universidad **central** del este

Res. No. 32/2020

DEL CONSEJO SUPERIOR UNIVERSITARIO

- Que la UCE, por la naturaleza relativa a los procesos atinentes a sus misiones de docencia, investigación, vinculación y responsabilidad social maneja y gestiona información sensible a dichos procesos como textos, cantidades, audiovisuales, diagramas, entre otras formas de información que se expresan en términos digitales o físicos.
- Que la gestión de la información institucional incluye unidades técnicas interdependientes coherentemente organizadas para la recopilación, procesamiento y difusión de información, a través de procedimientos manuales, parcial y completamente electrónicos.
- Que la UCE dispone de informaciones sensibles de estudiantes, profesores, tutores, funcionarios y colaboradores externos que no pueden suministrarse a personas o entidades extrañas por lo que la institución tiene establecidas políticas de seguridad de los sistemas informáticos de recopilación, mantenimiento y gestión de información para asegurar que la misma sea utilizada por las personas o entidades legítima y legalmente autorizadas.
- Que la UCE ha establecido una Política de Seguridad de la Información con el deliberado propósito de minimizar las amenazas y debilidades relativas a la infraestructura física y tecnológica de almacenamiento y uso de la misma.
- Que estas políticas del Departamento de Tecnología de la Información y de la Comunicación abarcan la recopilación, procesamiento y difusión de la información como los canales digitales para impedir la ocurrencia de eventos extraños de origen interno o externo que afecten la operatividad de las unidades de gestión tecnológica de la información.

VISTOS: a) La Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología,

b) El Código de Conducta en Ambientes Virtuales de la UCE, y

c) El Manual de Procedimientos del Departamento TIC de la UCE.

ACOGIDO: Los documentos, elaborados por un equipo Técnico liderado por el Director del Departamento de Tecnología de la Información y de la Comunicación de la UCE, que contienen las Propuestas de las Políticas de esa importante Unidad.

ACEPTADAS: Las opiniones y sugerencias de los señores miembros del Honorable Consejo Superior Universitario sobre esta propuesta.

En virtud de las atribuciones que otorgan los Estatuto de la UCE a este Consejo Superior Universitario,

RESUELVE

1. Aprobar, como al efecto aprueba, la documentación que se adjunta a la presente Resolución que contienen las Políticas que rigen para el Departamento de Tecnología de la Información y de la Comunicación y que incluyen, además, la Descripción del Funcionamiento de Sistema de Información de la Universidad Central del Este.

-sigue al dorso-

Ave. Francisco A. Caamaño Deñó, San Pedro de Macorís, Rep. Dom.
E-Mail: info@uce.edu.do
Tel.: 809-529-3562
RNC: 411001202

2. Ordenar, como al efecto ordena, a los funcionarios, unidades académicas o administrativas responsables de producir, recopilar y gestionar información, ajustar sus procesos de gestión a lo establecido en las presentes políticas de manejo y de seguridad de la Información.
3. Ordenar, como al efecto ordena, al director del Departamento TIC de la UCE, socializar entre las Vicerrectorías y sus dependencias el contenido, importancia y alcance de estas políticas
4. Derogar, como al efecto deroga, toda norma o disposición, que se oponga al espíritu y contenido de la Política aprobada por esta Resolución.
5. Notificar a las unidades académicas y administrativas pertinentes para los fines correspondientes.

Infórmese a la Comunidad UCEANA.

Dada en San Pedro de Macorís, República Dominicana, a los dieciséis (16) días del mes de diciembre del año 2020

Dr. José E. Hazim Frappier
Presidente del Consejo Superior Universitario

Lic. Vilma Kamel Hazim Torres
Secretaria del Consejo Superior Universitario.

JEHF/VKHT
ibm

DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y TELECOMUNICACIONES

DESCRIPCIÓN DEL FUNCIONAMIENTO DEL SISTEMA DE INFORMACIÓN UCE

Preparado por:	Revisado por:	Aprobado por:

CONTROL DE VERSIONES			
Versión	Revision	Modificado por	Revisado por
1.0	12/03/2020	Leandro de la Rosa	Leandro de la Rosa

ÍNDICE DE CONTENIDO

INTRODUCCION

El presente documento describe el funcionamiento del Sistema de Información de la Universidad Central del Este, el modo en cómo este apoya a las labores administrativas y académicas de la institución. Explica la forma en cómo se integran las diferentes soluciones que componen dicho sistema y finalmente nos dará una descripción de la forma en cómo este se mantiene en operación dia a dia.

DEPARTAMENTO DE TIC

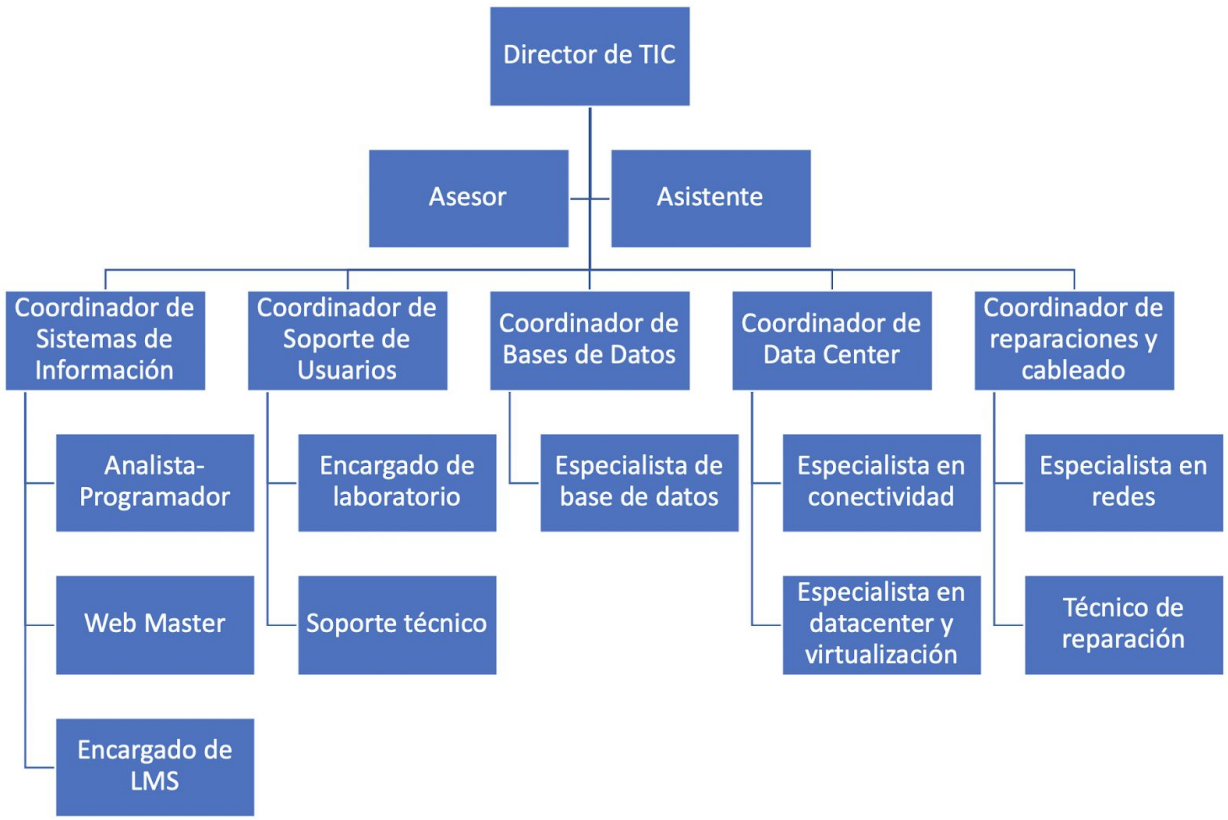
El departamento de TIC es el encargado de planear, desarrollar, implementar y mantener todos los servicios de tecnología de la información que contribuya a la transformación de los procesos institucionales de administración, académica, investigación, extensión y vinculación con entrega de valor para la UCE.

Algunos de nuestros valores son:

- Honestidad
- Respeto
- Puntualidad
- Responsabilidad
- Proactividad
- Trabajo en equipo
- Integridad

La universidad cuenta con equipo de ingenieros bien preparados y certificados en su mayoría, que brinda apoyo tecnológico a cada una de las necesidades de nuestra institución. El departamento de TIC está subdividido en 5 áreas administradas por coordinadores que atienden de manera eficiente a cada uno de los asuntos relacionados con su área de acción.

Organigrama



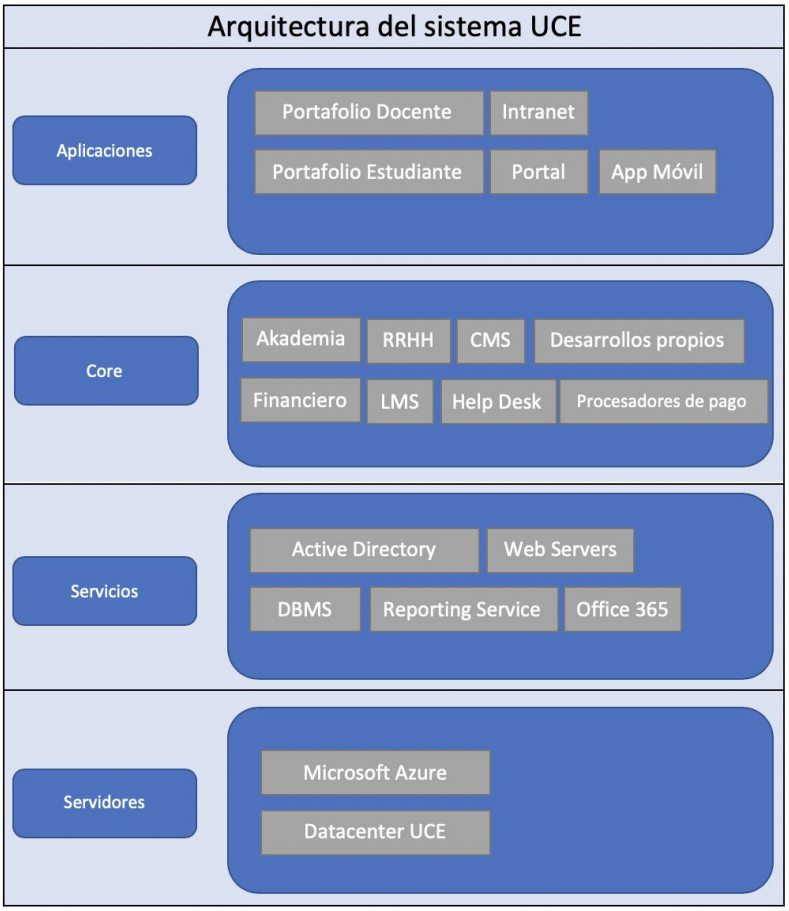
Descripción del sistema de información de la UCE

El sistema de información de la UCE, está desarrollado para brindar un soporte eficiente a toda la comunidad UCEANA sin importar el lugar donde se encuentre, las 24 horas del día los 7 días de la semana.

Está fundamentado sobre los mejores estándares de la industria de tecnologías web que brinda asistencia a las funciones sustantivas de la universidad:

- Academia
- Investigación
- Extensión

A continuación mostraremos un gráfico que muestra la arquitectura del Sistema de la UCE:



Como muestra el gráfico anterior nuestra plataforma tecnológica reside en la nube apoyándose de los servidores de Microsoft Azure y servidores en nuestro datacenter local.

Algunos de los servicios que utilizamos son:

Active Directory: Utilizamos este servicio para gestionar la autenticación y autorización de todas nuestras aplicaciones utilizando los grupos de permisos para mantener una gestión centralizada y eficiente.

Web Servers: Algunas de nuestras aplicaciones utilizan servidores webs de Linux (Apache) y Windows (IIS) para servir al público nuestras aplicaciones webs.

DBMS: DataBase Management System, nuestras aplicaciones utilizan diferentes manejadores de bases de datos entre los que se encuentran Microsoft SQL Server, MySQL y PosgreSQL.

Reporting Service: Es un producto de Microsoft utilizado para crear reportes que pueden ser consumidos desde aplicaciones Webs.

Office 365: Es utilizado en nuestra arquitectura para enviar mensajes de correo electrónico, crear tareas, agendar citas y eventos, crear videoconferencias, etc. Más adelante vamos a estar hablando en detalle de este producto.

A continuación vamos a dar una breve descripción de las principales aplicaciones y herramientas que utilizamos en la UCE:

El Portal Web

El portal web de la UCE es un sitio web que ofrece a los usuarios una forma fácil e integrada de acceder a los recursos y servicios que ofrece nuestra institución. Incluye: Enlaces webs, buscadores, documentos, aplicaciones, compra electrónica de servicios, entre otros.

Este se divide en varias secciones o subsitios que agrupa en un solo lugar toda la información necesaria para un ámbito en específico.

Intranet

La intranet es un subsitio del portal privado que agrupa todas las aplicaciones y reportes que nuestros usuarios internos utilizan para la toma de decisiones y realizar las operaciones propias de su labor. En este lugar los usuarios pueden acceder solamente a los lugares que tienen autorizados según el rol que ocupa dentro de la institución.

La intranet está dividida en 4 partes principales:

- Reportes: Aquí se agrupan todos los reportes que apoyan a la toma de decisiones oportunas de nuestros usuarios. Aquí podemos encontrar reportes relacionados con estudiantes, selecciones, horarios, estadísticas en general, informaciones financieras, etc.

- Aplicaciones: Aquí se encuentra el acceso directo a todas las aplicaciones que utilizan nuestros usuarios para fines académicos, administrativos y financieros.

- Documentos: Es un lugar centralizado donde se encuentran todos los documentos importantes de nuestra institución tales como: Manuales de usuario, reglamentos académicos, guías, manuales técnicos, etc.

- Departamentos: Es un lugar que contiene los enlaces a los Sub-Sitios privados de cada departamento.

Portafolio de estudiantes

El portafolio de estudiante agrupa todas las operaciones que los estudiantes pueden realizar con el sistema de información de la UCE en un solo lugar de fácil acceso. Disponible de manera web en el portal y desde el celular con nuestra aplicación móvil.

Desde este lugar el estudiante puede:

- Seleccionar asignaturas
- Pagar en línea con tarjeta de crédito
- Ver reportes estudiantiles tales como: Record de notas, selecciones, inasistencias reportadas por los docentes, etc.
- Cambiar su contraseña.
- Acceder a las aulas virtuales de nuestro LMS.
- Acceder a su correo electrónico.
- Actualizar su teléfono, email, foto de perfil.
- Recibir notificaciones de la universidad.
- Ver documentos pendientes.
- Ver horario.
- Ver calificaciones.
- Ver estado de cuenta.
- Ver indice académico.
- Acceder a documentación como: Reglamentos académicos, Manuales académicos, calendarios, etc.
- Solicitar comprobantes fiscales.
- Realizar reclamaciones y sugerencias.
- Acceder a los catálogos de bibliotecas en línea.
- Acceder a productos externos disponibles.

Portafolio docente

El portafolio de docente agrupa todas las operaciones que los docentes pueden realizar con el sistema de información de la UCE en un solo lugar de fácil acceso. Disponible de manera web en el portal y desde el celular con nuestra aplicación móvil.

Desde este lugar el docente puede:

- Reportar calificaciones.
- Reportar inasistencias.
- Hacer su autoevaluación profesoral.
- Cambiar su contraseña.
- Ver notificaciones.

- Ingresar a las aulas virtuales de nuestro LMS.
- Ver su horario de clases.
- Ver los resultados de sus evaluaciones profesorales.
- Ingresar a su correo electrónico.
- Acceder a documentación como: Reglamentos académicos, Manuales académicos, calendarios, etc.
- Acceder a los catálogos de bibliotecas en línea.
- Acceder a productos externos disponibles.

Oferta académica

Este apartado muestra las ofertas disponibles de la UCE en las áreas de grado, posgrado, técnico superior y educación continuada. En este lugar se puede visualizar fácilmente todos los detalles de cada una de nuestras ofertas tales como: requisitos de admisión, pensum, costo, opciones de financiamiento, información de contacto, etc.

Admisiones

Este apartado está dedicado al departamento de admisiones de la UCE, aquí los estudiantes tienen disponible todas las herramientas necesarias para convertirse en UCEANOS.

En este lugar pueden:

- Ver requisitos.
- Solicitar información.
- Llenar formularios de admisión en línea.
- Ver información sobre los procesos de legalizaciones.
- Ver información de asistencia financiera para extranjeros

Investigación

Este apartado está dedicado a la Dirección de Gestión de Investigaciones Científicas (DGIC) de la UCE, aquí se compilan una serie de recursos que apoyan al investigador en asuntos tales como:

- Información general del departamento
- Promoción de la investigación
- Soporte al investigador
- Visibilidad de la investigación

Biblioteca

Este apartado está dedicado a la dirección de la biblioteca de la UCE, desde aquí nuestros usuarios pueden:

- Acceder a bases de datos en línea, tales como EBSCO, Access Medicine, Access Engineering, etc.
- Consultar el catálogo de nuestras bibliotecas en línea.
- Acceder a las principales bibliotecas virtuales nacionales e internacionales.
- Ver los reglamentos de la biblioteca.

Extensión

Este apartado recopila todas las actividades de extensión realizadas por la universidad. Desde aquí se pueden ver fotografías, videos y información detallada de cada una de estas actividades.

Akademia

Akademia es un software de gestión académica desarrollado por Innova Technology en Costa Rica para las universidades de República Dominicana. La UCE contrató los servicios de Innova Technology para la implementación de algunos módulos adaptados a las necesidades particulares de la UCE.

Hoy en día la UCE continúa con el mantenimiento y mejora continua de este sistema gracias a la preparación de nuestro personal técnico certificado. Entre los principales módulos que podemos mencionar de este sistema se encuentran:

- Admisiones
- Becas
- Punto de servicio
- Cuentas por cobrar de estudiantes
- Calificaciones
- Programación de horarios
- Información general de los estudiantes
- Convalidaciones
- Entre otros...

Moodle

Moodle es una herramienta de gestión de aprendizaje (LMS) de distribución libre escrita en el lenguaje de programación PHP. Está concebida para ayudar a los docentes para crear comunidades de aprendizaje en línea y es ampliamente utilizado por Universidades en todo el mundo.

Sistema financiero

Nómina y recursos humanos

La aplicación dedicada a la gestión de recursos humanos es un desarrollo propio a medida de la necesidades de la institución que cuenta con varios módulos, uno destinado a la gestión de personal o otro para las operaciones relacionada con la nómina y diferentes secciones de configuración.

Gestión de personal

Este módulo cuenta con la funcionalidades para el registro, actualización y consulta de los datos de los empleados. Cada empleado tiene un perfil donde se mantiene un registro de las incapacitaciones, vacaciones, documentos y los diferentes puestos con sus generalidades.

Nomina

El propósito de este módulo es servir a las operaciones de elaboración, cálculo y emisión de pago de la nómina. En este módulo es posible registrar las deducciones y percepciones de los empleados y aplicar incapacitaciones.

Configuracion

Este módulo es pensado para propósito de configuración de los elementos de referencia utilizados en los procesos de gestión de personal y nómina. Entres los confortables están incluidos:

- Departamentos y Subdepartamentos
- Cargos
- Conceptos (Percepciones y Deducciones)
- Plantillas para documentos
- Configuraciones generales

Sistema de contabilidad

La UCE cuenta con un software de contabilidad desarrollado por Innova Technology, mejorado y mantenido por el equipo de Sistemas de información de TIC. En este se registran todas las operaciones financieras de la universidad.

Los módulos que se encuentran en este sistema son los siguientes:

- Catálogo de cuentas
- Bancos
- Activos fijos
- Cuenta por pagar
- Contabilidad general

Pago en línea

Es servicio ofrecidos a través de una aplicación integrada en Akademia que permite a los estudiantes realizar el pago de los servicios de naturaleza académica, principalmente la inscripción. Este módulo también permite realizar pagos de saldos pendientes generados en base a un plan de pagos. Los usuario pueden realizar sus pagos con tarjeta de debito o credito a traves de las pasarelas de pago de PayPal y CardNET.

Otros módulos y/o herramientas

Aplicación móvil IOS/Android

La aplicación móvil denomina UCE Mobile es una aplicación móvil multiplataforma desarrollada por la UCE para conectar con los usuarios los docentes y estudiantes ofreciendo facilidades de acceso a la informaciones y servicios de la institución.

La aplicación puede ser utilizada tanto por docente como estudiante. Para los docentes la aplicación ofrece acceso a horario de clases del periodo en cursos, registro de asistencia y registro de calificaciones mientras que los estudiantes tienen acceso a sus estado de cuenta, consulta de calificaciones, horario y retiro de asignaturas.

La aplicaciones es útil aún para aquellos que no tiene usuario registrado en nuestra plataforma pues ofrece una apartado de noticias, directorio telefónico, ubicación, preguntas frecuentes, oferta académica y vida estudiantil.

- **Noticias:** Ofrece acceso a las noticias más destacadas sobre la actividades realizadas por la institución.

- **Directorio telefónico:** Dá accesos las los números de contacto de la instituciones e los números de extensión de los diferentes departamentos de la institución.

- **Ubicación:** Muestra la ubicación de la intuición utilizando el servicio de Google Maps.

- **Preguntas frecuente:** Contiene un amplio catálogo de preguntas comunes sobre la oferta de las institución y los procesos de admisión.

- **Vida estudiantil:** Muestras las noticias más destacadas del ámbito estudiantil.

Sistema de evaluación profesoral

Para garantizar la calidad de la enseñanza a nuestros estudiantes de grado y posgrado, la UCE desarrolló un sistema de evaluación profesoral que permite a los estudiantes y directores académicos evaluar a los docentes.

Esta aplicación utilizando una serie de instrumentos permite medir los siguientes aspectos:

- Orientación inicial
- Proceso de aprendizaje
- Cumplimiento de las normas institucionales
- Relaciones humanas

Skype for Business

Skype for Business es una una aplicación de mensajería instantánea, llamadas de audio y videoconferencia. Internamente en la UCE lo utilizamos para establecer comunicación entre empleados, docentes estudiantes. También lo utilizamos para comunicarnos con personas externas a nuestra comunidad universitaria como partners, colaboradores, contratistas, personal de otras universidades y el público en general. Además Skype for Business tiene herramientas adicionales que permiten la interacción y asistencia remota. Entre las principales cosas que hacemos con Skype for Business están las siguientes:

- Iniciar conversaciones mediante mensajería instantánea, llamadas de voz y videollamadas.

- Ver cuándo nuestros contactos están disponibles en línea, en una reunión o en una presentación.
- Realizar difusiones en línea a un gran público.
- Presentar nuestras pantallas durante las reuniones o conceder el control a otros.

Microsoft Teams

Microsoft Teams está pautado a ser el sucesor de Skype for Business. Además de las funcionalidades de comunicación en línea que ofrece Skype for Business, Microsoft Teams integra opciones más avanzadas para la colaboración y trabajo en equipo de forma más eficiente.

En la UCE lo utilizamos para compartir archivos, trabajar simultáneamente documentos de texto, presentaciones, hojas de cálculo y otros. El cuerpo docente lo utiliza para potenciar las clases a distancia aprovechando la funcionalidad de pizarra y videoconferencias grupales.

Las características de Microsoft Teams permiten agilizar las tareas que competen a determinados grupos de colaboradores en la UCE, a partir de la comunicación instantánea y eficiente, la compartición de archivos y la integración tanto de las herramientas de la suite de Office, como de servicios de terceros. Entre sus características más relevantes están la productividad, comunicación efectiva, trabajo colaborativo, personalización y seguridad.

Office 365

Office 365 es una plataforma de productividad que integra una variedad de herramientas que permiten crear, acceder y compartir documentos. Además ofrece servicios de comunicación como correo electrónico, almacenamiento en la nube, gestión de calendarios, sitios web y otras funcionalidades. En la UCE lo utilizamos en todos los ámbitos de la comunidad universitaria para tener acceso al correo electrónico, mensajería instantánea, videoconferencias, pantallas compartidas, almacenamiento en la nube, calendarios y otras funcionalidades.

Plataforma tecnológica

Conectividad

La arquitectura de conectividad de la UCE está diseñada con tolerancia a fallos, permitiendo su función constante y correcta en caso de fallo de uno o varios de sus componentes. Estos incluyen:

- Dos proveedores de servicio de internet
- Dos Core Switches Cisco 4900 (Si el principal falle el Segundo asume la carga)
- Almacenamiento de backups de configuración de equipos (switches, routers, etc) en servidores físicos y la nube.

La red consiste mayormente en Switches Cisco de Capa 3 de diferentes modelos (según sus funciones respectivas). Tales funciones incluyen Switches de enlace de proveedores, de core y de distribución. Los switches Core y de distribución están conectados entre sí mayormente vía fibra óptica (10Gbps), mientras que los demás tienen conexión (por fibra) de 1Gbps.

Disponemos en un Router que hace la función de Enrutador de voz (telefonía), permitiendo los protocolos de Internet para la transmisión y recepción de comunicaciones de voz (VoIP).

Servidores

La mayor parte de los servidores de la institución están funcionando en el servicio de computación en la nube de Microsoft Azure, principalmente con la modalidad de infraestructura como servicio. Los servidores están configurados en balanceadores de carga y failovers para asegurar disponibilidad del servicio durante eventualidades inesperadas o fallos que se puedan presentar.

Tener los servidores en la nube nos permite asignarles recursos prácticamente ilimitados en los tiempos que hay mucha demanda de servicios en la universidad, como los días de selección o reajuste por ejemplo.

Además, cuando se presentan necesidades puntuales de nuevas herramientas y/o funcionalidades la modalidad de computación en la nube nos permite desplegar y configurar nuevos servidores en un corto tiempo.

También tenemos servidores físicos localmente, en los cuales virtualizamos otros servidores para alojar principalmente servicios y herramientas para consumo interno.

Equipos

En la institución hay equipos en todas las estaciones de trabajo que lo requieren. También tenemos computadoras portátiles que se asignan a empleados o equipos cuando necesitan desplazarse de su lugar de trabajo para realizar labores en otra ubicación.

La institución también dispone de equipos fijos o de escritorio en laboratorios de clases, como son computadoras y proyectores. Además, contamos con portátiles de alta capacidad que los técnicos de laboratorio movilizan a los lugares donde se presentan las necesidades.

Las computadoras fijas que están en los laboratorios de clases son Thin clients (clientes ligeros o terminales tontas). Esos equipos se conectan a los servidores que tenemos virtualizados en nuestros servidores locales para consumir todos los servicios de computación que ellos utilizan.

En esos servidores se gestiona de forma centralizada su sistema operativo, almacenamiento, memoria ram, procesador y demás características.

Bases de datos

La institución cuenta con base de datos para garantizar la disponibilidad de la información necesaria para para labores docentes, estudiantiles y administrativas. Se cuenta con varios sistemas gestores de base de datos siendo el principal Microsoft SQL Server y MySQL para algunas algunas aplicaciones de propósito específico.

Nuestra base de datos principal contiene la información de los los docentes, estudiante, horarios, calificaciones, cobro de servicios y procesos académicos en general. Esta base de datos sirve como fuente de información para varias de las aplicaciones de desarrollo propio, de la parte financiera y de RRHH.

El sistema financiero tiene su propia base de datos para las labores y procesos contables. La base de datos de Akademia sirve con fuente de información para la división de cuentas por cobrar del departamento financiero.

El sistema destinado a las labores de RRHH cuenta con sus propia base de datos. Este sistema integra información de Akademia para determinar los pagos de docencia y descuentos por inasistencia. La base de datos del sistema financiero sirve como fuente de consulta y depósito de la información generada por procesos que afectan la contabilidad como la emisión y pago de nómina.

Mantenimiento de equipos y actualizaciones

Mantenimiento de equipos

La universidad cuenta con un equipo de soporte técnico de respuesta rápida ante cualquier incidencia que presenten los equipos y se encarga de velar por el buen funcionamiento de la infraestructura física y de los programas instalados en los equipos.

Para realizar este trabajo contamos con herramientas de monitoreo en tiempo real del estado de los equipos que nos muestran asuntos tales como: Inventario, actualizaciones, capacidades, alertas, etc.

Como departamento de soporte contamos con herramientas para la reparación en caso de ser necesario de dichos equipos.

Actualizaciones de softwares propios

Para actualizar las soluciones de software propios utilizamos un procedimiento estándar. Cuando los programadores desarrollan actualizaciones y validan que están listas para publicar, el Coordinador de Sistemas envía al Coordinador de Conectividad y DataCenter las aplicaciones para ser instaladas en producción vía correo electrónico. Luego el Coordinador de Conectividad y Datacenter hace copias de seguridad de la versión que está en producción de las aplicaciones que se van a actualizar; después copia los nuevos archivos en los lugares que indicó el Coordinador de Sistemas en el correo electrónico. Finalmente responde vía correo al Coordinador de Sistemas que la actualización fue aplica.

Actualizaciones de software de terceros

Para la actualización de software de terceros utilizamos los procedimientos de actualización establecidos por los fabricantes correspondientes para cada uno de los productos de software procurando mantener siempre la última versión disponible estable.

Seguridad y privacidad

Seguridad física

Se establecieron controles para reducir los riesgos asociados a la seguridad de la información asociados al control de acceso físico a las instalaciones. Esos controles buscan evitar el acceso no autorizado, además establecer controles y auditorías, logrando el control total en los accesos en la Universidad Central del Este, los cuales exponen a la institución a

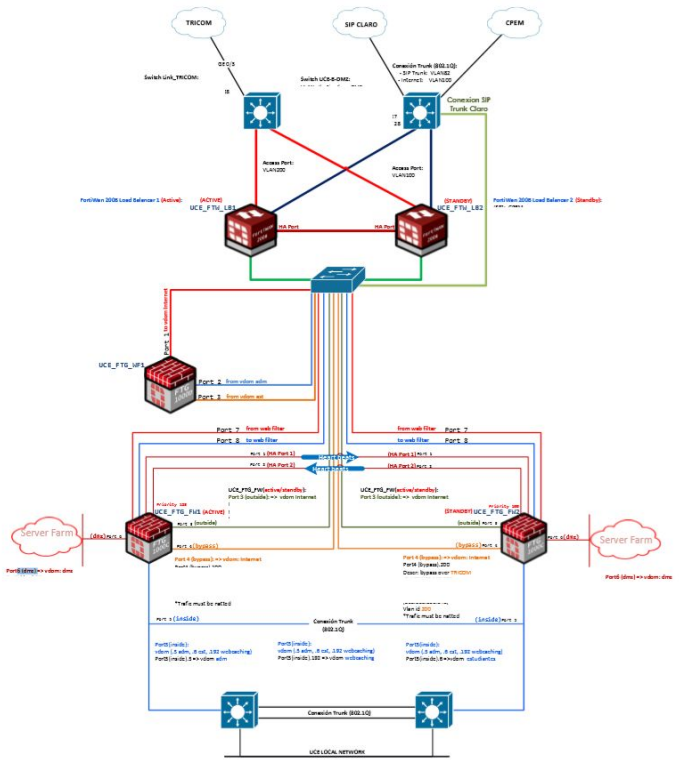
pérdidas de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

La política se aplica a todos los accesos restringidos que contenga la Universidad Central del Este, aplicando a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios a la Universidad Central del Este o que estén relacionados. Se incluye además, todas las dependencias que son parte de la institución o que transite por la red de la Universidad Central del Este.

Ésta política establece controles para reducir los riesgos asociados a la seguridad de la información asociados al control de acceso físico a las instalaciones.

Seguridad virtual

Para garantizar la seguridad virtual utilizamos equipos Firewall de última generación para el control de acceso a los dispositivos conectados a la red, tanto desde nuestra Intranet como desde Internet. También se ha establecido un sistema de control de acceso basado en Directorio Activo de Microsoft que permite limitar y monitorear el acceso a cada sistema y servicio virtual de la institución basándose en perfiles y roles.



Privacidad

El departamento de TIC se rige por las políticas que definen controles para proteger la privacidad de la información de la UCE y de todos los miembros de la comunidad universitaria (empleados, docentes y estudiantes). Esas políticas incluyen correos electrónicos en buzones institucionales, archivos almacenados en las plataformas de universidad y en dispositivos extraíbles que se conectan a computadoras del campus universitario.

Copias de seguridad

Para asegurar la restauración, persistencia y continuidad de las operaciones de la universidad en los casos en que se pierda parte o toda la información de la empresa realizamos copias de seguridad en lapsos de tiempo establecidos en nuestras políticas de respaldo de la información. La política se aplica a todos los activos de información de la Universidad Central del Este, sus empleados y demás empresas dependientes o relacionadas sin importar ubicación geográfica, información que maneje la UCE de empleados temporales de otras empresas o agencias, información de socios de negocios y contratistas.

Para esto utilizamos herramientas de software que automatizan el proceso y gestionan el almacenamiento seguro de los archivos de respaldo. Esas herramientas también restauran la información en caso de ser necesario.

PROPUESTAS DE POLITICAS DE SEGURIDAD DE LA INFORMACION
DEPARTAMENTO TIC UNIVERSIDAD CENTRAL DEL ESTE
Comité de Ciberseguridad TIC

ÍNDICE

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - PROPUESTA 2020
Universidad Central del Este
Departamento de tecnología de la información y comunicación
Comité de Ciberseguridad TIC

1. INTRODUCCIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la comunidad universitaria y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión de la Universidad.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, resulta necesaria la implementación de una Política de Seguridad de la Información que forme parte de la cultura organizacional de la Universidad, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

Como consecuencia de lo expuesto, la Universidad Central del Este se ha abocado a la tarea de implementar sus propias políticas de seguridad de la información, basándose en las características establecidas en el Modelo de Política de Seguridad de la Información.

Así mismo, con el propósito de que dicha implementación pueda realizarse en forma ordenada y gradual, la Universidad ha encomendado a su Comité de Ciberseguridad TIC, la tarea de elaborar y coordinar la ejecución de un Plan de Acción para el año en curso que fije objetivos y determine plazos de realización de los mismos.

2. TÉRMINOS Y DEFINICIONES

2.1. 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.

Adicionalmente, deberán considerarse los conceptos de:

• **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.

• **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

• **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.

• **No repudio**: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

• **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

• **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

2.2. 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.

2.3. 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.

2.4. Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Universidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.5. Comité de Ciberseguridad TIC: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivos:

a) Proteger los recursos de información de la Universidad y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

b) Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

c) Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

3.2. Sanciones Previstas por Incumplimiento: El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

4. ORGANIZACIÓN DE LA SEGURIDAD

Son sus objetivos:

a) Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

b) Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

c) Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Universidad.

4.1. Infraestructura de la Seguridad de la Información

4.1.1. Comité

de Ciberseguridad TIC: destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Responsabilidades:

1) Posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas para esta Universidad.
2) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de esta Universidad frente a posibles amenazas, sean internas o externas.
3) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de esta Universidad.
4) Aprobar las principales iniciativa para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
5) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de esta Universidad, sean prexistente o nuevos.
6) Promover la difusión y apoyo a la seguridad de la información dentro de la Universidad, como así, coordinar el proceso de administración de la continuidad de las actividades.

4.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información

El director del departamento TIC de la Universidad Central del Este deberá asigna las funciones relativas a la Seguridad Informática de la Universidad al **Ing. _____**, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática.

a) Control de Accesos
b) Seguridad en el Desarrollo y Mantenimiento de Sistemas
c) Planificación de la Continuidad Operativa

Así mismo, el Comité de Ciberseguridad TIC propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan, quienes serán los responsables de las unidades organizativas a cargo del manejo de la misma. Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

4.1.3. Proceso de Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Universidad.

4.1.4. Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la Universidad, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos.

4.1.5. Cooperación entre Organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con Organismos especializados en temas relativos a la seguridad informática.

4.1.6. Revisión Independiente de la Seguridad de la Información

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Ciberseguridad TIC realizará revisiones independientes sobre la vigencia e implementación de las Políticas de Seguridad de la Información, a efectos de garantizar que las prácticas de la Universidad reflejan adecuadamente sus disposiciones.

4.2. Seguridad Frente al Acceso por Parte de Terceros

4.2.1. Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Universidad, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

• El tipo de acceso requerido (físico/lógico y a qué recurso).
• Los motivos para los cuales se solicita el acceso.
• El valor de la información.
• Los controles empleados por la tercera parte.
• La incidencia de este acceso en la seguridad de la información del Organismo.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Universidad, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información de la Universidad.

b) Protección de los activos de la Universidad, incluyendo:

• Procedimientos para proteger los bienes de la Universidad, abarcando los activos físicos, la información y el software.
• Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.

• Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
• Restricciones a la copia y divulgación de información.
c) Descripción de los servicios disponibles.
d) Nivel de servicio esperado y niveles de servicio aceptables.
e) Permiso para la transferencia de personal cuando sea necesario.
f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
g) Existencia de Derechos de Propiedad Intelectual.
h) Definiciones relacionadas con la protección de datos.
i) Acuerdos de control de accesos que contemplen:
• Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
• Proceso de autorización de accesos y privilegios de usuarios.
• Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
o) Proceso claro y detallado de administración de cambios.
p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
r) Controles que garanticen la protección contra software malicioso.
s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
t) Relación entre proveedores y subcontratistas.

4.3. Tercerización

4.3.1. Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC de la Universidad, contemplarán además de los puntos especificados en (“Requerimientos de Seguridad en Contratos o Acuerdos con Terceros”, los siguientes aspectos:
a) Forma en que se cumplirán los requisitos legales aplicables.
b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.

c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Organismo.
d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Organismo.
e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.
g) Derecho a la auditoría por parte del Organismo sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc. Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

5. CLASIFICACIÓN Y CONTROL DE ACTIVOS

Son sus objetivos:
a) Garantizar que los activos de información reciban un apropiado nivel de protección.
b) Clasificar la información para señalar su sensibilidad y criticidad.
c) Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.
Esta Política se aplica a toda la información administrada en la Universidad, cualquiera sea el soporte en que se encuentre. Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.
El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan. Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

5.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.
El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.
El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

5.2. Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad:
a) confidencialidad,
b) integridad,
c) disponibilidad.

5.3. Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia;
- Almacenamiento;
- Transmisión por correo, fax, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

6. SEGURIDAD DEL PERSONAL

Son sus objetivos:

a) Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

b) Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

c) Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Universidad en el transcurso de sus tareas normales.

d) Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

e) Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la Universidad El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política..

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Ciberseguridad TIC, a los propietarios de la información.

El Comité de Ciberseguridad TIC será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Encargado, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las

sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Organismo es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

6.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

6.1.1. Incorporación de la Seguridad en los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo. Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de las Políticas de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

6.1.2. Control y Política del Personal

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto, alcanzan a la Universidad.

6.1.3. Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Universidad. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente. Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

6.1.4. Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

6.2. Capacitación del Usuario

6.2.1. Formación y Capacitación en Materia de Seguridad de la Información

Todos los empleados del Organismo y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Universidad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

6.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad

6.3.1. Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Encargado de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

6.3.2. Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

6.3.3. Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

c) Alertar inmediatamente al Responsable de Seguridad Informática o del Activo
de que se trate.

La recuperación será realizada por personal experimentado, adecuadamente habilitado.

6.3.4. Aprendiendo de los Incidentes

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

7. SEGURIDAD FÍSICA Y AMBIENTAL

Son sus objetivos:

a) Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Universidad.

b) Proteger el equipamiento de procesamiento de información crítica de la Universidad, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

c) Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

d) Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

e) Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información

de la Universidad: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

El Responsable de Seguridad Informática definirá junto con el Responsable del Área Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El Responsable del Área Informática asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la Universidad.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las a las áreas restringidas bajo su responsabilidad. Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la Universidad cuando lo crean conveniente.

Todo el personal de la Universidad es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

7.1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Organismo y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área Informática con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

7.2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el Responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado.

7.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas.

7.4. Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, que incluyan controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

7.5. Aislamiento de las Áreas de Recepción y Distribución

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

7.6. Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

7.7. Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

7.8. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

7.9. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

a) la realización de tareas de mantenimiento preventivo al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática.

b) el establecimiento de la práctica de que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) la registración de todas las fallas -supuestas y/o reales- y de todo el mantenimiento preventivo y correctivo realizado.

d) la registración del retiro de equipamiento para su mantenimiento de la sede de la Universidad.

e) la eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

7.10. Seguridad de los Equipos Fuera de las Instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Universidad será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Universidad para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

7.11. Desafectación o Reutilización Segura de los Equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos

rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

7.12. Políticas de Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

7.13. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede del Organismo sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Organismo.

8. GESTIÓN DE COMUNICACIONES Y OPERACIONES

Son sus objetivos:

a) Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

b) Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. Documentación de los Procedimientos Operativos Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

8.1.2. Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

8.1.3. Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

8.1.4. Separación de Funciones Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

En los casos en los que este método de control no se pudiera cumplirse, se implementarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

8.1.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

8.1.6. Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio que se incluirán en el contrato de tercerización.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información de la Universidad para el período estipulado de vida útil de cada componente.

Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema

El Responsable del Área Informática y el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

8.3. Protección Contra Software Malicioso

8.3.1. Controles Contra Software Malicioso

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementará dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

8.4. Mantenimiento

8.4.1. Resguardo de la Información

El Responsable del Área Informática y el de Seguridad Informática junto al Responsable del Área Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad.

En base a ello, se definirá y documentará un esquema de resguardo de la información.

8.4.2. Registro de Actividades del Personal Operativo

El Responsable del Área Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.
b) Errores del sistema y medidas correctivas tomadas.
c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
d) Ejecución de operaciones críticas
e) Cambios a información crítica

8.4.3. Registro de Fallas

El Responsable del Área Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

8.5. Administración de la Red

8.5.1. Controles de Redes

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo, contra el acceso no autorizado. El Responsable del Área Informática implementará dichos controles.

8.6. Administración y Seguridad de los Medios de Almacenamiento

8.6.1. Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como USB, discos, portatiles e informes impresos.

8.6.2. Eliminación de Medios de Información

El Responsable del Área Informática, junto con el Responsable de Seguridad Informática definirán procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

8.6.3. Procedimientos de Manejo de la Información Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a lo establecido en el capítulo 5 – “Clasificación y Control de Activos”.

8.6.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los recaudos para su protección, de almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

8.7. Intercambios de Información y Software

8.7.1. Acuerdos de Intercambio de Información y Software Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Universidad y las consideraciones de seguridad sobre la misma.

8.7.2. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiables, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

8.7.3. Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto "Aprobación del Sistema" incluyan, para las aplicaciones de Gobierno Electrónico, los siguientes aspectos:

a) Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la Universidad.

b) Autorización: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc.. Forma de comunicarlo al otro participante de la transacción electrónica.

c) Procesos de oferta y contratación pública: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.

d) Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.

e) Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios.

f) Cierre de la transacción: Forma de interacción más adecuada para evitar fraudes.

g) Protección a la duplicación: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

h) No repudio: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.

i) Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

8.7.4. Seguridad del Correo Electrónico

8.7.4.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.

b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.

c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.

e) El impacto de un cambio en el medio de comunicación en los procesos del Organismo.

f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.

g) Las implicancias de la publicación externa de listados de personal, accesibles al público.

h) El acceso de usuarios remotos a las cuentas de correo electrónico.

i) El uso inadecuado por parte del personal.

8.7.4.2. Política de Correo Electrónico

El Responsable de Seguridad Informática junto con el Responsable del Área Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.

b) Protección de archivos adjuntos de correo electrónico.

c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 10.3. Controles Criptográficos).

d) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.

e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

g) Definición de los alcances del uso del correo electrónico por parte del personal de la Universidad.

8.7.5. Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

8.7.6. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

8.7.7. Otras Formas de Intercambio de Información

Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

9. CONTROL DE ACCESOS

Son sus objetivos:

a) Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

b) Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

c) Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

d) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

e) Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

f) Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

9.1. Requerimientos para el Control de Acceso

9.1.1. Política de Control de Accesos

9.1.2. Reglas de Control de Acceso

9.2. Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

9.2.1. Registración de Usuarios

El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario,

9.2.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

9.2.3. Administración de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal.

9.2.4. Administración de Contraseñas Críticas

Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc.. 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.

El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas.

9.2.5. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

9.3. Responsabilidades del Usuario

9.3.1. Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las directivas que se impartan a tal efecto.

9.3.2. Equipos Desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

9.4. Control de Acceso a la Red

9.4.1. Política de Utilización de los Servicios de Red

Se controlará el acceso a los servicios de red tanto internos como externos. El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

9.4.2. Camino Forzado

El camino de las comunicaciones será controlado. Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

9.4.3. Autenticación de Usuarios para Conexiones Externas

El Responsable de Seguridad Informática, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

9.4.4. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Universidad.

Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas.

9.4.5. Protección de los Puertos (Ports) de Diagnóstico Remoto

Los puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado

9.4.6. Subdivisión de Redes

Se definirán y documentarán los perímetros de seguridad que sean convenientes, que se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

9.4.7. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para
todos los usuarios.

9.4.8. Control de Conexión a la Red

Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los “gateways” que separan los diferentes dominios de la red.

9.4.9. Control de Ruteo de Red

Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

9.4.10. Seguridad de los Servicios de Red

El Responsable de Seguridad Informática junto con el Responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red de la Universidad, tanto de los públicos como los privados.

9.5. Control de Acceso al Sistema Operativo

9.5.1. Identificación Automática de Terminales

El Responsable de Seguridad Informática junto con el Responsable del Área Informática realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

9.5.2. Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

9.5.3. Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

9.5.4. Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.

b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.

d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.

e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

f) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).

k) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

9.5.5. Uso de Utilitarios de Sistema

Existen programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado.

9.5.6. Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable de Seguridad Informática junto con el Responsable del Área Informática.

9.5.7. Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad Informática, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo. O que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, por un lapso que responderá a los riesgos de seguridad del área y de la información que maneje la terminal.. Para las PC’s, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra

las sesiones de aplicación o de red. Por otro lado, si un usuario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas.

9.5.8. Limitación del Horario de Conexión

Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo.

9.6. Control de Acceso a las Aplicaciones

9.6.1. Restricción del Acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la Universidad para el acceso a la información.

9.6.2. Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado).

La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones.

9.7. Monitoreo del Acceso y Uso de los Sistemas

9.7.1. Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

9.7.2. Monitoreo del Uso de los Sistemas

9.7.2.1. Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

9.7.2.2. Factores de Riesgo

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

9.7.2.3. Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.

La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

9.7.3. Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes. Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

9.8. Computación Móvil y Trabajo Remoto

9.8.1. Computación Móvil

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen la protección física necesaria, el acceso seguro a los dispositivos, la utilización de los dispositivos en lugares públicos. el acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

9.8.2. Trabajo Remoto

El trabajo remoto sólo será autorizado por el Responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad Informática, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

10. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Son sus objetivos:

a) Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.

b) Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

c) Definir los métodos de protección de la información crítica o sensible.

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Universidad en donde residan los desarrollos mencionados.

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad Informática definirá junto con el Responsable del Área de Sistemas, los métodos de encripción a ser utilizados.

10.1. Requerimientos de Seguridad de los Sistemas

10.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

10.2. Seguridad en los Sistemas de Aplicación

10.2.1. Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

10.2.2. Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

10.2.3. Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán controles criptográficos.

10.2.4. Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

a) Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.

b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.

c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.

d) Procedimientos para responder a las pruebas de validación de salidas.

e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

10.3. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

10.3.1. Política de Utilización de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.

2. Para la transmisión de información clasificada, fuera del ámbito del Organismo.

3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

10.3.2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

10.3.3. Firma Digital

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

10.3.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

10.3.5. Administración de Claves

10.3.5.1. Protección de Claves Criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar su utilización por parte de la Universidad. Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada. Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

10.4. Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

10.4.1. Control del Software Operativo

Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Área Informática. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción. El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado.

10.4.2. Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo.

Para proteger los datos de prueba se establecerán normas y procedimientos a tal efecto.

10.4.3. Control de Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos.

10.4.4. Control de Acceso a las Bibliotecas de Programas Fuentes

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes.

10.5. Seguridad de los Procesos de Desarrollo y Soporte

10.5.1. Procedimiento de Control de Cambios

Se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

10.5.2. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

10.5.3. Restricción del Cambio de Paquetes de Software

La modificación de paquetes de software suministrados por proveedores, previa autorización del Responsable del Área Informática, deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por el Organismo, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si el Organismo se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

10.5.4. Canales Ocultos y Código Malicioso

Se redactarán normas y procedimientos que incluyan:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.

b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c) Controlar el acceso y las modificaciones al código instalado.

d) Utilizar herramientas para la protección contra la infección del software con código malicioso.

10.5.5. Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos.

b) Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto 4.3.1. Requerimientos de Seguridad en Contratos de Tercerización.

e) Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

11. ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL ORGANISMO

Son sus objetivos:

a) Minimizar los efectos de las posibles interrupciones de las actividades normales de la Universidad (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

b) Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

c) Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

1) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.

2) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.

3) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

d) Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

11.1. Proceso de la Administración de la Continuidad del Organismo

El Comité de Ciberseguridad TIC, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Organismo.

11.2. Continuidad de las Actividades y Análisis de los Impactos

Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la Universidad que contemple los siguientes puntos:

• Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.

• Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.

• Identificar los controles preventivos.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades de la Universidad y no limitándose a las instalaciones de procesamiento de la información.

11.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Organismo

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Universidad. Estos procesos deberán ser propuestos por el Comité de Ciberseguridad TIC

11.4. Marco para la Planificación de la Continuidad de las Actividades del Organismo

Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

11.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo

El Comité de Ciberseguridad TIC establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

12. CUMPLIMIENTO

Son sus objetivos:

a) Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Universidad y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

b) Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Universidad.

c) Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

d) Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

e) Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

f) Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Universidad.

12.1. Cumplimiento de Requisitos Legales

12.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

12.1.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

12.1.2.1. Derecho de Propiedad Intelectual del Software

El Responsable de Seguridad Informática, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.

b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.

c) Mantener un adecuado registro de activos.

d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.

f) Verificar que sólo se instalen productos con licencia y software autorizado.

g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i) Utilizar herramientas de auditoría adecuadas.

j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

12.1.3. Protección de los Registros de la Universidad

Los registros críticos del Organismo se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la Universidad.

12.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La Universidad redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la Universidad.

12.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el

cual fueron provistos debe ser considerada como uso indebido. Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

12.1.6. Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/02, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

12.1.7. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

12.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

12.2.1. Cumplimiento de las Políticas de Seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.

b) Proveedores de sistemas.

c) Propietarios de información.

d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

12.2.2. Verificación de la Compatibilidad Técnica

El Responsable de Seguridad Informática verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

12.3. Consideraciones de Auditorías de Sistemas

12.3.1. Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

12.3.2. Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido. Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

12.4. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en las presente Políticas de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración de la Universidad, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Preparado por:	Revisado por:	Aprobado por:
Ing. Edwin E. Rosa Muñoz	Leandro De La Rosa.	Pendiente
Especialista Ciberseguridad	Encargado TIC	Comité de Ciberseguridad
Data Center y Conectividad	Pablo Trinidad	Consejo Academico
	Coordinador Data Center y Conectividad	

Universidad Central del Este Email Use Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
To prevent tarnishing the public image of Universidad Central del Este When email goes out from Universidad Central del Este the general public will tend to view that message as an official policy statement from the Universidad Central del Este.

2.0 Scope
This policy covers appropriate use of any email sent from a Universidad Central del Este email address and applies to all employees, vendors, and agents operating on behalf of Universidad Central del Este.

3.0 Policy
3.1 Prohibited Use. The Universidad Central del Este email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Universidad Central del Este employee should report the matter to their supervisor immediately.

3.2 Personal Use.
Using a reasonable amount of Universidad Central del Este resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Universidad Central del Este email account is prohibited. Virus or other malware warnings and mass mailings from Universidad Central del Este shall be approved by Universidad Central del Este VP Operations before sending. These restrictions also apply to the forwarding of mail received by a Universidad Central del Este employee.

3.3 Monitoring
Universidad Central del Este employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Universidad Central del Este may monitor messages without prior notice. Universidad Central del Este is not obliged to monitor email messages.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information	Information is considered sensitive if it can be damaging to Universidad Central del Este or its customers' reputation or market standing.
Virus warning.	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Universidad Central del Este, who do not have a need to know that information.

6.0 Revision History

Políticas de Acceso Físico

Departamento de TIC

Universidad Central del Este

Preparado por: Edwin E. Rosa Muñoz Encargado de Seguridad TI Departamento de Tecnologías de la Información	Revisado por : Manuel Solano. Encargado de Proyecto TI Pedro Mir Gerente TI	Aprobado por: Manuel Solano

Control de versiones

Versión	Revisión	Revisado Por	Modificado Por
1	18 Octubre 2012	Manuel Solano	Edwin E. Rosa

I. INTRODUCCIÓN

Propósito: El propósito de esta política es establecer normas para garantizar el buen funcionamiento del Data Center y servicios ofrecidos por el Departamento de TIC UCE.

La aplicación de esta política, buscar evitar el acceso no autorizado, además establecer controles y auditorías, logrando el control total en los accesos en la Universidad Central del Este, los cuales exponen a la institución a pérdidas de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

II. ALCANCE

La política se aplica a todos los accesos restringidos que contenga la Universidad Central del Este, aplicando a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios a la Universidad Central del Este o que estén relacionados. Se incluye además, todas las dependencias que son parte de la institución o que transite por la red de la Universidad Central del Este.

III. POLÍTICA

Ésta política especifica controles para reducir los riesgos asociados a la seguridad de la información asociados al control de acceso físico a las instalaciones.

ACCESO A LAS INSTALACIONES

- Todos los sistemas de seguridad física deben cumplir con todas las regulaciones aplicables como tal, pero no están limitados a los normas de construcción y prevención de incendios.
- Todo acceso físico a las personas será restringido, debiéndose gestionar y documentar.

- Todas las instalaciones de TI deberían estar físicamente protegidas en proporción a la criticidad o importancia de su función en la Universidad Central del Este.
- Todo acceso a las instalaciones de TI, sólo se concederán al personal designado por el Departamento de TI de la Universidad Central del Este y contratistas, cuyas responsabilidades de trabajo requieran el acceso a dicha instalación.
- El proceso para la obtención de las credenciales, tarjetas de acceso magnético o claves de acceso a instalaciones de TI deberán incluir la aprobación del Encargado del Departamento de TI de la Universidad Central del Este.
- Las tarjetas de acceso magnético o claves de acceso NO deben ser compartidas o cedidas a otros.
- Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltos al Departamento de TI de la UCE. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento.
- La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados al Departamento de TI de la UCE al correo monitor@uce.edu.do, incluyendo en el mensaje los siguientes datos: RUT, Nombre completo del empleado, departamento, y circunstancias en las cuales sucedió el robo o pérdida.
- Los registros de acceso de las tarjetas de acceso magnéticas o claves deberán conservarse para mantener una revisión de los accesos y rutinas realizadas basados en la criticidad de los recursos que se protegen
- El Departamento de TI de la UCE, en colaboración con el área de personal, serán los encargados de recuperar y eliminar los accesos a los lugares restringidos de las personas que sean desvinculadas ó que por cambios en el contrato, cambien sus roles operativos
- Los visitantes deberán ser escoltados por personal autorizado en el acceso a las zonas controlas por las instalaciones TI de la UCE

- El personal que acompañe a un visitante será el responsable directo de evitar cualquier acción indebida del mismo
- El acceso a todas las áreas restringidas serán monitoreadas por cámaras y captura de audio
- Las imágenes y/o audio capturado en las áreas restringidas podrán ser utilizadas en cualquier proceso legal o investigativo sin el consentimiento directo de las personas involucradas
- El área de seguridad de la Información, se encargará de revisar periódicamente los privilegios y derechos de acceso de las tarjetas de acceso magnético o claves para eliminar las de las personas que ya no requieran de éstos privilegios
- El área de seguridad de la Información se reserva el derecho de negar el acceso a un área especifica a cualquier personal previamente autorizado si considera que existe algún tipo de riesgo para la infraestructura y continuidad del Centro
- Las señaléticas para el acceso a las salas y locaciones restringidas deberá ser simple, sin embargo, deberá informar de forma simple la importancia de la ubicación
- Cualquier uso de las instalaciones de TI deberá contar con la aprobación del Encargado del Departamento TI o a quien éste designe.
- El personal autorizado debe tener las 24 horas de libre acceso a las instalaciones críticas de TI, lo que debe ser informado y aprobado por el departamento o unidad que corresponda.

IV. PERSONAL AUTORIZADO

El acceso al Data Center y racks de redes TI estarán restringidos sólo a los administradores de sistema TI y Jefes del Departamento de TI previamente autorizados. Los otros accesos a personal de servicios, Oficiales de seguridad física y otros actores, estarán restringidos y, según sea necesario, se solicitará al personal

correspondiente para gestionar con el Encargado del Departamento de TI dichos privilegios. Cualquier otro tipo de personal, deberá ingresar acompañado a las instalaciones.

V. RESPONSABILIDADES

El Departamento de TI de la UCE es el responsable de la seguridad de los datos en la red y sus equipos, con el fin de ejecutar a cabalidad la tarea de mantener la infraestructura de la red.

VI. APLICACIÓN DE LAS POLÍTICAS DE ACCESO FÍSICO

La infracción a las obligaciones establecidas en el artículo anterior, podrá constituir una violación a las normativas, y será sancionada en conformidad a las disposiciones establecidas por las autoridades de UCE. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Departamento de TI de la UCE velará por el cumplimiento de estas políticas, resguardando los intereses de la Institución.

El Departamento de TI no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

VII. DIFUSIÓN

Se mantendrá publicada dentro de la Intranet de la Universidad Central del Este, las normas de uso y políticas de seguridad establecidas en el presente reglamento.

Políticas de Respaldo

Departamento de TIC

Universidad Central del Este

Preparado por:	Revisado por :	Aprobado por:

Control de versiones

Versión	Revisión	Revisado Por	Modificado Por
1.0	4 Abril 2014	Ing. Edwin E. Rosa	Ing. Edwin E. Rosa

I. INTRODUCCIÓN

Propósito: El presente documento tiene como finalidad dar a conocer las políticas y estándares para la realización de Respaldos y proteger adecuadamente la información de la Universidad Central de Este.

La aplicación de estas políticas busca asegurar la restauración, persistencia y continuidad de las operaciones de la universidad en los casos en que se pierda parte o toda la información de la empresa.

II. ALCANCE

La política se aplica a todos los activos de información de la Universidad Central del Este, sus empleados y demás empresas dependientes o relacionadas sin importar ubicación geográfica, información que maneje la UCE de empleados temporales de otras empresas o agencias, información de socios de negocios y contratistas.

a) La información que será respaldada podrá variar desde archivos del sistema operativo, bases de datos, aplicaciones, instaladores, Discos y/o archivos de configuración de Máquinas Virtuales y elementos activos de la red. Estos se dividen en **datos estáticos y datos dinámicos.**

1. **Datos estáticos**:
   a) Sistema operativo, service packs, Hot Fix y actualizaciones.
   b) Sofware propio y software de terceros instalados en los servidores (sistemas, antivirus, plataformas y demás herramientas)
   c) Scripts de rutinas especiales y archivos de configuraciones.
   d) Archivos de configuración de Maquinas virtuales.
2. **Datos dinámicos**
   b) Directorio de usuarios
   c) Bases de datos
   d) Datos almacenados en los Servidores de archivos
   e) Discos virtuales.

No es obligación del Departamento de TI hacer Respaldos de la información que contengan los equipos personales de usuarios y relacionados que no pertenezcan a la UCE.

III. POLÍTICA

Ésta política específica procedimientos y normas para el correcto respaldo y restauración de activos de información que maneje la Universidad Central del Este.

IV. CUMPLIMIENTO

Para Mantener la Integridad y confiabilidad de la información se cuenta con licenciamiento de Antivirus, servicios de actualizaciones a sistemas operativos y aplicaciones, soporte y mantenimiento a los dispositivos de almacenamiento (Data Storage), herramientas de respaldo local como Microsoft System Center DPM 2012 R2, VEEAM Backup para el respaldo a los servidores y discos virtuales, Windows Azure Backup como herramienta de respaldo en la nube entre otras herramientas que permiten dar cumplimiento y seguimiento a las políticas establecidas. Todo esto de la mano con un seguimiento permanente de los encargados de las áreas pertinentes minimizando así los riesgos y amenazas en contra de la información.

V. RESPONSABILIDADES

El Departamento de TI de la UCE es el responsable del respaldo y restauración de los datos. Cualquier pregunta o comentario referente a la presente política debe ser dirigido al Departamento de TI de la UCE.

La aplicación y cumplimiento de esta política es obligatoria. El Departamento de TI debe asegurarse del cumplimiento y monitoreo continuo de la misma dentro de la UCE. Violaciones a la política, sus estándares y procedimientos resultarán en acciones correctivas por parte de los órganos superiores de la institución. Esas acciones serán consistentes con la severidad del incidente según lo determinado por una investigación. Pueden incluir, pero no están limitadas a:

- Pérdida de privilegios de acceso a ciertos activos de información.

- Otras acciones consideradas apropiadas por la administración, Recursos Humanos y el Departamento Legal.

VI. OPERACIÓN DE RESPALDO

A continuación se describen los procedimientos, normas y determinación de responsabilidades establecidos para la realización de los respaldos:

1. Los respaldos siempre se harán de acuerdo a este documento estándar de políticas.
2. El respaldo de información se efectuará en discos locales (SAN) y en servicios en la nube.
3. Se harán respaldos completos y respaldos incrementales. Los respaldos completos consistirán en copias de seguridad de toda la información de una aplicación, archivo o Base de Datos en particular. Los respaldos incrementales consistirán en copias de la información que se ha generado desde que se hizo el último respaldo completo de un dato dinámico en particular.
4. La frecuencia y retención de cada respaldo dependerá de la relevancia de los datos.
5. Los respaldos completos se harán preferiblemente en horario no laborable. El último respaldo completo se almacenará fuera de la infraestructura local, su retención y frecuencia se determinaran según su relevancia.
6. Los respaldos completos e incrementales se eliminarán cuando se haya cumplido su ciclo de retención previamente determinado.
7. Si por alguna razón no se puedo hacer algún respaldo el mismo se deberá realizar en la próxima ventana de tiempo lo antes posible.
8. El nombre de archivo y/o los metadatos de los respaldos debe contener la fecha en que fueron realizados.

9. Toda conexión hacia servicios de respaldos en la nube se establecerá de manera segura ya sea a través de una VPN o utilizando certificados debidamente emitidos de manera que se garantice la integridad de los datos transmitidos.

10. Cada respaldo almacenado que sea trasladado fuera de la infraestructura de UCE debe estar debidamente cifrado para garantizar la integridad de la información.

11. Los respaldos de equipos de estaciones de trabajo y archivos de uso general de los usuarios serán responsabilidad de los mismos usuarios y de la unidad de soporte técnico y asistencia a usuarios.

VII. POLITICAS DE RESPALDOS

Detalles:

Datos	Respaldos Incrementales	Respaldo Completo (Full Backup)	Ubicación	Respaldos Externos	Herramienta utilizada
BD Akademia	2 Diarios 12pm 6pm Retención 10 Días	Diario a las 8:00 PM, retención: 120		Frecuencia: Mensual Ultimo dia del mes Retención: Anual	DPM 2012 R2 & Azure Backup
BD Financiero	2 Diarios 12pm 6pm Retención 10 Días	Diario a las 8:00 PM, retención: 120		Frecuencia: Mensual Ultimo día del mes Retención: Anual	DPM 2012 R2 & Azure Backup
BD RRHH_UCE	2 Diarios 12pm 6pm Retención 10 Días	Diario a las 8:00 PM, retención: 120		Frecuencia: Mensual Ultimo dia del mes Retención: Anual	DPM 2012 R2 & Azure Backup
BD histórica					Windows Azure
Configuracion					

VIII. RECUPERACIÓN DE RESPALDOS

Los procedimientos de Recuperación dependerán del tipo de dato y/o de la herramienta utilizada previamente para respaldarlo.

1. La obtención de copias para fines de pruebas y los procesos de recuperación de los respaldos debe contar con la autorización previa del gerente del departamento.
2. Antes de recuperar un respaldo este debe ser cargado a un ambiente de pruebas para comprobar su integridad.
3. Previo a la recuperación se recomienda realizar un respaldo a los Datos en su estado actual. Esto para tener un respaldo en caso de una recuperación errónea.
4. Todo proceso de recuperación debe ser debidamente documentado.
5. En los casos donde se realice una recuperación sin la utilización de una herramienta que deje un registro del evento se debe documentar en la documentación de recuperación de respaldos. \\ucefs01\documentacion\DocRecResp.docx

IX. PRUEBAS PERIODICAS DE RESPALDOS

Se realizaran pruebas periódicas de los Respaldos almacenados en disco para verificar su funcionalidad.

La frecuencia de las pruebas dependerá del tipo dato y su relevancia.

I. DIFUSIÓN

Estas políticas de Respaldo se mantendrán publicadas dentro de la Intranet de la Universidad Central del Este con acceso restringido, sólo el personal del Departamento de TI podrá accederlo para su consulta y posibles ediciones.

Políticas de uso de Thin-client/mini-pc en los laboratorios

- Se mantendrán funcionando paralelamente VMWare y Hyper-V para la plataforma de VDI. VMWare se utilizará para los modelos de thin client CISCO, los cuales no son compatibles con RDP. Hyper-V se utilizará para los ViewSonic y mini pc.
- Se pondrán disponibles aplicaciones remotas (RemoteApps).
- Las aplicaciones más básicas (las que menos recursos demandan) se instalarán en los servidores locales, las más avanzadas (las que más recursos demandan, como la suite AUTODESK) se instalarán en Azure.
- Los servidores de Azure se encenderán por lo menos 15 minutos antes de cada clase que necesite las RemoteApps que estén instaladas en ellos y se apagarán cuando la clase termine. Se programarán reglas que hagan eso automáticamente.
- En vista de las limitantes que tienen los modelos CISCO para conectarse a Hyper-V se moverán todas las unidades a laboratorios del CU que estén destinados a materias básicas de informática y uso de AL-UCE.

Thin-client CISCO

- Se conectarán exclusivamente a pool de sesiones de VMWare.
- Se les instalará un explorador de internet y la suite ofimática Microsoft Office a las sesiones del pool.
- En las ocasiones que necesiten software adicional se les distribuirá a través de RemoteApp.
- Los técnicos de los laboratorios se encargarán de descargar y poner en el escritorio de las sesiones los accesos directos a las aplicaciones remotas que necesite cada materia. Serán responsables de revisar el funcionamiento antes de cada clase.
- Los usuarios se conectarán a las RemoteApps utilizando sus credenciales. De esa forma se les creará un perfil en el servidor y solo tendrán acceso a los datos de ese perfil. Luego desde cualquier thin client o mini pc que se conecten con sus credenciales a una RemoteApp podrán ver su perfil.
- Los usuarios almacenarán sus archivos en su cuenta de OneDrive.
- Hay dos formas para almacenar archivos en OneDrive. 1 - Si la aplicación es de Microsoft es posible guardar directamente a OneDrive: la opción es visible en el menú “Guardar como” de cada aplicación; 2 – Guardando los archivos en alguna carpeta local y luego de haber iniciado sesión en la versión web de OneDrive cargarlos manualmente. Los técnicos de los laboratorios deben dominar la herramienta para que puedan instruir a los profesores y estudiantes que lo necesiten.
- Los técnicos de laboratorio deben cerrar las sesiones al finalizar cada clase.

Thin-client ViewSonic

- Los ViewSonic se conectarán a sesiones de Hyper-V.
- Se les instalará un explorador de internet a la colección de sesiones.
- Se publicarán las aplicaciones adicionales como RemoteApp.
- Los técnicos de los laboratorios se encargarán de descargar y poner en el escritorio de las sesiones los accesos directos a las aplicaciones remotas que necesite cada materia. Serán responsables de revisar el funcionamiento antes de cada clase.
- Los usuarios se conectarán a las RemoteApps utilizando sus credenciales. De esa forma se les creará un perfil en el servidor y solo tendrán acceso a los datos de ese perfil. Luego desde cualquier thin client o mini pc que se conecten con sus credenciales a una RemoteApp podrán ver su perfil.
- Los usuarios almacenarán sus archivos en su cuenta de OneDrive.
- Hay dos formas para almacenar archivos en OneDrive. 1 - Si la aplicación es de Microsoft es posible guardar directamente a OneDrive: la opción es visible en el menú “Guardar como” de cada aplicación; 2 – Guardando los archivos en alguna carpeta local y luego de haber iniciado sesión en la versión web de OneDrive cargarlos manualmente. Los técnicos de los laboratorios deben dominar la herramienta para que puedan instruir a los profesores y estudiantes que lo necesiten.
- Los técnicos de laboratorio deben cerrar las sesiones al finalizar cada clase.

Mini PC’s

- Se conectarán a sesiones de Hyper-V (las mismas que los ViewSonic)
- Se pondrá en el escritorio de las mini pc un archivo RDP apuntando a una VM fija.
- Se configurará el archivo RDP para que reconozca los dispositivos plug and play que se conecten a la mini pc.
- Los técnicos de laboratorios abrirán ese archivo antes de cada clase.
- Los usuarios se conectarán a las RemoteApps utilizando sus credenciales. De esa forma se les creará un perfil en el servidor y solo tendrán acceso a los datos de ese perfil. Luego desde cualquier thin client o mini pc que se conecten con sus credenciales a una RemoteApp podrán ver su perfil.
- Los usuarios almacenarán sus archivos en su cuenta de OneDrive.
- Hay dos formas para almacenar archivos en OneDrive. 1 - Si la aplicación es de Microsoft es posible guardar directamente a OneDrive: la opción es visible en el menú “Guardar como” de cada aplicación; 2 – Guardando los archivos en alguna carpeta local y luego de haber iniciado sesión en la versión web de OneDrive cargarlos manualmente. Los técnicos de los laboratorios deben dominar la herramienta para que puedan instruir a los profesores y estudiantes que lo necesiten.
- Los técnicos de laboratorio deben cerrar las sesiones al finalizar cada clase.

1. Visión general

El acceso remoto a nuestra red Institucional es esencial para mantener la productividad de nuestros colaboradores, pero en muchos casos este acceso remoto se origina a partir de redes que ya pueden estar comprometidas o están en una postura de seguridad significativamente menor que nuestra red Institucional. Si bien estas redes remotas están fuera del control de la política de UCE, debemos mitigar estos riesgos externos lo mejor que nos permita nuestra capacidad.

2. Propósito

El propósito de esta política es definir reglas y requisitos para conectarse a la red de Universidad Central del Este desde cualquier host y ubicación geográfica. Estas reglas y requisitos están diseñados para minimizar la exposición potencial a Universidad Central del Este de los daños que pueden resultar del uso no autorizado de los recursos. Los daños incluyen la pérdida de datos sensibles o confidenciales de la empresa, propiedad intelectual, daños a la imagen pública, daños a los sistemas internos críticos y multas u otras responsabilidades financieras incurridas como resultado de esas pérdidas.

3. Alcance

Esta política se aplica a todos los empleados, estudiantes contratistas, proveedores y agentes de Universidad Central del Este que utilizan equipos de propiedad de la empresa o de propiedad personal para conectarse a la red institucional. Esta directiva se aplica a las conexiones de acceso remoto utilizadas para realizar el trabajo en nombre de Universidad Central del Este, incluida la lectura o el envío de correo electrónico y la visualización de recursos web de intranet. Esta directiva cubre todas y cada una de las implementaciones técnicas de acceso remoto utilizadas para conectarse a redes de Universidad Central del Este.

4. Política

Es responsabilidad de cada empelado, contratista, proveedor y agente con privilegios de acceso remoto a la red institucional de Universidad Central del Este asegurarse de que su conexión de acceso remoto tenga la misma consideración que la conexión in situ del usuario a la institución.

El acceso general a Internet para uso recreativo a través de la red institucional está estrictamente limitado a empleados, estudiantes, contratistas, proveedores y agentes (en adelante, "Usuarios autorizados"). Al acceder a la red Universidad Central del Este desde un ordenador personal, los Usuarios Autorizados son responsables de impedir el acceso a cualquier recursos o datos informáticos por parte de Usuarios no autorizados. Está prohibido realizar actividades ilegales a

través de la red de Universidad Central del Este por parte de cualquier usuario (Autorizado o de otro tipo). El Usuario Autorizado asume la responsabilidad y las consecuencias del uso indebido del acceso del Usuario Autorizado. Para obtener más información y definiciones, consulte la *Política de seguridad de la información*.

Los Usuarios Autorizados no utilizarán la red de UCE para acceder a Internet con intereses comerciales externos, maliciosos o vandálicos.

4.1 Requisitos

4.1.1 El acceso remoto seguro debe controlarse estrictamente con cifrado (es decir, redes privadas virtuales (VPN)) y frases de contraseña sólidas. Para obtener más información, consulte la política de cifrado *aceptable* y la política de administración de usuarios y manejo de credenciales.

4.1.2 Los Usuarios Autorizados protegerán su nombre de usuario y contraseña, incluso de los miembros de la familia.

4.1.3 Al utilizar un equipo propiedad de UCE para conectarse de forma remota a la red Institucional de UCE, los Usuarios Autorizados se asegurarán de que el host remoto no esté conectado a ninguna otra red al mismo tiempo, con la excepción de las redes personales que están bajo su completo control o bajo el control de un Usuario Autorizado o un tercero debidamente autorizado.

4.1.4 El uso de recursos externos para realizar actividades propias de la UCE debe ser aprobado previamente por el responsable de seguridad de la información y el encargado de área correspondiente.

4.1.5 Todos los hosts que están conectados a las redes de UCE a través de tecnologías de acceso remoto deben utilizar el software antivirus más actualizado (https://microsoft.com/es-es/windows/comprehensive-security), esto incluye los equipos personales. Las conexiones de terceros deben cumplir con los requisitos previamente establecidos en el Acuerdo *de Terceros*.

4.1.6 El equipo personal utilizado para conectarse a las redes de Universidad Central del Este debe cumplir los requisitos de equipos propiedad de UCE para el acceso remoto como se indica en el Estándar de configuración hardware y software para el acceso a las redes de UCE.

5. Cumplimiento de políticas

5.1 Medición de cumplimiento

El encargado de Seguridad Informática verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, las revisiones periódicas de registros, la supervisión de

vídeo, los informes de herramientas empresariales, las auditorías internas y externas, la inspección física o lógica del dispositivo en cuestión y proporcionará comentarios al propietario de la información y al encargado del área correspondiente.

5.2 Excepciones
Cualquier excepción a la política debe ser aprobada por el comité de Seguridad de la información previamente.

5.3 Incumplimiento
Un usuario que se encuentre que ha violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo y/o sanciones académicas según sea el caso.

6 Normas, Políticas y Procesos Relacionados

Revise las siguientes políticas para obtener más información sobre cómo proteger la información al acceder a la red Institucional a través de métodos de acceso remoto y el uso aceptable de la red de Universidad Central del Este:

- *Políticas de Seguridad de la Información*
- *Políticas de administración de usuarios y manejo de credenciales*

Política de seguridad de Routers, Switch's y dispositivos de interconexión.

1. Propósito

Este documento describe una configuración de seguridad mínima requerida para todos los routers y switches que se conectan a una red de producción o se utilizan en capacidad de producción en o en nombre de Universidad Central del Este.

2. Alcance

Todos los empleados, contratistas, consultores, trabajadores temporales y de otro tipo en Universidad Central del Este y sus subsidiarias deben adherirse a esta política. Todos los enrutadores y conmutadores y otros dispositivos de interconexión conectados a Universidad Central del Este se ven afectados.

3. Política

Cada router debe cumplir con los siguientes estándares de configuración:

1. No se configura ninguna cuenta de usuario local en el router. El Routers y el Switches deben utilizar el TACACS+, Radius o el método u protocolo definido en el servidor NAC para toda la autenticación de usuario.
2. La contraseña de habilitación (enable) en el router o el Switch se debe mantener en una forma cifrada segura. Los dispositivos deben tener la contraseña de habilitación establecida en la contraseña actual de producción.
3. Se deben deshabilitar los siguientes servicios o características:
    a. Difusiones dirigidas por IP
    b. Paquetes entrantes en el router/switch originados con direcciones no válidas tales como direcciones RFC1918, según sea el caso.
    c. small services TCP
    d. small services UDP
    e. All source routing and switching
    f. Todos los servicios web no seguros que se ejecutan en el dispositivo
    g. Universidad Central del Este protocolo de detección en interfaces conectadas a Internet
    h. Servicios Telnet, FTP y HTTP
    i. Configuración automática

4. Los siguientes servicios deben deshabilitarse a menos que se proporcione una justificación empresarial:
    a. Universidad Central del Este protocolo de detección y otros protocolos de descubrimiento
    b. Enlace troncal dinámico
    c. Entornos de scripting, como el shell TCL
5. Se deben configurar los siguientes servicios:
    a. Cifrado de contraseña
    b. NTP configurado a una fuente estándar corporativa
6. Todas las actualizaciones de enrutamiento se realizarán mediante actualizaciones de enrutamiento seguras.
7. Utilice cadenas de comunidad SNMP estandarizadas corporativas. Las cadenas predeterminadas, como public o private, deben quitarse. EL SNMP se debe configurar para utilizar la versión más segura del protocolo permitido por la combinación del dispositivo y los sistemas de administración.
8. Las listas de control de acceso se deben utilizar para limitar el origen y el tipo de tráfico que puede terminar en el propio dispositivo.
9. Las listas de control de acceso para el tránsito del dispositivo deben agregarse a medida que surjan las necesidades empresariales.
10. El router debe incluirse en el sistema de administración de empresas corporativas con un punto de contacto designado.
11. Cada router debe tener la siguiente declaración presentada para todas las formas de inicio de sesión, ya sean remotas o locales:

    "SE PROHÍBE EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO DE RED. Debe tener permiso explícito para acceder o configurar este dispositivo. Todas las actividades realizadas en este dispositivo pueden ser registradas, y las violaciones de esta política pueden resultar en una acción disciplinaria, y pueden ser reportadas a las fuerzas del orden. No hay derecho a la privacidad en este dispositivo. La utilización de este sistema constituirá un consentimiento para el seguimiento."

12. Telnet nunca se puede utilizar a través de ninguna red para manejar a un router, a menos que haya un túnel seguro que proteja toda la trayectoria de comunicación. SSH versión 2 es el protocolo de administración preferido.

13. Los protocolos de enrutamiento dinámico deben utilizar la autenticación en las actualizaciones de enrutamiento enviadas a los vecinos. El hash de contraseña para la cadena de autenticación debe estar habilitado cuando se admite.
14. El estándar de configuración del router corporativo definirá la categoría de dispositivos sensibles de enrutamiento y conmutación, y requerirá servicios o configuración adicionales en dispositivos sensibles, incluidos:
    a. Contabilidad de listas de acceso IP
    b. Registro de dispositivos
    c. Los paquetes entrantes en el router originados con direcciones no válidas, tales como direcciones RFC1918, o aquellos que podrían ser utilizados para suplantar el tráfico de red se eliminarán
    d. El acceso a la consola del router y al módem debe estar restringido por controles de seguridad adicionales

4. Cumplimiento de políticas

5.1 Medición de cumplimiento

El Responsable de Seguridad Informática verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, los tutoriales periódicos, la supervisión de vídeo, los informes de herramientas empresariales, las auditorías internas y externas y los comentarios al propietario de la directiva.

5.2 Excepciones

Cualquier excepción a la política debe ser aprobada por el equipo de Infosec con antelación.

5.3 Incumplimiento

Un empleado que se encuentre que ha violado esta política puede estar sujeto a medidas disciplinarias, hasta e incluyendo la terminación del empleo.

6 Normas, Políticas y Procesos Relacionados

Ninguno.

7 Definiciones y términos

Ninguno.

1. OBJETIVO

El propósito de esta política es establecer normas y procedimientos para garantizar el correcto manejo de las credenciales, además de la creación, modificación, desactivación y Eliminación del acceso de los usuarios a los sistemas de información. Establecer los mecanismos de archivo y custodia de las credenciales de super usuario.
La aplicación de esta política, buscar evitar el acceso no autorizado, además establecer controles y auditorías, logrando el control total de los accesos a los sistemas los cuales exponen a la institución a pérdidas de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

2. ALCANCE

La política se aplica a todos los sistemas de información y activos digitales de la empresa, aplicando a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios a la empresa o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución o que transite por la red de la empresa.

3. REFERENCIAS

Formulario de Respaldo a PCs Usuarios.

4. GLOSARIO DE TERMINOS

Credenciales: Conjunto de datos que incluye la identificación y prueba de identificación que se utiliza para obtener acceso a recursos locales y de red.

Contraseña: es una cadena de caracteres, que hay que suministrar para obtener la autorización para un acceso o un nombre de inicio de sesión. Puede estar formada por letras, números y símbolos.

Super Usuario: usuario con privilegios de administrador o root del sistema.

Perfil: Asignación de acceso a las funcionalidades de las aplicaciones de acuerdo al rol de trabajo del empleado y el cual debe estar debidamente aprobado por el Comité de Ciberseguridad TIC.

5. DESARROLLO

5.1. Nomenclatura de usuario y contraseñas

Esta política establece la nomenclatura para la creación de usuarios y específica las características que deben cumplir las contraseñas para reducir los riesgos.
Los usuarios serán creados utilizando la primera letra del primer nombre seguido de primer apellido, en caso de coincidencias se utilizarán segundos nombres y apellidos o de ser necesario numeración (ej: Juan Perez, usuario: jperez. Juan Perez usuario: jperez2).
Todos los usuarios deberán ser protegidos por una contraseña la cual será introducida por la persona física a la que se le asigna el usuario. La misma deberá cumplir con las siguientes características:
Edad máxima de la contraseña 90 días.
Longitud mínima de contraseña 8 caracteres.
Requisitos de complejidad: utilizar una combinación de minúsculas y mayúsculas, números y caracteres especiales [como ~!@#$%^&*()_+=?><./].

5.2. Política de manejo de credenciales:

Esta política específica controles para el manejo de las credenciales de usuarios y sus diferentes roles en los sistemas de información, dominio, equipo local y servicios en la nube.

Custodia de credenciales administrativas:
Se establece un documento de credenciales el cual será encriptado utilizando una longitud de clave mínima de 20 caracteres. Se guardará una copia impresa de esta clave en la caja fuerte de la empresa.
Para los servicios en la nube se utilizar métodos de 2AF (autenticación en dos pasos).

5.3 Política de administración de usuarios

Esta política define los procedimientos para la creación, modificación, desactivación y eliminación de usuarios de los diferentes sistemas de información de UCE.
En UCE existen los siguientes sistemas en los cuales se crean usuarios:

1. Controlador del dominio uce.edu.do: los usuarios y grupos creados en este controlador de dominio tienen acceso a los equipos terminales para las tareas regulares como son herramientas ofimáticas, acceso a archivos de texto, hojas de cálculo, informes, reportes y o cualquier otra data para la cual haya sido previamente autorizado.

2. Sistemas de correo electrónico alojado en Office 365 para los dominios pertenecientes a UCE: uce.edu.do, aluce.edu.do, chuce.com, los usuarios creados en estas plataformas tienen acceso al correo empresarial, así como también almacenamiento de archivos en la nube, servicios de colaboración en línea y mensajería instantánea.

3. Sistema de gestión académica - AKADEMIA:
   Los usuarios de AKADEMIA utilizan las credenciales del dominio uce.edu.do para autenticarse. De acuerdo con sus funciones desde la aplicación se le aplican los perfiles agregándole roles y permisos según sean requerido.

4. Sistema de gestión de recursos humanos: Los usuarios del sistema de RRHH se crean de manera particular en esta aplicación y se le aplican perfiles y roles según sean requeridos para desempeñar sus funciones.

5. Sistema de gestión Financiera:
   Los usuarios del sistema de gestión financiera se crean de manera particular en esta aplicación y se le aplican perfiles y roles según sean requeridos para desempeñar sus funciones.

5.3.1 Creación de usuarios

Se debe recibir formalmente un requerimiento de creación de cuentas de usuario con la información mínima requerida. El responsable de Seguridad Informática o quien delegue el Comité de Ciberseguridad TIC, recibe vía correo electrónico la solicitud de creación de usuarios del departamento de RRHH o del Responsable de Área solicitante especificando el asunto: *"Solicitud de Creación de Cuentas de Usuario"*, en el cual se deben indicar entre otros los siguientes campos: 1) nombre de la persona, 2) Número de Identificación o ID de empleado 3) Rol que desempeñará, posición y departamento, 3) Sistemas en los cuales se le creara un usuario 4) Jefe inmediato o supervisor 5) Duración de la validez de la cuenta o contrato.

5.3.2 Desactivación de usuarios

Se debe recibir formalmente un requerimiento de desactivación de usuario con la información mínima requerida. El responsable de Seguridad Informática o quien delegue el Comité de Ciberseguridad TIC, recibe vía correo electrónico la solicitud de desactivación de usuarios del departamento de RRHH o del Responsable de Área solicitante especificando el asunto: *"Solicitud de Desactivación de Cuentas de Usuario",* en el cual se deben indicar entre otros los siguientes campos: 1) nombre de la persona, 2) Número de Identificación o ID de empleado 3) Rol que desempeño, posición y departamento, 3) Sistemas en los cuales se le creo un usuario 4) Jefe inmediato o supervisor 5) Motivo de la desactivación.

5.3.3 modificación de usuarios

Se debe recibir formalmente un requerimiento de modificación de usuario con la información mínima requerida. El responsable de Seguridad Informática o quien delegue el Comité de Ciberseguridad TIC, recibe vía correo electrónico la solicitud de modificación de usuarios del Responsable de Área a la cual pertenece el usuario solicitante especificando el asunto: *"Solicitud de modificación de Cuentas de Usuario",* en el cual se deben indicar entre otros los siguientes campos: 1) Usuario existente 2) posición y departamento 3) Sistema en el cual desea modificar el usuario 4) Jefe inmediato o supervisor 5) Motivo de la modificación 6) Rol, campos y permisos específicos a modificar. 6) autorización de la modificación aprobada por el Comité de Ciberseguridad TIC.
Este procedimiento aplica y se exige para toda asignación o cambios de permisos y roles de usuarios nuevos, existentes o desactivados.

5.3.4 eliminación de usuarios

Queda prohibido eliminar usuarios de cualquiera de los sistemas, ya que los mismos pueden servir para la comprobación durante auditorias. Esta política de eliminación de usuario pudiera ser omitida en el caso de que se refiera a un usuario creado en un servicio tercerizado como correo electrónico no oficial, colaboración, mensajería instantánea, etc. o donde la permanencia de un usuario pueda involucrar el impedimento de funcionalidad, limitación de uso por licenciamiento o suponga una carga y/o costo fijo para la empresa, en tales casos el responsable de seguridad informática deberá guardar una copia digital debidamente documentando la existencia previa del usuario y la plataforma en la que existió.

6. RESPONSABILIDAD

Responsable estratégico:
Responsable de Seguridad Informática persona designada por el encargado de TIC y el Consejo Académico.
Responsable operativo:
Enc. De Tecnología.

El Responsable de Seguridad Informática o quien haya sido designado por el encargado de TIC para administrar cada sistema según sus funciones y responsabilidades.
Se asignarán roles establecidos por política de Directorio Activo de Windows Server para manejar las funciones y responsabilidades.
Para aplicaciones desarrolladas por terceros se recomienda el soporte para protocolos como LDAP para lograr inicio de sesión único a través de las credenciales del Directorio Activo.
Cada persona responsable de una función deberá tener un usuario personal único con los permisos adecuados para desempeñar sus labores. En caso de que requiera elevación de privilegios deberá pasar por un proceso de aprobación establecido por la administración.

El usuario Super Usuario: "Administrator", "admin" o "root" de los sistemas de información, sistemas operativos servidor o cliente no deberán ser utilizados por ningún

otro usuario, a menos que una situación especial lo amerite como en el caso de una implementación en tal caso el comité debe designar 2 miembros del comité al azar que revisen el historial de eventos antes, durante y después de la implementación.

La infracción a las obligaciones establecidas en este documento podrá constituir una violación a las normativas, y será sancionada en conformidad a las disposiciones establecidas por la institucion. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.
El Departamento TIC de Universidad Central del Este velará por el cumplimiento de estas políticas, resguardando los intereses de la Institución.

Fin del Documento.

Universidad Central del Este

Política de Seguridad de la Información[1]

San Pedro de Macorís, Rep. Dominicana
2021

INDICE

[1] Preparada por: Departamento de Tecnologías de la Información y Comunicaciones – Director, Leandro de la Rosa
Revisada por:
Aprobada por:
Fecha de aprobación:

1. Antecedentes

La información es un recurso que, como el resto de los activos, tiene valor para la comunidad universitaria y, por consiguiente, debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo, de esta manera, a una mejor gestión de la Universidad.

En vista de ello, la Universidad Central del Este (UCE) crea su Departamento de Tecnologías de la Información y Comunicaciones (TIC) con el objetivo de planear, desarrollar, implementar y mantener todos los servicios de Tecnologías de la Información que contribuyan a la transformación de los procesos institucionales de administración, academia, investigación, extensión y vinculación con entrega de valor para la UCE[2].

Durante su proceso de elaboración del **Plan Estratégico Quinquenal para el período 2018-2022**[3], la UCE detectó ciertas debilidades y amenazas relacionadas con este departamento, llevándola a establecer un eje estratégico específico para mitigar y/o remediar las consecuencias futuras de estos hallazgos:

> **Eje estratégico no. 04: "Actualización y modernización de la infraestructura"**
> **Objetivo Específico:** Mejora de las condiciones físicas y tecnológicas para incrementar la calidad y efectividad de los aprendizajes.
> **Líneas de Acción:**
> - Adecuación, ampliación y modernización de la infraestructura física conforme el crecimiento de la matrícula universitaria, la calidad y efectividad de los aprendizajes y el desarrollo de las funciones administrativas.
> - *Modernización de la infraestructura tecnológica para aumentar la calidad y efectividad del proceso de enseñanza-aprendizaje, y la eficiencia y eficacia de los procesos.*
> - *Actualización y modernización de laboratorios según requerimientos de los avances científicos en las áreas de enseñanza aprendizaje de la UCE.*
> - *Mejora de acceso a recursos tecnológicos por parte de profesores y estudiantes.*
> - *Aumento del uso de recursos digitales por docentes y estudiantes.*
> - Mejora del mantenimiento, iluminación y seguridad en el campus.

Como consecuencia de lo expuesto anteriormente y con miras a cumplir su visión[4] institucional, la UCE se ha abocado a la tarea de implementar su propia **Política de Seguridad de la Información**, basándose en las características establecidas para el desarrollo de esta.

Esta Política de Seguridad de la Información se ha definido para identificar los principios, objetivos y responsabilidades que se deben asumir, ejecutar y respetar para acceder a la información y los recursos tecnológicos institucionales.

---

[2] Ver Anexo 1.

[3] Ver Anexo 2.

[4] Ser una institución de prestigio y proyección nacional e internacional; de excelencia académica en el desarrollo y gestión del conocimiento. Centrada en la formación de profesionales, con valores fundamentados en la verdad; al servicio y transformación de la realidad social y económica, al **avance científico tecnológico** de la región, el país y el mundo.

Para que lo establecido en esta Política sea implementado, esta ha sido incluida como parte de la cultura organizacional de la Universidad, contando con el compromiso y apoyo de sus directivos para contribuir a la difusión, consolidación y cumplimiento.

Así mismo, con el propósito de que dicha implementación pueda realizarse en forma ordenada y gradual, la Universidad ha encomendado a su Comité de Ciberseguridad TIC[5], la tarea de elaborar y coordinar la ejecución de un Plan de Acción Anual o Plan Operativo Anual que fije los objetivos y determine plazos de realización de estos.

2. Propósito(s)

La **Política de Seguridad de la Información** se crea con el propósito de establecer los lineamientos que permitan *asegurar*, *proteger* y *salvaguardar* la información y los sistemas de la Universidad Central del Este, garantizando la *integridad*, *confidencialidad* y *disponibilidad* de la información, teniendo en cuenta la misión, visión y objetivos institucionales, así como, los estatutos, normativas y documentos legales vigentes que regulan la Universidad.

3. Alcance

La presente **Política de Seguridad de la Información** se desarrolla con el objetivo de gestionar adecuadamente los siguientes aspectos:

- Seguridad de la información.
- Sistemas de información.
- Control de activos.
- Seguridad del personal.
- Seguridad física y ambiental.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Administración de la continuidad de las actividades.
- Cumplimiento.

La Política es de aplicación para toda la comunidad universitaria: Administración, academia, investigación, extensión y vinculación, así como, toda persona que, de alguna manera, esté relacionada con la Universidad Central del Este y sea beneficiario/usuario de los servicios TIC.

Es importante destacar que esta debe ser conocida y cumplida por todo el personal del Departamento TIC y sus usuarios (grupos de interés), sea cual fuere su nivel jerárquico o nivel de incidencia.

4. Documentos de referencia

[5] Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la empresa que así lo requieran.

4.1. Marco legal

El componente normativo expone los lineamientos o disposiciones legales de la República Dominicana que guardan relación, orientan, sustentan y contribuyen a la estructuración de esta Política de Seguridad de la Información de la Universidad Central del Este.

A continuación, detalles del marco legal:

No.	Nombre	Descripción	Fecha
1	Ley No. 153-98	La Ley General de las Telecomunicaciones constituye el marco regulatorio básico que se ha de aplicar en todo el territorio nacional para regular la instalación, mantenimiento y operación de redes, la prestación de servicios y la provisión de equipos de telecomunicaciones.	27 de mayo del 1998
2	Ley No. 20-00	La Ley sobre la Propiedad Industrial es la que se encarga de la protección de los derechos relacionados a la propiedad industrial, contribuyendo con la creación y difusión de los avances de la tecnología, en beneficio recíproco de los productores y de los usuarios de conocimientos tecnológicos.	08 de mayo del 2000
3	Ley No. 139-01	Esta Ley crea el Sistema Nacional de Educación Superior, Ciencia y Tecnología y establece la normativa para su funcionamiento, los mecanismos que aseguran la calidad y la pertinencia de los servicios que prestan las instituciones que lo conforman y sienta las bases jurídicas para el desarrollo científico y tecnológico nacional.	13 de agosto del 2001
4	Ley No. 126-02	La Ley sobre Comercio Electrónico, Documentos y Firmas Digitales regula toda relación comercial, estructurada a partir de la utilización de uno o más documentos digitales o mensajes de datos o de cualquier otro medio similar.	04 de septiembre del 2002
5	Decreto No. 463-04	El Reglamento de las Instituciones de Educación Superior (IES) establece el conjunto de disposiciones y normas destinadas a definir el alcance y funcionamiento de las IES de la República Dominicana.	24 de mayo del 2004
6	Ley No. 53-07	La Ley contra Crímenes y Delitos de Alta Tecnología tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información y comunicación y su contenido, así como, la prevención y sanción de los delitos cometidos contra estos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas física o morales en los términos previstos en esta ley.	23 de abril del 2007
7	Ley No. 172-13	La Ley de Ciberseguridad de la Rep. Dom. tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados.	15 de diciembre del 2013

4.2. Términos y definiciones

Con el propósito de dar a entender los términos manejados en la formulación y creación de la Política de Seguridad de la Información, a continuación, se presentan unos conceptos claves, lo que permitirá una mejor interpretación de las informaciones:

4.2.1. Seguridad de la Información
Se entiende como la preservación de las siguientes características:

- Confidencialidad: Se garantiza que la información sea accesible solo 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.

Adicionalmente, deberán considerarse los conceptos de:

- Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: Consiste en asegurar que una transacción solo 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.
- No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto la empresa.
- Confiabilidad de la Información: Que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

4.2.2. 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.

4.2.3. 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.

4.2.4. Tecnología de la Información
Se refiere al hardware y software operados por la empresa o por un tercero que procese información en su nombre para llevar a cabo una función propia de la Universidad sin

tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

4.2.5. Comité de Ciberseguridad TIC

Es el departamento que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la empresa que así lo requieran.

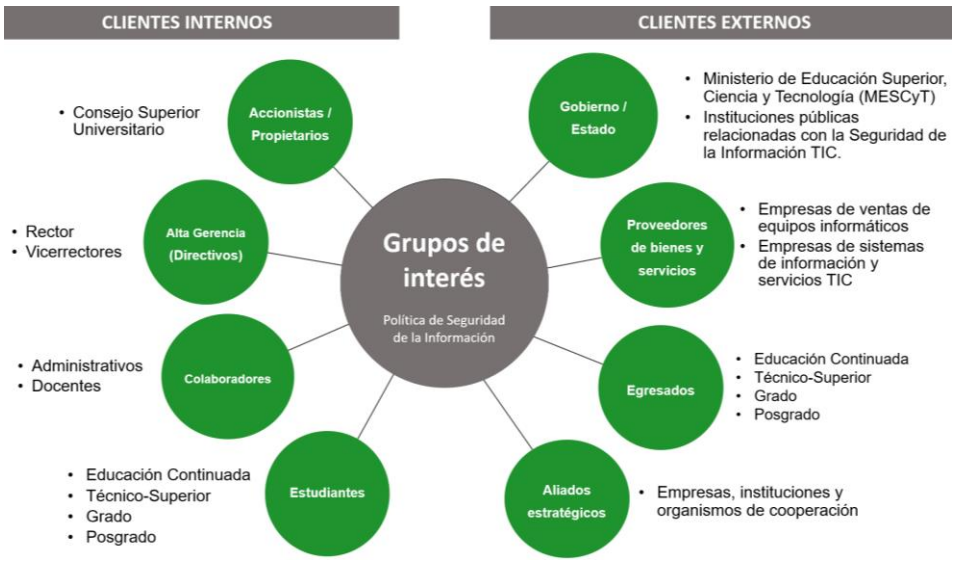
Comentado [WB1]: Verificar si persona es el termino correcto.

Comentado [RAT2R1]: Lo generalice

5. Grupos de interés

Los Grupos de interés o Stakeholders (en inglés) son grupos con poder real o potencial para influir en las decisiones de las organizaciones dentro de un espacio y tiempo delimitados para la existencia y desarrollo de un atributo tecnológico para una comunidad.

Los stakeholders de la Política de Seguridad de la Información de la Universidad Central del Este se clasifican en dos tipos de clientes: Internos y Externos. A continuación, se presenta un gráfico con los detalles de cada grupo:



6. Principios (aspectos específicos)

6.1. Organización de la Seguridad

6.1.1. Infraestructura de la Seguridad de la Información

- Comité de Ciberseguridad TIC: Destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

  Responsabilidades:
  - Posterior aprobación, revisar y ajustar periódicamente la Política de Seguridad de la Información y las funciones generales que fuesen convenientes y apropiadas para la Universidad.
  - Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Universidad frente a posibles amenazas, sean internas o externas.
  - Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información que se produzcan en el ámbito de la Universidad.
  - Aprobar las principales iniciativas para incrementar la seguridad de la información de acuerdo con las competencias y responsabilidades asignadas a cada sector, así como, acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
  - Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios de la Universidad, sean preexistente o nuevos.
  - Promover la difusión y apoyo a la seguridad de la información dentro de la Universidad, y coordinar el proceso de administración de la continuidad de las actividades.

- Asignación de Responsabilidades en Materia de Seguridad de la Información: El director del Departamento TIC de la Universidad Central del Este deberá asignar a un Ingeniero especializado, el cual ocupará el puesto de "Responsable de Seguridad Informática", para ejecutar las funciones relativas a la seguridad de los sistemas de información de la Universidad:

  - Control de accesos.
  - Seguridad en el desarrollo y mantenimiento de sistemas.
  - Planificación de la continuidad operativa.

  Así mismo, el Comité de Ciberseguridad TIC propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan, los cuales serán los responsables de las unidades organizativas a cargo del manejo de esta. Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones al personal idóneo a su cargo, estos conservarán la responsabilidad del cumplimiento de ellas. La delegación de la administración por parte de los

Comentado [WB3]: Verificar esta palabra, falta una 'e'

Comentado [RAT4R3]: Se la agrege

Comentado [WB5]: Cambiar por 'los cuales'

Comentado [RAT6R5]: Lo cambie

propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

- Proceso de Autorización para Instalaciones de Procesamiento de Información: Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, juntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes. Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Universidad.

- Asesoramiento Especializado en Materia de Seguridad de la Información: El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en la Universidad, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Este podrá obtener asesoramiento de otras empresas/instituciones/organismos.

- Cooperación entre Empresas/instituciones/organismos: A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con empresas, instituciones u organismos especializados en temas relativos a la seguridad informática.

- Revisión Independiente de la Seguridad de la Información: La Unidad de Auditoría Interna o, en su defecto, quien sea propuesto por el Comité de Ciberseguridad TIC realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la Universidad reflejen adecuadamente sus disposiciones.

Comentado [WB7]: Revisar

Comentado [RAT8R7]: Le deje la u por que suena mas logico

6.1.2. Seguridad Frente al Acceso por Parte de Terceros

- Identificación de Riesgos del Acceso de Terceras Partes: Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Universidad, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

    - El tipo de acceso requerido (físico/lógico y a qué recurso).
    - Los motivos para los cuales se solicita el acceso.
    - El valor de la información.
    - Los controles empleados por la tercera parte.
    - La incidencia de este acceso en la seguridad de la información de la Universidad.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la Universidad, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo, al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

- Requerimientos de Seguridad en Contratos o Acuerdos con Terceros: Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

    - Cumplimiento de la Política de Seguridad de la Información de la Universidad.
    - Protección de los activos de la Universidad, incluyendo:
        - Procedimientos para proteger los bienes de la Universidad, abarcando los activos físicos, la información y el software.
        - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
        - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia de este.
        - Restricciones a la copia y divulgación de información.
    - Descripción de los servicios disponibles.
    - Nivel de servicio esperado y niveles de servicio aceptables.
    - Permiso para la transferencia de personal cuando sea necesario.
    - Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
    - Existencia de Derechos de Propiedad Intelectual.
    - Definiciones relacionadas con la protección de datos.
    - Acuerdos de control de accesos que contemplen:
        - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
        - Proceso de autorización de accesos y privilegios de usuarios.
        - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
    - Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
    - Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de estos.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de estos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Relación entre proveedores y subcontratistas.

6.1.3. Tercerización

- Requerimientos de Seguridad en Contratos de Tercerización: Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC de la Universidad, contemplarán, además de los puntos especificados en "Requerimientos de Seguridad en Contratos o Acuerdos con Terceros", los siguientes aspectos:

  - Forma en que se cumplirán los requisitos legales aplicables.
  - Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
  - Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos de la Universidad.
  - Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la Universidad.
  - Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
  - Niveles de seguridad física que se asignarán al equipamiento tercerizado.
  - Derecho a la auditoría por parte de la Universidad sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc. Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

6.2. Clasificación y Control de Activos

Esta Política se aplica a toda la información administrada en la Universidad, cualquiera sea el soporte en que se encuentre. Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad; documentar y mantener

actualizada la clasificación efectuada; y definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan. Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

6.2.1. Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación para, luego, elaborar un inventario con dicha información. El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

6.2.2. Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad:

- Confidencialidad.
- Integridad.
- Disponibilidad.

6.2.3. Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo con el esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos, como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia.
- Almacenamiento.
- Transmisión por correo, fax, correo electrónico.
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

6.3. Seguridad del Personal

Esta Política se aplica a todo el personal de la Universidad, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito de la Universidad El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la Seguridad de la Información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de

Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como, su comunicación al Comité de Ciberseguridad TIC, a los propietarios de la información.

El Comité de Ciberseguridad TIC será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. A su vez, dicho Encargado, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la Universidad, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal de la Universidad es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

6.3.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

- Incorporación de la Seguridad en los Puestos de Trabajo: Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo. Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad de la Información y las responsabilidades específicas vinculadas a la protección de cada uno de los activos o la ejecución de procesos o actividades de seguridad determinadas.

- Control y Política del Personal: Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan a la Universidad.

- Compromiso de Confidencialidad: Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Universidad. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra unidad competente. Así mismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades

que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

- Términos y Condiciones de Empleo: Establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la Universidad y del horario normal de trabajo. Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

6.3.2. Capacitación del Usuario

- Formación y Capacitación en Materia de Seguridad de la Información: Todos los empleados de la Universidad y, cuando sea pertinente, los usuarios externos y terceros que desempeñen funciones en la Universidad recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la UCE. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como, la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como, por ejemplo, su estación de trabajo.

6.3.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad

- Comunicación de Incidentes Relativos a la Seguridad: Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática será informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. A su vez, mantendrá al Encargado de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

- Comunicación de Debilidades en Materia de Seguridad: Los usuarios de servicios de información, al momento de tomar conocimiento, directa o indirectamente, acerca de una debilidad de seguridad son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

- Comunicación de Anomalías del Software: Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

    - Registrar los síntomas del problema y los mensajes que aparecen en pantalla.

- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- Alertar inmediatamente al Responsable de Seguridad Informática o del Activo
- de que se trate.
- La recuperación será realizada por personal experimentado, adecuadamente habilitado.

- Aprendiendo de los Incidentes: Se definirá un proceso que permitirá documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

6.4. Seguridad Física y Ambiental

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Universidad: Instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

El Responsable de Seguridad Informática definirá junto con el Responsable del Departamento TIC y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente apartado.

El Responsable del Departamento TIC asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas y coordinará su implementación. A su vez, controlará el mantenimiento del equipamiento informático de acuerdo con las indicaciones de proveedores tanto dentro, como fuera de las instalaciones de la Universidad.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las áreas restringidas bajo su responsabilidad. Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la Universidad cuando lo crean conveniente.

Todo el personal de la Universidad es responsable del cumplimiento de la política de pantallas y escritorios limpios para la protección de la información relativa al trabajo diario en las oficinas.

6.4.1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de los recintos de la Universidad y de las instalaciones de procesamiento de información. La Universidad utilizará perímetros

de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, suministro de energía eléctrica, aire acondicionado y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Departamento TIC con el asesoramiento del Responsable de Seguridad Informática, de acuerdo con la evaluación de riesgos efectuada.

6.4.2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el Responsable del Departamento TIC, a fin de permitir el acceso solo al personal autorizado.

6.4.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También, se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas.

6.4.4. Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales que incluyan controles para el personal que trabaja en el área protegida, así como, para las actividades de terceros que tengan lugar allí.

6.4.5. Aislamiento de las Áreas de Recepción y Distribución

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

6.4.6. Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.

6.4.7. Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

6.4.8. Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

6.4.9. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

- La realización de tareas de mantenimiento preventivo al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Departamento TIC.
- El establecimiento de la práctica de que solo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- El registro de todas las fallas -supuestas y/o reales- y de todo el mantenimiento preventivo y correctivo realizado.
- El registro del retiro de equipamiento para su mantenimiento de la sede de la Universidad.
- La eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

6.4.10. Seguridad de los Equipos Fuera de las Instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Universidad será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de esta. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Universidad para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

6.4.11. Desafectación o Reutilización Segura de los Equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo, discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

6.4.12. Políticas de Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos

de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo, como fuera del mismo.

6.4.13. Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de la Universidad sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Universidad.

6.5. Gestión de las Comunicaciones y las Operaciones

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el Responsable del Departamento TIC, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo con su nivel de criticidad.

6.5.1. Procedimientos y Responsabilidades Operativas

- Documentación de los Procedimientos Operativos: Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

- Control de Cambios en las Operaciones: Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad. El Responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de estos ni de la información que soportan. El Responsable del Departamento TIC evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

- Procedimientos de Manejo de Incidentes: Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

- Separación de Funciones: Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas. En los casos en los que este método de control no pudiera cumplirse, se implementarán controles, tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

- Separación entre Instalaciones de Desarrollo e Instalaciones Operativas: Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados, preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

- Gestión de Instalaciones Externas: En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio que se incluirán en el contrato de tercerización.

6.5.2. Planificación y Aprobación de Sistemas

- Planificación de la Capacidad: El Responsable del Departamento TIC, o el personal que este designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello, tomará en cuenta, además, los nuevos requerimientos de los sistemas, así como, las tendencias actuales y proyectadas en el procesamiento de la información de la Universidad para el período estipulado de vida útil de cada componente. También, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento y puedan planificar una adecuada acción correctiva.

- Aprobación del Sistema: El Responsable del Departamento TIC y el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

6.5.3. Protección contra Software Malicioso

- Controles Contra Software Malicioso: El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Departamento TIC o el personal designado por este, implementará dichos controles. El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

6.5.4. Mantenimiento

- Resguardo de la Información: El Responsable del Departamento TIC y el de Seguridad Informática junto a los Propietarios de Información determinarán los

requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá un esquema de resguardo de la información.

- Registro de Actividades del Personal Operativo: El Responsable del Departamento TIC asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:
  - Tiempos de inicio y cierre del sistema.
  - Errores del sistema y medidas correctivas tomadas.
  - Intentos de acceso a sistemas, recursos o información crítica o acciones
  - Restringidas.
  - Ejecución de operaciones críticas.
  - Cambios a información crítica.

- Registro de Fallas: El Responsable del Departamento TIC desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones que permita tomar medidas correctivas.

6.5.5. Administración de la Red

- Controles de Redes: El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Universidad contra el acceso no autorizado. El Responsable del Departamento TIC implementará dichos controles.

6.5.6. Administración y Seguridad de los Medios de Almacenamiento

- Administración de Medios Informáticos Removibles: El Responsable del Departamento TIC, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como USB, discos, portátiles e informes impresos.
- Eliminación de Medios de Información: El Responsable del Departamento TIC, junto con el Responsable de Seguridad Informática definirán procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

- Procedimientos de Manejo de la Información: Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo con lo establecido en el principio 2 sobre “Clasificación y Control de Activos”.

- Seguridad de la Documentación del Sistema: La documentación del sistema puede contener información sensible, por lo que se considerarán los recaudos para su protección de almacenar la documentación del sistema en forma segura y restringir el acceso al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

6.5.7. Intercambios de Información y Software

- Acuerdos de Intercambio de Información y Software: Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Universidad y las consideraciones de seguridad sobre la misma.

- Seguridad de los Medios en Tránsito: Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiables, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

- Seguridad del Gobierno Electrónico: El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto "Aprobación del Sistema" incluyan, para las aplicaciones de Gobierno Electrónico, los siguientes aspectos:

    - *Autenticación:* Nivel de confianza recíproca suficiente sobre la identidad del usuario y la Universidad.
    - *Autorización:* Niveles de autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.
    - *Procesos de oferta y contratación pública:* Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
    - *Trámites en línea:* Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
    - *Verificación:* Grado de verificación apropiado para constatar la información suministrada por los usuarios.
    - *Cierre de la transacción:* Forma de interacción más adecuada para evitar fraudes.
    - *Protección a la duplicación:* Asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario.
    - *No repudio:* Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
    - *Responsabilidad:* Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

- Seguridad del Correo Electrónico:

- *Riesgos de Seguridad:* Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

  - La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
  - La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de estos.
  - Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, la confiabilidad y disponibilidad general del servicio.
  - La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
  - El impacto de un cambio en el medio de comunicación en los procesos.
  - Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
  - Las implicaciones de la publicación externa de listados de personal accesibles al público.
  - El acceso de usuarios remotos a las cuentas de correo electrónico.
  - El uso inadecuado por parte del personal.

- *Política de Correo Electrónico:* El Responsable de Seguridad Informática junto con el Responsable del Departamento TIC definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

  - Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
  - Protección de archivos adjuntos de correo electrónico.
  - Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver Controles Criptográficos).
  - Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
  - Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
  - Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
  - Definición de los alcances del uso del correo electrónico por parte del personal de la Universidad.

- *Seguridad de los Sistemas Electrónicos de Oficina:* Se controlarán los mecanismos de distribución y difusión, tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de

voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

- *Sistemas de Acceso Público:* Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

- *Otras Formas de Intercambio de Información:* Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

6.6. Control de Acceso

6.6.1. Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información:

- Registración de Usuarios: El Responsable de Seguridad Informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario,

- Administración de Privilegios: Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuarios que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.
- Administración de Contraseñas de Usuario: La asignación de contraseñas se controlará a través de un proceso de administración formal.

- Administración de Contraseñas Críticas: Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como hacer instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que solo 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. El Responsable de Seguridad Informática definirá procedimientos para la administración de dichas contraseñas críticas.

- Revisión de Derechos de Acceso de Usuarios: A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

6.6.2. Responsabilidades del Usuario

- Uso de Contraseñas: Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario y, consecuentemente, un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las directivas que se impartan a tal efecto.

- Equipos Desatendidos en Áreas de Usuarios: Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos. El Responsable de Seguridad Informática debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad para la protección de equipos desatendidos, así como, sus funciones en relación con la implementación de dicha protección.

6.6.3. Control de Acceso a la Red

- Política de Utilización de los Servicios de Red: Se controlará el acceso a los servicios de red tanto internos, como externos. El Responsable del Departamento TIC tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.
- Camino Forzado: El camino de las comunicaciones será controlado. Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder mediante la implementación de controles en diferentes puntos de esta.

- Autenticación de Usuarios para Conexiones Externas: El Responsable de Seguridad Informática juntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

- Autenticación de Nodos: Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Universidad. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas.

- Protección de los Puertos (Ports) de Diagnóstico Remoto: Los puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado.

- Subdivisión de Redes: Se definirán y documentarán los perímetros de seguridad convenientes que se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

- Acceso a Internet: Será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite y se definirán las pautas de utilización para todos los usuarios.

- Control de Conexión a la Red: Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo con las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los “gateways” que separan los diferentes dominios de la red.

- Control de Ruteo de Red: Se incorporarán controles de ruteo para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

- Seguridad de los Servicios de Red: El Responsable de Seguridad Informática junto con el Responsable del Departamento TIC definirán las pautas para garantizar la seguridad de los servicios de red de la Universidad tanto de los públicos, como los privados.

6.6.4. Control de Acceso al Sistema Operativo

- Identificación Automática de Terminales: El Responsable de Seguridad Informática junto con el Responsable del Departamento TIC realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

- Procedimientos de Conexión de Terminales: El acceso a los servicios de información solo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

- Identificación y Autenticación de los Usuarios: Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

- Sistema de Administración de Contraseñas: El sistema de administración de contraseñas debe:

    - Imponer el uso de contraseñas individuales para determinar responsabilidades.
    - Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de estas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
    - Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.
    - Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Uso de Contraseñas”.
    - Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
    - Mantener un registro de las últimas contraseñas utilizadas por el usuario y evitar la reutilización de estas.
    - Evitar mostrar las contraseñas en pantalla cuando son ingresadas.
    - Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
    - Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
    - Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, etc.).
    - Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

- Uso de Utilitarios de Sistema: Existen programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado.

- Alarmas Silenciosas para la Protección de los Usuarios: Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable de Seguridad Informática junto con el Responsable del Departamento TIC.

- Desconexión de Terminales por Tiempo Muerto: El Responsable de Seguridad Informática junto con los Propietarios de la Información de que se trate, definirán cuáles se consideran terminales de alto riesgo o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un período definido de inactividad, por un lapso que responderá a los riesgos de seguridad del área y de la información

que maneje la terminal. Para las PC's, se implementará la desconexión por tiempo muerto que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red. Por otro lado, si un usuario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas.

- Limitación del Horario de Conexión: Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente, aquellas terminales instaladas en ubicaciones de alto riesgo.

6.6.5. Control de Acceso a las Aplicaciones

- Restricción del Acceso a la Información: Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida sobre la base de los requerimientos de cada aplicación y conforme a lo establecido por la Universidad para el acceso a la información.

- Aislamiento de los Sistemas Sensibles: Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada que solo debe compartir recursos con los sistemas de aplicación confiables o no tener limitaciones.

6.6.6. Monitoreo del Acceso y Uso de los Sistemas

- Registro de Eventos: Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

- Monitoreo del Uso de los Sistemas:

    - *Procedimientos y Áreas de Riesgo:* Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información a fin de garantizar que los usuarios solo estén desempeñando actividades que hayan sido autorizadas explícitamente.

    - *Factores de Riesgo:* Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

- *Registro y Revisión de Eventos:* Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad Informática, de acuerdo con la evaluación de riesgos efectuada.

- Sincronización de Relojes: A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros deberán tener una correcta configuración de sus relojes. Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará, también, la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

6.6.7. Computación Móvil y Trabajo Remoto

- Computación Móvil: Se desarrollarán procedimientos adecuados para estos dispositivos que abarquen la protección física necesaria, el acceso seguro a los dispositivos, la utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios de la Universidad a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

- Trabajo Remoto: Solo será autorizado por el Responsable de la Unidad Organizativa o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, en conjunto con el Responsable de Seguridad Informática cuando se verifique que son adoptadas todas las medidas en materia de seguridad de la información para cumplir con la política, normas y procedimientos existentes.

6.7. Desarrollo y Mantenimiento de los Sistemas

Esta Política se aplica a todos los sistemas informáticos, tanto a desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Universidad en donde residan los desarrollos mencionados. El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Auditoría Interna definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad Informática definirá junto con el Responsable del Departamento TIC, los métodos de encriptación a ser utilizados.

6.7.1. Requerimientos de Seguridad de los Sistemas

- Análisis y Especificaciones de los Requerimientos de Seguridad: Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, así como, los controles manuales de apoyo.

6.7.2. Seguridad en los Sistemas de Aplicación

- Validación de Datos de Entrada: Se definirá un procedimiento que, durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando, también, datos permanentes y tablas de parámetros.

- Controles de Procesamiento Interno: Se definirá un procedimiento para que, durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

- Autenticación de Mensajes: Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán controles criptográficos.
- Validación de Datos de Salidas: Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

    - Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
    - Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
    - Provisión de información suficiente para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
    - Procedimientos para responder a las pruebas de validación de salidas.
    - Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

6.7.3. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

- Política de Utilización de Controles Criptográficos: Se utilizarán controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada fuera del ámbito de la Universidad.
- Para el resguardo de información, cuando así surja, de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad Informática.

- Cifrado: Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad Informática, se identificará el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

- Firma Digital: Se tomarán recaudos para proteger la confidencialidad de las claves privadas. A su vez, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

- Servicios de No Repudio: Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquel que haya originado una transacción electrónica niegue haberla efectuado.

- Administración de Claves

  - *Protección de Claves Criptográficas:* Se implementará un sistema de administración de claves criptográficas para respaldar su utilización por parte de la Universidad. Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada. Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

6.7.4. Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos de este.

- Control del Software Operativo: Toda aplicación desarrollada por la Universidad o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Departamento TIC. Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción. El Responsable del Departamento TIC propondrá, para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado.

- Protección de los Datos de Prueba del Sistema: Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos a tal efecto.

- Control de Cambios a Datos Operativos: La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos.

- Control de Acceso a las Bibliotecas de Programas Fuentes: El Responsable del Departamento TIC propondrá, para su aprobación por parte del superior jerárquico que corresponda, la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes.

6.7.5. Seguridad de los Procesos de Desarrollo y Soporte

- Procedimiento de Control de Cambios: Se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Estos garantizarán que se cumplan los procedimientos de seguridad y control respetando la división de funciones.

- Revisión Técnica de los Cambios en el Sistema Operativo: Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

- Restricción del Cambio de Paquetes de Software: La modificación de paquetes de software suministrados por proveedores, previa autorización del Responsable del Departamento TIC, deberá:

    - Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
    - Determinar la conveniencia de que la modificación sea efectuada por la Universidad, por el proveedor o por un tercero.
    - Evaluar el impacto que se produce si la Universidad se hace cargo del mantenimiento.
    - Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

- Canales Ocultos y Código Malicioso: Se redactarán normas y procedimientos que incluyan:

    - Adquirir programas a proveedores acreditados o productos ya evaluados.

- Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
- Controlar el acceso y las modificaciones al código instalado.
- Utilizar herramientas para la protección contra la infección del software con código malicioso.

- Desarrollo Externo de Software: Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

  - Acuerdos de licencias, propiedad de código y derechos conferidos.
  - Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
  - Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
  - Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto de Requerimientos de Seguridad en Contratos de Tercerización.
  - Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

6.8. Administración de la Continuidad de las Actividades de la Universidad

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la Universidad.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Universidad.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Universidad.

6.8.1. Proceso de la Administración de la Continuidad de la Universidad

El Comité de Ciberseguridad TIC será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la Universidad.

6.8.2. Continuidad de las Actividades y Análisis de los Impactos

Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la Universidad que contemple los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño, como del período de recuperación.
- Identificar los controles preventivos.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades de la Universidad y no limitándose a las instalaciones de procesamiento de la información.

6.8.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades de la Universidad

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Universidad. Estos procesos deberán ser propuestos por el Comité de Ciberseguridad TIC.

6.8.4. Marco para la Planificación de la Continuidad de las Actividades de la Universidad

Se mantendrá un solo marco para los planes de continuidad de las actividades de la Universidad, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento. Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como, las personas a cargo de ejecutar cada componente de este. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

6.8.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la Universidad

El Comité de Ciberseguridad TIC establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

7. Objetivos

Los objetivos establecidos para guiar esta Política de Seguridad de la Información de la Universidad Central del Este son:

Generales

1. Proteger los recursos de información de la Universidad y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
2. Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
3. Mantener esta Política actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Organización de la Seguridad

1. Administrar la seguridad de la información dentro de la Universidad y establecer un marco gerencial para iniciar y controlar su implementación, así como, para la distribución de funciones y responsabilidades.
2. Fomentar la consulta y cooperación con empresas y/o instituciones especializadas para la obtención de asesoría en materia de seguridad de la información.
3. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Universidad.

Clasificación y Control de Activos

1. Garantizar que los activos de información reciban un apropiado nivel de protección.

2. Clasificar la información para señalar su sensibilidad y criticidad.
3. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Seguridad del Personal

1. Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
2. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
3. Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información y se encuentren capacitados para respaldar esta Política en el transcurso de sus tareas normales.
4. Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
5. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como, los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Seguridad Física y Ambiental

1. Proteger el equipamiento de procesamiento de información crítica de la Universidad, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección de este su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
2. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Universidad.

Gestión de Comunicaciones y Operaciones

1. Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
2. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Control de Accesos

1. Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información e implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
2. Controlar la seguridad en la conexión entre la red de la Universidad y otras redes públicas o privadas; y garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.
3. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas; y concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Desarrollo y Mantenimiento de Sistemas

1. Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
2. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
3. Definir los métodos de protección de la información crítica o sensible.

Administración de la Continuidad de las Actividades de la Universidad

1. Minimizar los efectos de las posibles interrupciones de las actividades normales de la Universidad (sean estas el resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
2. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
3. Maximizar la efectividad de las operaciones de contingencia de la Universidad con el establecimiento de planes y asegurar la coordinación con el personal de la Universidad y los contactos externos que participarán en estos planes.

8. Frecuencia de revisión, modificación y aprobación

Frecuencia de revisión, modificación y cumplimiento: La presente política deberá ser revisada cada dos (2) años por el Comité de Ciberseguridad TIC con el fin de supervisar su cumplimiento, mantenerla actualizada y efectuar toda modificación necesaria en función de posibles cambios que puedan afectar su definición, tales como: Cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, entre otros.

Cada Responsable de Unidad Organizativa velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos dentro de su área de responsabilidad.

El Responsable de Seguridad Informática realizará revisiones periódicas de todas las áreas de la Universidad a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- Sistemas de información.
- Proveedores de sistemas.
- Propietarios de información.
- Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

Aprobación y comunicación: La presente política es aprobada por el Consejo Superior Universitario de la Universidad Central del Este, siguiendo los estatutos, normativas y documentos oficiales de esta. Estará disponible en las plataformas digitales de la Universidad

para todos los grupos de interés. A su vez, esta Política será objeto de las adecuadas acciones de comunicación, formación y sensibilización para su oportuna comprensión y puesta en práctica.

Sanciones previstas por incumplimiento: El incumplimiento de las disposiciones establecidas por la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

	PREPARADA POR	REVISADA POR	APROBADA POR
Nombre	Leandro de la Rosa		
Cargo	Director		
Departamento	Tecnologías de la Información y Comunicaciones		
Firma			
Fecha			

9. Anexos

- Anexo 1: Descripción del Sistema de Información, UCE TIC
- Anexo 2: Plan quinquenal UCE (2018-2022)
- Anexo 3: Políticas de Ciberseguridad, UCE TIC 2020
- Anexo 4: Política de Uso de correo electrónico, UCE TIC
- Anexo 5: Políticas de Acceso Físico, UCE TIC
- Anexo 6: Políticas de Respaldo-Backup, UCE TIC
- Anexo 7: Políticas uso de thin clients y mini pcs, UCE TIC
- Anexo 8: Política de acceso remoto, UCE TIC
- Anexo 9: Política de seguridad de router, switch y dispositivos de interconexión, UCE TIC
- Anexo 10: Políticas de administraticón de usuarios y manejo de credenciales, UCE TIC