**Políticas de mantenimiento**

**Elección de Reina de Faculta**

**Introducción**

Las políticas de mantenimiento del sistema utilizado para la elección de reina de facultad son directrices diseñadas para garantizar el correcto funcionamiento y la seguridad de las herramientas tecnológicas implementadas durante el proceso. Estas políticas aseguran que el sistema sea confiable, accesible y cumpla con los estándares requeridos.

**Objetivo de las Políticas de Mantenimiento**

Como objetivo principal establecer directrices claras para asegurar el funcionamiento óptimo del sistema tecnológico utilizado en la elección de reina de facultad. Esto incluye garantizar la transparencia de los procesos, proteger los datos de los participantes, minimizar posibles interrupciones técnicas y proporcionar una experiencia fluida para los usuarios.

**Alcance de las Políticas de Mantenimiento**

El alcance de las políticas de mantenimiento se centra en todas las actividades relacionadas con el sistema tecnológico en la elección de reina de facultad. Estas actividades incluyen la instalación, configuración, actualización, monitoreo y soporte técnico, así como la protección de datos.

**Normas y Políticas de Seguridad**

**Normas de Seguridad:**

* **Autenticación y control de acceso:** Se implementaron métodos seguros de autenticación (como contraseñas fuertes o autenticación de dos factores) para restringir el acceso al sistema únicamente a usuarios autorizados.
* **Encriptación de datos:** Toda la información almacenada y transmitida esté cifrada para protegerla de accesos no autorizados.
* **Actualizaciones regulares:** Mantener el sistema actualizado con los últimos parches de seguridad para prevenir vulnerabilidades conocidas.
* **Monitoreo continuo:** Establecer herramientas de monitoreo que detecten actividades sospechosas no autorizados en tiempo real.
* **Políticas de respaldo:** Copias de seguridad periódicas y almacenadas en ubicaciones seguras para garantizar la recuperación de datos en caso de pérdida.

**Políticas de Seguridad:**

* **Confidencialidad de los datos:** La información de los participantes y los resultados de la elección sean manejados únicamente por personal autorizado y bajo estrictas medidas de seguridad.
* **Gestión de incidentes:** Responder a posibles incidentes de seguridad, como intentos de hackeo o pérdida de datos.
* **Capacitación de usuarios:** Brindar formación regular a los usuarios sobre buenas prácticas de seguridad, como el manejo de contraseñas y la identificación de correos electrónicos sospechosos.
* **Pruebas de seguridad:** Auditorías y simulaciones de ciberataques para identificar y solucionar posibles vulnerabilidades del sistema.
* **Política de acceso limitado:** Restringir los permisos de acceso según las funciones y responsabilidades de cada usuario, minimizando riesgos innecesarios.

**Políticas de Mantenimiento: Consideración de Costos**

|  |  |
| --- | --- |
| 1 | Costos de Infraestructura: |
|  | * + **Servidores:** Gastos relacionados con la contratación de servicios en la nube o la adquisición de hardware físico.   + **Licencias:** Pago por software, herramientas utilizadas para la implementación del sistema. |
| 2 | **Costos Operativos:** |
|  | * + **Mano de obra:** Al personal técnico encargado del mantenimiento.   + **Capacitación:** Inversión en la formación de organizadores y usuarios finales para el uso correcto del sistema.   + **Monitoreo:** Gastos asociados a la supervisión en tiempo real del sistema durante el evento. |
| 3 | **Costos de Seguridad:** |
|  | * + **Auditorías:** Inversiones en pruebas de seguridad y simulaciones para identificar vulnerabilidades.   + **Protección de datos:** Costos por implementar tecnologías de encriptación y herramientas de ciberseguridad. |
| 4 | **Mantenimiento Post-evento:** |
|  | * + **Auditoría post-evento:** Análisis del sistema para identificar mejoras.   + **Actualizaciones:** Implementación de mejoras técnicas o parches después del evento |
| 5 | **Costos de Respaldo y Contingencia:** |
|  | * **Copias de seguridad:** Almacenamiento en la nube y servidores físicos para respaldos de información. * **Planes alternativos:** Recursos destinados a la activación de soluciones en caso de fallas críticas. |

**Políticas de Calidad**

Establecer estándares de calidad para el sistema ya que es importante garantizar su correcto funcionamiento, accesibilidad, y aceptación por parte de los usuarios.:

* **Disponibilidad:** El sistema debe estar operativo al 99.9% durante el evento.
* **Velocidad:** Respuestas rápidas a las acciones del usuario (por ejemplo, tiempo de carga inferior a 2 segundos).
* **Usabilidad:** El sistema debe ser intuitivo y fácil de utilizar tanto para organizadores como para participantes.
* **Trazabilidad:** Registro detallado de todas las acciones realizadas en el sistema para garantizar transparencia.