el alcance de la información permitida para cumplir con el objetivo de su unidad.

SERVICIO CRÍTICO: Es todo servicio que afecte directa o indirectamente al buen funcionamiento de la Institución (misión y visión) y maneje información "Estrictamente Confidencial", "Confidencial" y/o de "Uso Interno".

SERVICIO DE NO REPUDIO: Evitar que alguno de los participantes en la comunicación niegue (repudie) haber formado parte de ella. Es la imposibilidad de negar la autoría de un mensaje o información del que alguien es autor.

SERVIDOR: Computador que provee servicios, a una serie de computadores denominadas clientes.

SISTEMA OPERATIVO: Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.

SOFTWARE: es todo equipamiento lógico de un sistema informático.

SOFTWARE LIBRE: Programa de computación cuya licencia garantiza al usuario el acceso al código fuente y lo autoriza a ejecutarlo con cualquier propósito; modificarlo y redistribuirlo con sus modificaciones, en las mismas condiciones de licenciamiento acordadas en el programa original.

SPAM: Correo basura o no solicitado, habitualmente de tipo publicitario enviados en cantidades masivas que pueden perjudicar al receptor.

TRATAMIENTO DE LOS ACTIVOS DE INFORMACIÓN: Es la forma adecuada bajo la cual se debe almacenar, manejar y destruir la información, con la finalidad de garantizar su confidencialidad, integridad y disponibilidad.

UNIDAD RESPONSABLE DE LA PLATAFORMA TECNOLÓGICA: Áreas encargadas de administrar y gestionar la plataforma tecnológica.

UNIDAD RESPONSABLE DE LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN: Área encargada de la Seguridad de la Información de la UPTOSCR y de cada dependencia adscrita, que debe velar por la implantación de medidas de seguridad que permitan regular lo concerniente a la creación, administración, modificación, manipulación, destrucción y protección de los activos de información.

USUARIO: Todas las trabajadoras y trabajadores de la UPTOSCR, y sus unidades adscritas así como invitados y/o estudiantes que están autorizados al acceso de la plataforma tecnológica.



Gobierno Bolivariano
de Venezuela

Ministerio del Poder Popular
para Educación Universitaria

Universidad Politécnica Territorial del
Oeste de Sucre "Clodosbaldo Russián"



VIRUS: Es un código malicioso que tiene por objeto alterar el normal funcionamiento del computador, sin el permiso o el conocimiento del usuario.

Sección II. Siglas

MPPEUCT: Ministerio del Poder Popular para la Educación Universitaria Ciencia y Tecnología.

UPTOSCR: Universidad Politécnica Territorial del Oeste del Estado Sucre "Clodosbaldo Russián".

OTIC: Oficina de Tecnologías de Información y Comunicación (OTIC) de la UPTOSCR.

SUSCERTE: Superintendencia de Servicios de Certificación Electrónica.

CAPD: Centros de Almacenamiento y Procesamiento de Datos.

IA: Inteligencia Artificial.

Comuníquese y Publíquese,
En la Ciudad de Cumaná, a los xx días del mes de xx del año 2026.

Prof. Enry Gustavo Gómez Maiz

**PRESIDENTE CONSEJO UNIVERSITARIO
UPTOS "CLODOSBALDO RUSSIAN"**

Designado según Gaceta Oficial Nº 39.911 de
fecha viernes 27 de abril de 2012

Prof. Jesús Alejandro Blanco Méndez

**SECRETARIO CONSEJO UNIVERSITARIO
UPTOS "CLODOSBALDO RUSSIAN"**

Designado según Resolución Nº 58, publicado en
Gaceta Oficial Nº 41.932 de fecha 30 de julio de
2020 y según Aviso Oficial, publicado en Gaceta