PLAN DE MEJORA

MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS

El presente documento es un **plan de mejora** en cuanto a las **buenas prácticas de seguridad de la información** que el **Colegio P. Andrés de Urdaneta** adopta, con el fin de aumentar la protección de la información personal y cumplir con la normativa de protección de datos vigente.

Todas las organizaciones tienen la obligación de custodiar los datos personales de tal forma que se mantenga su **confidencialidad** (la información solamente debe ser accesible por el personal autorizado), **integridad** (la información debe ser correcta y libre de modificaciones y errores) y **disponibilidad** (la información debe estar siempre accesible) y actuar de forma proactiva evitando que se produzcan brechas de seguridad.

La concienciación, el sentido común y las buenas prácticas son las mejores defensas para prevenir y detectar contratiempos en la utilización de **sistemas de las Tecnologías de la Información y la Comunicación (TIC).** Por lo tanto, con el fin de implementar la seguridad de la información y minimizar riesgos es necesario determinar **medidas de seguridad**, así como la observación continua y actualización de las mismas (mejora continua).

A continuación, tras analizar la situación concreta del **Colegio P. Andrés de Urdaneta,** en base al cuestionario para el análisis de riesgos completado por el mismo, se señalan las actuaciones y medidas técnicas y organizativas que se deben adoptar.

Estas son las **acciones de mejora** que debe llevar a cabo el centro:

MEDIDAS A ADOPTAR POR LA DIRECCIÓN	SEGUIMIENTO	FECHA
Auditorías		
Concretar un plan de auditorías periódicas para verificar la seguridad y el cumplimiento de la normativa de protección de datos.		
Personal		
Sensibilización y formación del personal		
Concretar un plan de formación para el personal con el fin de elevar su conocimiento en protección de datos, promoviendo así una cultura de seguridad de la información.		
Comunicar al personal los aspectos más importantes en materia de seguridad de la información, incluyendo las obligaciones que tienen que cumplir al finalizar su contrato.		
Servicios en la nube		
Informar al personal sobre el proceso adecuado de borrado de la información en la nube.		
Informar al personal sobre el tipo de información que pueden almacenar en la nube y si necesita ser cifrada.		
Conocer la política de seguridad y política de privacidad de las empresas proveedoras de almacenamiento en la nube.		

Relaciones con empresas proveedoras de servicios informáticos		
Disponer de un inventario de encargados de tratamiento con el fin de tener constancia de los proveedores de servicios informáticos en todo momento.		
Soportes en papel		
Eliminar la información de manera segura una vez terminada su vida útil, utilizando el proceso de triturado.		
Promover entre el personal una política de mesas limpias y el deber de almacenar la documentación en dispositivos bajo llave, de manera que se impidan los accesos no autorizados a la información.		

MEDIDAS A ADOPTAR POR EL PERSONAL EN SU PUESTO DE TRABAJO	**SEGUIMIENTO**	**FECHA**
Conocer y aplicar las buenas prácticas en materia de seguridad que ha implantado el colegio.		

MEDIDAS A ADOPTAR POR EL DEPARTAMENTO DE SISTEMAS	**SEGUIMIENTO**	**FECHA**
Información crítica y datos personales		
Revisar la eliminación de los permisos de acceso y cuentas de usuario de los empleados cuando finalizan su contrato.		
Programar la deshabilitación por defecto de los puertos USB y habilitarlos únicamente para el personal que lo necesite.		
Actualización del Software		
Activar por defecto las actualizaciones del fabricante del software.		
Malware		
Verificar que el antivirus se mantiene actualizado y activo en todo momento.		
Control de accesos		
Establecer un registro de los accesos realizados cuando sea necesario saber quién accede a la información.		
Contraseñas		
Establecer una política segura en la creación, mantenimiento y cambio de contraseñas, manteniendo la seguridad y la privacidad de la información.		
Copias de seguridad		

Guardar al menos una copia completa fuera de las instalaciones del centro bajo condiciones adecuadas de seguridad.		
Dispositivos extraíbles (pendrives, discos duros externos etc.)		
Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en el dispositivo extraíble (cifrado de datos, autenticación, cambio periódico de contraseñas, etc.).		
Eliminar la información para la reutilización de soportes electrónicos (proceso de sobreescritura).		
Hacer un borrado seguro de la información una vez que ésta ya no sea necesaria.		
Eliminar la información antes de deshacerse de soportes electrónicos (proceso de desmagnetización o destrucción física).		
Gestión de incidencias		
Documentar la información relativa a la detección y gestión de incidentes de seguridad de la información y mantenerla actualizada.		
Estudiar los incidentes producidos anteriormente, analizando sus causas y estableciendo medidas adicionales que protejan los activos de posibles incidentes posteriores.		
Comunicaciones externas y cifrado		
Verificar que si se autorizan accesos al sistema desde el exterior, ya sea por personal del centro o por proveedores que lo requieran para la prestación de sus servicios, se utilicen canales VPN.		
Seguridad en la web		
Mantener un registro de la actividad de los administradores externos.		
Dispositivos móviles (Portátiles, Smartphones, Tablets, etc.)		
Mantener un registro de equipos asignados y también el uso que se le da a los mismos, así como el software y hardware que contienen.		
Comunicar al usuario del dispositivo en caso de disponer de software de localización.		
Informar y concienciar al usuario sobre el tipo de información que pueden almacenar en los dispositivos remarcando lo relativo al almacenamiento de documentos personales, archivos de música, fotografías, etc.		
Correo electrónico		

Disponer de una normativa de uso del correo electrónico.		
Instalar y activar aplicaciones antimalware y antispam.		