**Propuesta de control interno informático**

**En el área computacional de la Biblioteca “Roberto Osorio”**

Para llevar a cabo el control interno informático dentro de la biblioteca se consideran importante el empleo de las siguientes medidas:

## Control General Organizativo

Orientado a obtener un mejor orden administrativo y facilitar la realización de las tareas asignadas dentro de la empresa.

|  |  |  |  |
| --- | --- | --- | --- |
| Riesgos (situaciones) | Preventivo | Detectivo | Correctivo |
| 1a. Poca eficiencia al realizar las tareas dentro de la biblioteca por parte de los administradores. | + Realizar una junta con el personal administrativo para visualizar posibles dificultades de trabajo. | + Puntos de chequeó en las actividades de administrativas internas de la biblioteca. | + Realizar actividades en tiempo y forma apegadas a la forma de trabajo antes planeada. |
| 2a. Incumplimiento de objetivos del área administrativa. | + Planificación de actividades específicas en el área. | + Realizar reporte periódico de las actividades planeadas dentro de los objetivos administrativos. | + Reestructuración de los objetivos para facilitar su cumplimiento.  + Capacitación al personal de la biblioteca para garantizar que conozcan las formas de trabajo. |

## Control de adquisición y mantenimiento de sistemas de información

Para permitir alcanzar la eficiencia del sistema, integridad de los datos, protección de recursos y cumplimiento de las normas.

|  |  |  |  |
| --- | --- | --- | --- |
| Riesgos (situaciones) | Preventivo | Detectivo | Correctivo |
| 1b. Bajo rendimiento del sistema de administración de la biblioteca. | + Asignar los recursos informáticos necesarios para que el sistema funcione al 100% (espacio de almacenamiento, velocidad de procesado, entre otros). | + Medir periódicamente los tiempos que el sistema ocupa para realizar sus procesos (velocidad de respuesta). | + Aumentar el espacio de almacenamiento destinado al sistema.  + Gestionar el equipo para verificar que otras aplicaciones no interfieran con el sistema y/o disminuyan sus recursos. |
| 2b. Equipos de cómputo infectados con virus dañinos. | + Instalar un software antivirus de tipo preventor en todos los equipos de cómputo de la biblioteca.  + Restringir el acceso de los usuarios a páginas de internet con posible contenido dañino para el equipo. | + Realizar un análisis del equipo con un antivirus detector para identificar amenazas. | + Llevar a cabo una limpieza de todos los archivos del equipo de cómputo, para garantizar la eliminación de amenazas. |
| 3b. Daños físicos a las computadoras de la biblioteca. | + Promover la cultura del cuidado del equipo (con apoyo del área de administración).  + Registrar los préstamos de equipo de cómputo para verificar en qué momento se produce el posible daño. | + Llevar a cabo mensualmente un proceso de mantenimiento y revisión de las computadoras.  + Apoyarse en el registro mencionado antes para identificar al infractor. | + Establecer sanciones en caso de maltrato a los equipos.  + Reparar los daños del equipo de cómputo. |
| 4b. Aplicaciones con mal funcionamiento y medidas inseguras. | + Instalar un Antivirus de aplicaciones tomando como ejemplo PCPROTECT. | + Chequeo de funcionalidad de programas por parte de personal autorizado. | + Desinstalar y reinstalar las aplicaciones dañadas o bien obtener una versión mejorada. |

## Controles en aplicaciones

El control en las aplicaciones dentro de la biblioteca nos permitirá bloquear aquellos programas que amenacen la seguridad de nuestro sistema y equipo, asimismo permitirá verificar que las aplicaciones tengan un rendimiento óptimo y exista una alta seguridad de entrada y salida de datos.

|  |  |  |  |
| --- | --- | --- | --- |
| Riesgos (situaciones) | Preventivo | Detectivo | Correctivo |
| 1c. Uso no autorizado del sistema en la computadora de administración. | + Uso de cuentas y contraseñas en el sistema para el control de acceso, que permita únicamente el acceso a archivos importantes a los administradores. | + Realizar una revisión de los intentos de iniciar sesión (tanto fallidos como correctos). | + Verificar que el sistema esté respetando el acceso mediante cuentas, en caso de no ser así, reparar dicho aspecto. |
| 2c. Excesivas cuentas por parte de un usuario (administrador). | + Añadir al sistema una opción de recuperación de contraseña (pregunta de seguridad). | + Gestión de cuentas de usuario por parte del encargado del sistema. | + Eliminación de cuentas extra no necesarias (pertenecientes al mismo usuario). |
| 3c. Fallas o errores al momento de realizarse los procesos del sistema. | + Diseñar el sistema de forma integral preparándolo para cualquier tipo de error. | + Realizar un test de medición contra fallos al sistema, para identificar los fallos específicos que el sistema presente. | + Trabajar en la corrección de dichas situaciones problema, evitando así futuros errores del mismo tipo. |

## Controles específicos de ciertas tecnologías

\*\* Gestión de datos y base de datos.

Control enfocado a gestionar de forma correcta la información contenida en la base de datos y permitir una mejor manipulación de la misma.

|  |  |  |  |
| --- | --- | --- | --- |
| Riesgos (situaciones) | Preventivo | Detectivo | Correctivo |
| 1d. Errores al realizar consultas a los datos almacenados (datos incorrectos como salida). | + Diseñar debidamente la base de datos.  +Definir las consultas de la base de datos asegurándose de estructurarlas correctamente. | + Llevar a cabo una simulación de diferentes consultas a los datos, con el fin de identificar si son o no acertadas. | + Reestructurar las instrucciones de consulta a la base de datos.  + Revisar las relaciones entre tablas dentro de la base de datos. |
| 2d. Perdida de información (datos almacenados). | + Estructurar correctamente los archivos involucrados en el guardado de los datos.  + Verificar que el dispositivo de almacenamiento o servidor donde los datos serán alojados funcione correctamente. | + Realizar pruebas periódicas a la base de datos para saber si la información se pierde después de un tiempo determinado. | + Establecer un nuevo medio de almacenamiento y/o servidor para guardar los datos.  + Corregir errores de estructura en los archivos relacionados con el almacenamiento de datos. |

\*\* Redes

|  |  |  |  |
| --- | --- | --- | --- |
| Riesgos (situaciones) | Preventivo | Detectivo | Correctivo |
| 3d. Mala conexión a Internet en los equipos de usuarios y de administrador. | + Evitar el exceso de conexiones activas de dispositivos móviles.  + Acordar una velocidad de conexión adecuada con el proveedor de servicios de internet. | + Medir la velocidad de conexión a la red (subida y bajada) en los diferentes equipos de cómputo.  + Verificar que el cableado y dispositivos relacionados estén en buen estado. | + Restructurar el acomodo de la red local (cableado y dispositivos).  + En caso extremo, cambiar de proveedor de servicios de internet. |
| 4d. Error al acceder a la página web y base de datos alojada en un servidor web. | + Elegir un servidor web estable, es decir, con el mínimo de fallas reportadas.  + Estructurar de forma correcta la relación entre sistema, base de datos y sitio web de la biblioteca. | + Monitoreo constante de la página web para determinar si está o no funcionando adecuadamente.  + Chequeo del acceso a la base de datos. | + Revisar y corregir la estructura de relación entre sistema, base de datos y sitio web de la biblioteca. |

# Anexo: Políticas de recursos informáticos

## Alcance

Esta sección es aplicable a todos los administradores y usuarios que en algún momento cuenten con acceso a los recursos informáticos o información de la biblioteca.

## Sobre la asignación y el uso de los recursos

1. Únicamente el administrador en turno tendrá acceso a la computadora principal e impresora de la biblioteca (sistema central).

2. Los usuarios deben hacer buen uso equipos de cómputo disponibles, así como también deberán notificar a los administradores en caso de fallas del equipo y/o sistema.

3. La duración de una sesión en un equipo de cómputo para un usuario común será de una hora. Si se requiere más tiempo se debe solicitar al administrador indicando el motivo.

4. El uso de la conexión a internet se permitirá solo para consultar información didáctica y/o escolar, exceptuando contenidos de entretenimiento (videos, música, redes sociales, páginas de juegos).

## Sobre la seguridad de la información

5. Cada tres días se realizarán backups automáticos en la base de datos del sistema central.

6. El acceso a los sistema principal estará protegido mediante un mecanismo de usuario y contraseña, esto para evitar que se modifique la información en caso de un uso no autorizado de la computadora principal.

7. Las contraseñas de acceso para los administradores serán proporcionadas por los diseñadores del sistema central.

8. Tanto a la computadora principal como a los equipos destinados a usuarios se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

• Actualizar su base de firmas de virus (actualización de la lista de amenazas)

• Búsqueda de virus (análisis del equipo)

• Eliminación de virus si fue detectado.

## Sobre el mantenimiento y buen uso de la infraestructura

9. Los equipos de toda la biblioteca deberán estar conectados a un regulador de corriente, como medida de prevención de descargas eléctricas, con el fin de resguardar la información en ellos contenida.

10. Si se presentara una suspensión de servicio eléctrico se deben guardar las modificaciones realizadas en el sistema de la computadora principal (administrador).

11. Periódicamente, por espacio de 6 meses, se realizará una limpieza física a los equipos de cómputo por parte del personal de sistemas.

12. Toda actividad elaborada por el equipo de sistemas deberá estar documentada para darle seguimiento y que sirva como evidencia en los procesos de gestión de la biblioteca.