**Acanner**

**Plan de Respaldo de datos**

**Página de control de revisiones**

| **Fecha** | **Resumen de cambios realizados** | **Cambios realizados por (Nombres y Apellidos)** |
| --- | --- | --- |
| 12/03/2024 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Propósito**

El propósito del sistema de información web (Planner) es facilitar la gestión eficiente de actividades académicas relacionadas con la formación ADSO en la ficha 2558104. Este sistema tiene como objetivo principal proporcionar a estudiantes, profesores y administradores una plataforma centralizada para el seguimiento de tareas, registro de asistencia y comunicación, mejorando así la organización, la colaboración y el rendimiento académico.

**Alcance del Sistema de Información Web (Planner):**

El alcance del sistema se limita a las actividades académicas relacionadas con la formación ADSO y abarca las siguientes funcionalidades:

**Gestión de Tareas:**

1. **Creación, edición y eliminación de tareas.**

**-** Asignación de tareas a estudiantes con fechas de vencimiento.

1. **Registro de Asistencia:**

* Registro electrónico de asistencia para clases, seminarios u otros eventos académicos.
* Generación de informes de asistencia para estudiantes y profesores.

1. **Calendario:**

* Visualización de eventos académicos, fechas límite y actividades planificadas.
* Recordatorios y notificaciones para eventos próximos.

1. **Comunicación:**

* Sistema de mensajería interna para facilitar la comunicación entre estudiantes y profesores.
* Foros o tableros de discusión para intercambio de información relevante.

1. **Informes y Estadísticas:**

* Generación de informes de progreso académico individual para estudiantes.
* Estadísticas agregadas sobre asistencia y rendimiento académico.

**Objetivos del Sistema de Información Web (Planner) Acanner:**

1. **Gestión Efectiva de Actividades Académicas:**

* Facilitar la organización y gestión eficiente de las actividades académicas relacionadas con la formación ADSO en la ficha 2558104.

1. **Seguimiento de Tareas:**

* Proporcionar una funcionalidad robusta para el seguimiento de tareas, permitiendo a estudiantes y profesores mantenerse al tanto de las asignaciones pendientes y fechas de vencimiento.

1. **Registro de Asistencia Automatizado:**

* Implementar un sistema automatizado para el registro de asistencia, simplificando el seguimiento de la participación de los estudiantes en clases, seminarios y otros eventos académicos.

1. **Colaboración y Comunicación:**

* Fomentar la colaboración entre estudiantes y profesores mediante funciones de comunicación integradas, como mensajería interna, foros o tableros de discusión.

1. **Integración Temática (ADSO):**

* Alinear el sistema con las temáticas específicas de la formación ADSO, asegurando que las funcionalidades y características se adapten a las necesidades particulares de este programa educativo.

1. **Interfaz Intuitiva y Fácil de Usar:**

* Desarrollar una interfaz de usuario intuitiva y fácil de usar para garantizar la accesibilidad y aceptación por parte de estudiantes, profesores y administradores.

1. **Flexibilidad y Adaptabilidad:**

* Diseñar el sistema con la flexibilidad necesaria para adaptarse a cambios en los requisitos académicos y procesos de la formación ADSO.

1. **Seguridad de Datos:  
   -** Implementar medidas de seguridad sólidas para proteger la información sensible, garantizando la privacidad y confidencialidad de los datos académicos.
2. **Generación de Informes y Estadísticas:**

* Facilitar la generación de informes y estadísticas sobre el progreso académico, asistencia y otros indicadores relevantes para evaluar el rendimiento individual y colectivo.

1. **Cumplimiento Normativo:**

* Asegurar que el sistema cumpla con las regulaciones y normativas pertinentes en cuanto a la gestión de datos académicos y la privacidad de los usuarios.

***Supuestos***

• Los empleados clave de respaldo de datos de TI estarán disponibles luego de un desastre.

• Los sistemas de respaldo de datos y las herramientas de recuperación estarán disponibles y funcionales después de un desastre:

•Los proveedores de servicios de almacenamiento en la nube o de infraestructura estarán disponibles y operativos para respaldar la infraestructura de respaldo de datos en caso de un desastre

***Definición de desastre***

Un desastre se define como cualquier evento o situación que cause una interrupción significativa en las operaciones normales de la tecnología de la información (TI) y que afecte la disponibilidad, integridad o confidencialidad de los datos y sistemas críticos. Esto puede incluir, pero no se limita a, cortes de energía prolongados, fallas graves del sistema, incendios, inundaciones, terremotos, ciberataques, actos de sabotaje, entre otros eventos catastróficos o disruptivos.

• Equipo de respaldo de datos

• Equipo de soporte técnico de TI

***Responsabilidades de los miembros del equipo***

*Responsabilidades de Allison (Líder del Equipo):*

* Designar Suplentes: Allison designará a un suplente para cada miembro del equipo, asegurando que haya cobertura en caso de ausencia de algún miembro del equipo principal.
* Mantener el Plan como Referencia: Allison asegurará que todos los miembros del equipo tengan una copia del plan de respaldo de datos y lo mantendrá como referencia en casa, en caso de que ocurra una interrupción después del horario normal de trabajo.
* Familiarizarse con el Contenido del Plan: Allison se asegurará de que todos los miembros del equipo estén familiarizados con el contenido del plan de respaldo de datos y comprendan sus roles y responsabilidades en caso de un desastre.

*Responsabilidades de Katalina y Marlon (Miembros del Equipo):*

* Designar Suplentes: Katalina y Marlon designarán a un suplente cada uno, según las instrucciones de Allison, para garantizar la cobertura completa del equipo en caso de ausencia.
* Monitoreo de Actividades de Respuesta: Katalina estará a cargo de monitorear y registrar las actividades de respuesta durante y después de un desastre, manteniendo un registro detallado de las acciones tomadas y cualquier problema encontrado.
* Gestión de Recursos Adicionales: Katalina se encargará de identificar y solicitar recursos adicionales que puedan ser necesarios para la recuperación de datos, como personal adicional, hardware o software específico, según las necesidades del equipo.
* Pruebas y Mantenimiento de Equipos de Respuesta: Marlon será responsable de realizar pruebas regulares y mantener en condiciones óptimas los equipos y herramientas utilizados para la recuperación de datos, como los dispositivos de almacenamiento, los servidores de respaldo, etc.
* Evaluación de Riesgos y Vulnerabilidades: Marlon estará a cargo de evaluar y documentar los riesgos y vulnerabilidades potenciales en el sistema de respaldo de datos, proponiendo medidas correctivas y mejoras para mitigar dichos riesgos.
* Capacitación y Concienciación del Personal: Marlon y Katalina se encargarán de organizar sesiones de capacitación y concienciación para el personal sobre las mejores prácticas de respaldo de datos, seguridad informática y procedimientos de respuesta ante desastres.

**Política de respaldo**

Las copias de seguridad completas e incrementales protegen y preservan la información de la red corporativa y deben realizarse con regularidad para los registros del sistema y los documentos técnicos que no se reemplazan fácilmente, tienen un alto costo de reemplazo o se consideran críticos. Los medios de respaldo deben almacenarse en un lugar seguro, geográficamente separado del original y aislado de los peligros ambientales. Los componentes de la red de respaldo, el cableado y los conectores, las fuentes de alimentación, las piezas de repuesto y la documentación relevante deben almacenarse en un área segura en el sitio, así como en otras ubicaciones corporativas.

Las políticas de retención de datos y documentos se establecen para especificar qué registros deben conservarse y durante cuánto tiempo. Todos los departamentos son responsables de especificar su gestión de datos, retención de datos, destrucción de datos y requisitos generales de gestión de registros.

El soporte técnico de TI sigue estos estándares para la copia de seguridad y el archivo de datos:

**Bases de datos del sistema**

• Se debe realizar una copia de las bases de datos de misión crítica más actualizadas al menos dos veces al mes, o según la frecuencia de los cambios realizados.

• Las copias de seguridad deben almacenarse fuera del sitio.

• El administrador de datos principal es responsable de esta actividad.

**Datos de misión crítica**

• Los datos y bases de datos de misión crítica actuales deben respaldarse de acuerdo con los objetivos de punto de recuperación (RPO) establecidos, y deben reflejarse o replicarse para asegurar ubicaciones de respaldo dentro de los plazos de RPO.

• Las copias de seguridad deben almacenarse fuera del sitio en una o más ubicaciones seguras en la nube o en oficinas o centros de datos alternativos de la empresa, o una combinación de estos.

• El administrador de datos principal es responsable de esta actividad.

**Datos que no son de misión crítica**

• Los datos que no son de misión crítica del software "Acanner" deben respaldarse regularmente de acuerdo con los objetivos de punto de recuperación (RPO) establecidos, teniendo en cuenta la frecuencia de los cambios realizados en estos datos.

• Se recomienda realizar copias de seguridad de estos datos al menos dos veces por semana, o según las métricas de RPO definidas por la empresa.

• Las copias de seguridad de los datos que no son de misión crítica del software "Acanner" pueden almacenarse en el sitio en instalaciones de almacenamiento seguro, así como fuera del sitio en ubicaciones geográficamente separadas y protegidas.

• Se debe garantizar que los medios de almacenamiento utilizados para respaldar estos datos estén protegidos contra peligros ambientales y accesibles en caso de necesidad de recuperación.

• Se deben realizar pruebas periódicas de las copias de seguridad de los datos que no son de misión crítica del software "Acanner" para verificar su integridad y la capacidad de recuperación.

• Se debe mantener una supervisión regular de los procesos de respaldo y restauración para identificar y abordar cualquier problema o anomalía de manera oportuna.

• Se deben revisar y actualizar regularmente los procedimientos de respaldo de datos que no son de misión crítica del software "Acanner" para garantizar su relevancia y eficacia.

• Se debe mantener una comunicación abierta con los usuarios y administradores del sistema para recopilar retroalimentación y realizar ajustes según sea necesario.

**Procedimientos de almacenamiento fuera del sitio**

• Estos medios alternativos deben cumplir con los mismos estándares de seguridad y protección del almacenamiento, asegurando la integridad y disponibilidad de los datos respaldados.

• Se debe establecer un procedimiento para la sincronización regular de los datos entre el almacenamiento en sitio y fuera del sitio, garantizando la consistencia y actualización de los respaldos.

**Realización de copias de seguridad de datos**

Las copias de seguridad de datos se programarán diaria, semanal y mensualmente, según la naturaleza de la copia de seguridad. Los administradores de datos deben utilizar la tecnología de respaldo de datos aprobada para preparar, programar, ejecutar y verificar respaldos. Las copias de seguridad se pueden realizar en recursos de almacenamiento local (por ejemplo, disco, cinta, RAID) localmente o en ubicaciones seguras fuera del sitio (por ejemplo, proveedores de servicios de copia de seguridad de datos en la nube, proveedores de copia de seguridad como servicio) aprobados por la administración de TI.

**Recuperación de datos**

Se deben establecer, documentar y probar periódicamente procedimientos para recuperar datos, bases de datos, sistemas, aplicaciones y otros activos de información si ocurre un evento disruptivo que requiera la recuperación de esos activos y recursos.

**Revisión y mantenimiento del plan**

Este plan de copia de seguridad de datos debe revisarse periódicamente y los procedimientos deben validarse (y actualizarse según sea necesario) para garantizar que las copias de seguridad se realicen según sea necesario y cuando sea necesario. Como parte de esta actividad, es recomendable revisar las listas del personal del equipo de respaldo de datos, proveedores de servicios de respaldo de datos y proveedores de respaldo de datos en la nube, y actualizar los datos de contacto según sea necesario.

La versión impresa de este plan de respaldo de datos se almacenará en una ubicación común donde el personal de TI, como los administradores de datos, pueda verlo. Las versiones electrónicas estarán disponibles a través del Soporte técnico de TI.