



TECNOLÓGICO
UNIVERSITARIO
PICHINCHA



GUÍA PRÁCTICA ASIGNATURA SOFTWARE APLICADO

Tema:

Uso de sistemas de
Recursos Humanos



Carrera:

Tecnología Superior en
Gestión del Talento Humano

1.- Datos generales:



1.1 Asignatura: Software Aplicado

1.2 Nivel académico: Tercero

1.3 Docente Responsable: Cristian López C

2.- Datos específicos:



2.1 Título de la Práctica: Uso de sistemas de Recursos Humanos.



2.2 Tiempo de duración: 30-45 minutos diario.

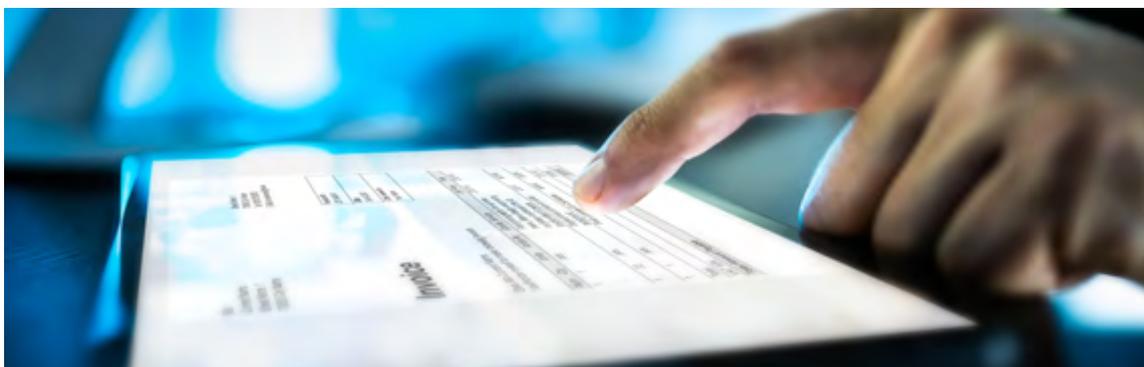


2.3 Objetivo de la práctica: Conocer el manejo de un sistema de Recursos Humanos.

2.4 Resultado de aprendizaje de la asignatura que tributa a la práctica:



El estudiante manejará los módulos de un sistema de recursos humanos ingresará información, modificará esta y configurará algunos elementos importantes para el control del recurso humano de una organización.





3.- Materiales, recursos y equipos



- PC de laboratorio.
- Equipo portátil si el estudiante desea traer su propio equipo.
- Correo Institucional.
- Acceso a internet.

4.- Normas de seguridad para laboratorios de informática:

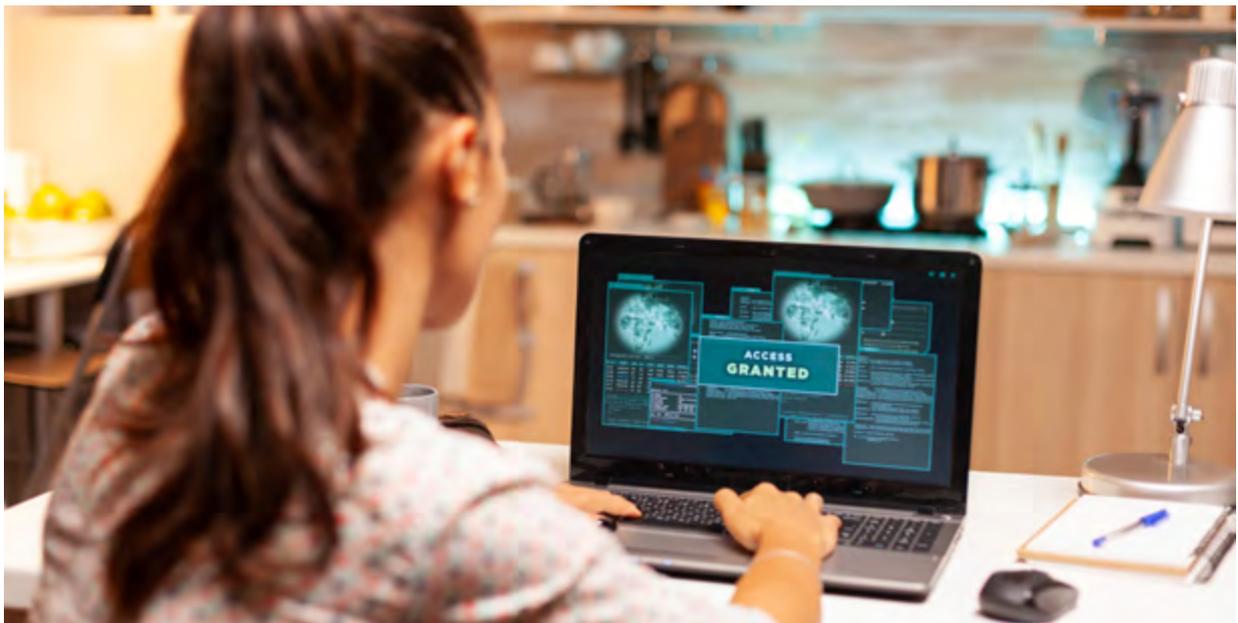


1. Seguridad General

- **Acceso restringido.** - Solo estudiantes y personal autorizado pueden ingresar a los laboratorios de informática.
- **Identificación.** - Todos los usuarios deben portar la identificación visible de la institución.
- **Limpieza.** - Mantener el área de trabajo limpia y libre de polvo y obstáculos que impidan libre circulación de estudiantes.
- **Orden.** - Asegurarse que los cables y accesorios en los cubículos estén organizados y no representen un riesgo de tropiezo o afecten el correcto funcionamiento del laboratorio
- **Equipamiento y Ergonomía.** - Uso de sillas y mesas ergonómicas para prevenir problemas musculoesqueléticos. Ajustar la altura de pantallas para que estén a la altura de la visual del usuario.
- **Ventilación y Temperatura.** - Asegurar la ventilación adecuada y mantener una temperatura confortable al interior del laboratorio y que adicionalmente cuide el correcto funcionamiento de los equipos de informática.
- **Prohibición de Alimentos y Bebidas.** - No se permite consumir alimentos o bebidas en los laboratorios, para evitar daños a los equipos electrónicos.
- **Emergencias.** - Conocer de la ubicación exacta de extintores, salidas de emergencia, puntos de encuentro y botiquín de primeros auxilios.

2. Uso de Hardware y Software

- **Inspección de Equipos.** - Con regularidad se inspeccionarán el buen estado de cables y conexiones eléctricas. No se deben utilizar cables o equipos con defectos o dañados.
- **Uso de Equipos Eléctricos y Electrónicos.** - Verificar las conexiones que no se encuentren sobrecargadas por enchufes y utilizar regletas de protección. Desconectar equipos de la fuente eléctrica cuando no se encuentren en uso o no se estén utilizando.
- **Hardware.** - Apagar y desconectar los equipos antes de realizar cualquier mantenimiento o modificación.
- **Manejo de Equipos.** – Manipular equipos (computadoras, impresoras, TVs, pantallas, monitores y hardware en general) con cuidado y siguiendo las instrucciones del personal de soporte informático responsable.
- **Software Autorizado.** – No modificar, desinstalar, o instalar software sin autorización previa del personal de Soporte para evitar la introducción de virus o la alteración del funcionamiento de equipos informáticos.
- **Actualizaciones.** – El Mantenimiento y actualización de los sistemas operativos y software necesario, será exclusivamente responsabilidad de personal autorizado.
- **Cierre de sesión.** - Al finalizar la sesión, cerrar todos los programas y apagar el equipo adecuadamente para proteger la información personal y asegurar el correcto funcionamiento del sistema para el siguiente usuario.
- **Comportamiento adecuado:** Mantener un comportamiento respetuoso dentro del laboratorio, evitando ruido excesivo, correr o realizar actividades que puedan distraer a otros usuarios o causar accidente.





3. Seguridad Digital y de Datos

- **Contraseñas.** – Utilizar contraseñas fuertes y cambiarlas regularmente.
- **Almacenamiento Seguro.** – Guardar los datos sensibles en ubicaciones seguras y respaldar información importante.
- **Privacidad.** – No compartir información personal o académica de otros usuarios sin autorización.
- **Acceso Remoto.** – Utilizar conexiones seguras, Red Privada Virtual (VPN) de ser el caso, para acceso remoto a los sistemas del laboratorio.
- **Software Autorizado.** - Instalar software autorizado y mantener los programas y sistemas operativos actualizados con los últimos parches de seguridad.
- **Antivirus.** – Mantenimiento y análisis de equipos con antivirus y firewalls, así como su actualización y funcionamiento, será responsabilidad exclusiva de personal autorizado.
- **Copia de Seguridad.** - Realizar copias de seguridad regularmente de los datos importantes y almacenarlas en ubicaciones seguras.

4. Conducta y Ética Profesional

- **Internet.** - Utilizar el internet únicamente para fines académicos. Está prohibido navegar por sitios inapropiados o realizar actividades que no estén relacionadas con el trabajo académico.
- **Propiedad Intelectual.** - No plagiar ni usar software sin licencia, además de respetar las políticas de copyright.
- **Confidencialidad.** - Mantener la confidencialidad de la información y de los datos involucrados en los proyectos de estudiantes. No acceder, ni modificar, ni divulgar información sin autorización.

5. Manejo de Equipos y Herramientas

- **Manipulación de Componentes.** - Utilizar pulseras antiestáticas para manipular componentes electrónicos que garanticen la no presencia de electricidad estática.

No forzar las conexiones y asegurarse de que todas las piezas estén bien conectadas y ensambladas y siempre debidamente supervisado por el docente.

- **Herramientas Adecuadas.** - Utilizar las herramientas que son asignadas a cada tarea y asegurarse de que su estado sea óptimo para el correcto uso.
- **Manuales.** - Familiarizarse o recibir capacitación con los manuales de instrucciones de los equipos y herramientas antes de utilizarlos.



6. Protocolos y Laboratorios

- **Supervisión y Horarios.** - Respetar los horarios de uso del laboratorio y garantizar que siempre tienen supervisión de un docente o personal autorizado.
- **Registros.** - Las actividades realizadas al interior del laboratorio, llevarán un registro que incluye a los equipos utilizados y cualquier incidente o problema encontrado.
- **Problemas o Imprevistos.** - Informar cualquier problema técnico o de seguridad al personal responsable del laboratorio.

7. Plan de Emergencia

- **Evacuación.** – Conocer las rutas de evacuación, ubicación de extintores y puntos de encuentro en caso de emergencia. (incendio, terrorismo, sismo, etc....).
- **Respuesta Primera.** - Los estudiantes y personal que labora deberán saber cómo reaccionar a situaciones de emergencia, como cortes eléctricos, problemas de hardware o incidentes de ciberseguridad.
- **Primeros Auxilios.** – Informarse sobre la ubicación del botiquín de primeros auxilios y como acceder a la asistencia médica.
- **Cortes de Energía.** – Desconectar los equipos, así como evitar el contacto con conductores expuestos o puntos eléctricos y seguir las instrucciones del personal, en caso de suspensión o corte de energía para evitar descargas eléctricas.
- **Contacto de Emergencia.** - Tener acceso a los números de emergencia y servicios de emergencia y los procedimientos a seguir en caso de incidentes graves

LEER NORMAS



5.- Preparación previa:



El estudiante deberá revisar los enlaces que se encuentran dentro de la guía práctica para conocer los módulos con los que cuenta la aplicación, deberá tener acceso a su correo institucional para verificar la cuenta creada dentro del sistema.

1. Prerrequisitos:

- Manejo básico del PC
- Uso de navegadores web
- Manejo de correo electrónico

2. Conceptos básicos:

- **Sistemas Informático:** Conjunto integrado de hardware, software, datos y personas que trabajan de manera coordinada para recolectar, procesar, almacenar y distribuir información. Estos sistemas están diseñados para facilitar la ejecución de tareas específicas, como la automatización de procesos, la toma de decisiones, la comunicación o la gestión de información dentro de una organización o entorno particular.
- **Hardware:** Incluye todos los componentes físicos del sistema, como computadoras, servidores, dispositivos de almacenamiento, impresoras y redes de comunicación.
- **Software:** Comprende los programas y aplicaciones que ejecutan instrucciones para procesar datos.
- **Datos:** Es la información que el sistema utiliza, procesa y produce, y puede estar en diferentes formatos (numérico, textual, multimedia, etc.).
- **Usuarios:** Son quienes interactúan con el sistema, ya sea para administrarlo (como los técnicos) o para utilizarlo en actividades específicas (como los usuarios finales).
- **Procesos:** Son los procedimientos y reglas que definen cómo interactúan los componentes del sistema para cumplir con sus objetivos.
- **Sistema de recursos humanos:** Conjunto de herramientas y procesos informáticos diseñados para gestionar, automatizar y optimizar las actividades relacionadas con la administración del personal en una organización. Su objetivo principal es centralizar la información del talento humano y facilitar tareas administrativas, operativas y estratégicas relacionadas con el ciclo de vida del empleado, desde la contratación hasta la desvinculación.

6.- Descripción de la actividad práctica o descripción de procedimientos



Procedimiento Detallado

Clase 3 a 4

1. Abrir el navegador web y digitar SAGE HR o accede al siguiente enlace <https://www.sage.com/es-es/sage-business-cloud/hr>
2. Creará una cuenta con su correo institucional la cual le servirá para el registro y acceso al sistema.
3. Escogerá los módulos que van a ir dentro de la prueba del sistema antes de su registro.
4. Dentro del sistema en el menú compañía primero editará su perfil colocando los datos y luego la foto de perfil.
5. Una vez realizado esto procederá dentro del módulo personal a ingresar datos de 5 compañeros que fungirán como empleados de este.

Clase 4 a 5

6. En el módulo feedback 360 configurará una evaluación 360 grados con la ayuda de la IA.
7. Creará el formulario en base a las preguntas que le proporcione la IA.
8. El formulario deberá contener mínimo 10 temas de evaluación con 2 preguntas como máximo de lo que vaya a evaluar y dependiendo de la empresa que haya escogido.
9. Utilizará uno de los módulos del sistema y procederá a detallar su funcionamiento dentro del informe solicitado.
10. La entrega se realizará en una actividad cargada en el EVA del ISTP-U en formato PDF.



7.- Mecanismo de evaluación y anexos:



Instrucciones:

La presente lista de cotejo sirve para la observación estructurada o sistemática del procedimiento realizado.

Solo se indica si el paso del procedimiento se realiza o no, sin admitir valores intermedios.

En los casos en que el paso del procedimiento haya sido realizado, con la observación que se deba mejorar algún aspecto de este, esto se consignará en la columna de observaciones.

Calificación:

A cada paso del procedimiento se le asignará el valor de 1 punto, en caso de que no realice la calificación sería 0.

Para la calificación final se tomará en cuenta la puntuación de la tabla de calificación adjunta a la lista de cotejo.

Nombre y apellidos del estudiante:

Nombre y apellidos del docente:

Fecha:

Describa los pasos a seguir en la actividad práctica

DESCRIBA LOS PASOS A SEGUIR	
PASO 1	
PASO 2	
PASO 3	
PASO 4	
PASO 5	
PASO 6	



NORMAS DE SEGURIDAD PARA LABORATORIOS DE INFORMÁTICA

1. Seguridad General

- **Acceso restringido.** - Solo estudiantes y personal autorizado pueden ingresar a los laboratorios de informática.
- **Identificación.** - Todos los usuarios deben portar la identificación visible de la institución.
- **Limpieza.** - Mantener el área de trabajo limpia y libre de polvo y obstáculos que impidan libre circulación de estudiantes.
- **Orden.** - Asegurarse que los cables y accesorios en los cubículos estén organizados y no representen un riesgo de tropiezo o afecten el correcto funcionamiento del laboratorio.
- **Equipamiento y Ergonomía.** - Uso de sillas y mesas ergonómicas para prevenir problemas musculoesqueléticos. Ajustar la altura de pantallas para que estén a la altura de la visual del usuario.
- **Ventilación y Temperatura.** - Asegurar la ventilación adecuada y mantener una temperatura confortable al interior del laboratorio y que adicionalmente cuide el correcto funcionamiento de los equipos de informática.
- **Prohibición de Alimentos y Bebidas.** - No se permite consumir alimentos o bebidas en los laboratorios, para evitar daños a los equipos electrónicos.
- **Emergencias.** - Conocer de la ubicación exacta de extintores, salidas de emergencia, puntos de encuentro y botiquín de primeros auxilios.



NORMAS DE SEGURIDAD PARA LABORATORIOS DE INFORMÁTICA

2. Uso de Hardware y Software

- **Inspección de Equipos.** - Con regularidad se inspeccionarán el buen estado de cables y conexiones eléctricas. No se deben utilizar cables o equipos con defectos o dañados.
- **Uso de Equipos Eléctricos y Electrónicos.** - Verificar las conexiones que no se encuentren sobrecargadas por enchufes y utilizar regletas de protección. Desconectar equipos de la fuente eléctrica cuando no se encuentren en uso o no se estén utilizando.
- **Hardware.** - Apagar y desconectar los equipos antes de realizar cualquier mantenimiento o modificación.
- **Manejo de Equipos.** - Manipular equipos (computadoras, impresoras, TVs, pantallas, monitores y hardware en general) con cuidado y siguiendo las instrucciones del personal de soporte informático responsable.
- **Software Autorizado.** - No modificar, desinstalar, o instalar software sin autorización previa del personal de Soporte para evitar la introducción de virus o la alteración del funcionamiento de equipos informáticos.
- **Actualizaciones.** - El Mantenimiento y actualización de los sistemas operativos y software necesario, será exclusivamente responsabilidad de personal autorizado.
- **Cierre de sesión.** - Al finalizar la sesión, cerrar todos los programas y apagar el equipo adecuadamente para proteger la información personal y asegurar el correcto funcionamiento del sistema para el siguiente usuario.
- **Comportamiento adecuado:** Mantener un comportamiento respetuoso dentro del laboratorio, evitando ruido excesivo, correr o realizar actividades que puedan distraer a otros usuarios o causar accidentes.



NORMAS DE SEGURIDAD PARA LABORATORIOS DE INFORMÁTICA

3. Seguridad Digital y de Datos

- **Contraseñas.** – Utilizar contraseñas fuertes y cambiarlas regularmente.
- **Almacenamiento Seguro.** – Guardar los datos sensibles en ubicaciones seguras y respaldar información importante.
- **Privacidad.** – No compartir información personal o académica de otros usuarios sin autorización.
- **Acceso Remoto.** – Utilizar conexiones seguras, Red Privada Virtual (VPN) de ser el caso, para acceso remoto a los sistemas del laboratorio.
- **Software Autorizado.** - Instalar software autorizado y mantener los programas y sistemas operativos actualizados con los últimos parches de seguridad.
- **Antivirus.** – Mantenimiento y análisis de equipos con antivirus y firewalls, así como su actualización y funcionamiento, será responsabilidad exclusiva de personal autorizado.
- **Copia de Seguridad.** - Realizar copias de seguridad regularmente de los datos importantes y almacenarlas en ubicaciones seguras.

4. Conducta y Ética Profesional

- **Internet.** - Utilizar el internet únicamente para fines académicos. Está prohibido navegar por sitios inapropiados o realizar actividades que no estén relacionadas con el trabajo académico.
- **Propiedad Intelectual.** - No plagiar ni usar software sin licencia, además de respetar las políticas de copyright.
- **Confidencialidad.** - Mantener la confidencialidad de la información y de los datos involucrados en los proyectos de estudiantes. No acceder, ni modificar, ni divulgar información sin autorización.



NORMAS DE SEGURIDAD PARA LABORATORIOS DE INFORMÁTICA

5. Manejo de Equipos y Herramientas

- **Manipulación de Componentes.** - Utilizar pulseras antiestáticas para manipular componentes electrónicos que garanticen la no presencia de electricidad estática. No forzar las conexiones y asegurarse de que todas las piezas estén bien conectadas y ensambladas y siempre debidamente supervisado por el docente.
- **Herramientas Adecuadas.** - Utilizar las herramientas que son asignadas a cada tarea y asegurarse de que su estado sea óptimo para el correcto uso.
- **Manuales.** - Familiarizarse o recibir capacitación con los manuales de instrucciones de los equipos y herramientas antes de utilizarlos.

6. Protocolos y Laboratorios

- **Supervisión y Horarios.** - Respetar los horarios de uso del laboratorio y garantizar que siempre tienen supervisión de un docente o personal autorizado.
- **Registros.** - Las actividades realizadas al interior del laboratorio, llevarán un registro que incluye a los equipos utilizados y cualquier incidente o problema encontrado.
- **Problemas o Imprevistos.** - Informar cualquier problema técnico o de seguridad al personal responsable del laboratorio.



NORMAS DE SEGURIDAD PARA LABORATORIOS DE INFORMÁTICA

7. Plan de Emergencia

- **Evacuación.** – Conocer las rutas de evacuación, ubicación de extintores y puntos de encuentro en caso de emergencia. (incendio, terrorismo, sismo, etc....).
- **Respuesta Primera.** - Los estudiantes y personal que labora deberán saber cómo reaccionar a situaciones de emergencia, como cortes eléctricos, problemas de hardware o incidentes de ciberseguridad.
- **Primeros Auxilios.** – Informarse sobre la ubicación del botiquín de primeros auxilios y como acceder a la asistencia médica.
- **Cortes de Energía.** – Desconectar los equipos, así como evitar el contacto con conductores expuestos o puntos eléctricos y seguir las instrucciones del personal, en caso de suspensión o corte de energía para evitar descargas eléctricas.
- **Contacto de Emergencia.** - Tener acceso a los números de emergencia y servicios de emergencia y los procedimientos a seguir en caso de incidentes graves.

<https://www.tecnologicopichincha.edu.ec/>



TECNOLÓGICO
UNIVERSITARIO
PICHINCHA

