Manual de Seguridad Informática Parte II

Erik Fabian Alarcón Riaño

Samuel David Ballesteros Cristo

Juan David Cadena Vera

Sistema Gestores Bases de Datos

Fundación Universitaria Compensar

Facultad de Ingeniería, Ingeniería en Sistemas

Ingeniero: Camilo Alfonso Salamanca

Bogotá DC, Colombia

10 de Abril de 2024

Tabla de Contenido

Introducción

La seguridad de la información es un aspecto crítico en el entorno digital actual. Con el crecimiento exponencial de las amenazas cibernéticas, es fundamental que el Instituto implemente medidas efectivas de seguridad informática para proteger los activos digitales y la privacidad de la comunidad educativa. Este manual proporciona una guía completa sobre las políticas, procedimientos y mejores prácticas de seguridad informática que deben seguirse en el Instituto.

Objetivos del manual:

El presente manual de seguridad informática tiene como propósito principal salvaguardar los activos digitales del Instituto de Inglés InterAmerican, asegurando que la información confidencial de nuestros estudiantes, docentes y personal administrativo se mantenga protegida contra amenazas cibernéticas. Los objetivos específicos de este manual son:

- Identificar y evaluar los riesgos potenciales para la seguridad informática en el Instituto de Inglés InterAmerican.
- Establecer políticas y procedimientos claros para mitigar riesgos y proteger los activos digitales.
- Educar y sensibilizar al personal sobre las mejores prácticas de seguridad informática.
- Implementar controles de seguridad efectivos para prevenir y detectar posibles incidentes de seguridad.
- Garantizar la continuidad del negocio mediante la preparación y respuesta ante incidentes de seguridad.

Alcance y aplicabilidad

Este manual de seguridad informática es aplicable a todos los empleados, estudiantes, proveedores y cualquier otra entidad que interactúe con los sistemas y datos del Instituto de Inglés InterAmerican. Su alcance abarca todas las actividades relacionadas con el procesamiento, almacenamiento y transmisión de información dentro de nuestra infraestructura tecnológica.

Definición de términos clave

Para una comprensión precisa y uniforme de las medidas de seguridad informática establecidas en este manual, es importante definir algunos términos clave:

- ***Activos digitales:*** Cualquier información o recurso electrónico que posea valor para el Instituto de Inglés InterAmerican, incluyendo datos de estudiantes, materiales didácticos, notas, horarios, registros académicos, software entre otras cosas.
- ***Amenazas cibernéticas:*** Acciones maliciosas o incidentes que tienen el potencial de comprometer la seguridad de los sistemas informáticos y la información almacenada.
- ***Políticas de seguridad:*** Directrices y procedimientos establecidos para proteger los activos digitales y mitigar los riesgos de seguridad informática.
- ***Incidente de seguridad:*** Evento que compromete la integridad, confidencialidad o disponibilidad de la información, y que requiere una respuesta inmediata.
- ***Continuidad del negocio:*** Planificación y preparación para garantizar que las operaciones críticas del Instituto de Inglés InterAmerican puedan continuar de manera efectiva en caso de un incidente de seguridad o interrupción.

En conjunto, estos objetivos, alcance y definiciones proporcionan un marco sólido para el desarrollo e implementación de medidas de seguridad informática efectivas en el Instituto de Inglés InterAmerican, fortaleciendo así la protección de nuestros activos digitales y la confianza de nuestra comunidad educativa.

Políticas de Seguridad

La seguridad de la información es un componente vital para la protección de los activos y la confidencialidad de los datos en cualquier organización. La Política de Seguridad establece un marco de referencia para garantizar la integridad, confidencialidad y disponibilidad de los recursos de información. En el caso del Instituto InterAmerican, esta política se enfoca en proteger la base de datos que contiene información sensible sobre estudiantes, personal y operaciones académicas.

Política de acceso y autenticación

- Todos los usuarios deben tener una cuenta única y personal para acceder a la base de datos del Instituto InterAmerican.
- El acceso a la base de datos se basará en roles definidos, que determinarán los privilegios de cada usuario.
- Los usuarios deberán autenticarse utilizando un nombre de usuario y una contraseña seguros.
- Se implementará un procedimiento de gestión de cuentas para agregar, modificar y eliminar cuentas de usuario según sea necesario.
- Se registrarán los intentos de acceso fallidos para detectar posibles intentos de intrusión.

Política de contraseñas

- Las contraseñas deberán tener al menos 8 caracteres de longitud.

- Deberán incluir al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.
- Se requerirá que las contraseñas se cambien cada 90 días.
- No se permitirá reutilizar contraseñas anteriores.
- Los usuarios recibirán capacitación sobre la importancia de mantener sus contraseñas seguras y protegidas.

Política de uso aceptable

- El acceso a la base de datos está limitado a actividades relacionadas con las operaciones del Instituto InterAmerican.
- No se permitirá el acceso no autorizado a la información confidencial de los estudiantes o el personal.
- No se tolerará el uso de la base de datos para actividades ilegales o maliciosas.
- Los usuarios serán responsables de proteger su información de inicio de sesión y no compartir sus credenciales con otras personas.
- Se aplicarán sanciones disciplinarias a los usuarios que violen esta política.

Política de respaldo y recuperación

- Se realizarán copias de seguridad completas de la base de datos diariamente.
- Se almacenarán las copias de seguridad en un lugar seguro y fuera del sitio.
- Se llevarán a cabo pruebas de recuperación periódicas para garantizar la eficacia de los procedimientos de respaldo.

- Se documentarán los procedimientos de recuperación de datos para facilitar la restauración rápida en caso de pérdida de datos.

Política de seguridad física

- El acceso físico a los servidores y equipos de la base de datos estará restringido a personal autorizado.
- Se implementarán medidas de seguridad física, como sistemas de alarma, cerraduras y cámaras de seguridad.
- Los servidores se ubicarán en una sala de servidores con acceso restringido y control de temperatura y humedad.
- Se desarrollará un plan de contingencia para proteger los equipos en caso de desastres naturales o emergencias.

Política de seguridad en dispositivos móviles

- Todos los dispositivos móviles que accedan a la base de datos deberán estar protegidos con contraseña o PIN.
- Se requerirá la instalación de software de seguridad en los dispositivos móviles, incluyendo antivirus y antimalware.
- Se fomentará el uso de conexiones seguras, como VPN, al acceder a la base de datos desde dispositivos móviles.
- Se desactivará el acceso remoto a la base de datos en dispositivos móviles perdidos o robados.

Política de seguridad en redes

- Se implementarán firewalls para controlar el tráfico de red entrante y saliente.
- Se utilizará el cifrado para proteger la comunicación entre los dispositivos y la base de datos.
- Se llevarán a cabo escaneos regulares de vulnerabilidades en la red para identificar posibles puntos de entrada para los ataques.
- Se aplicarán políticas de seguridad en el acceso a la red Wi-Fi del instituto para proteger contra el acceso no autorizado.

Procedimientos

Los procedimientos de seguridad son documentos que establecen las acciones específicas a seguir para garantizar la protección de los activos y la integridad de los sistemas de información de una organización. En el caso del Instituto InterAmerican, estos procedimientos son fundamentales para mantener un entorno seguro y protegido para la gestión de datos sensibles relacionados con estudiantes, personal y operaciones académicas.

Procedimiento para la gestión de contraseñas:

- Los usuarios deben crear contraseñas que cumplan con los criterios de seguridad establecidos, incluyendo longitud mínima, uso de caracteres especiales, letras mayúsculas y minúsculas, y números.
- Se establecerá un periodo de caducidad para las contraseñas, y los usuarios serán notificados para cambiarlas de manera regular.
- Se implementará un mecanismo para la gestión segura de contraseñas, evitando su compartición y almacenamiento en lugares no seguros.

Procedimiento para la autenticación de usuarios

- Los usuarios deberán autenticarse utilizando un nombre de usuario y contraseña válidos.
- En casos donde sea necesario un nivel adicional de seguridad, se empleará la autenticación multifactor.
- Se registrarán y monitorizarán los intentos de acceso fallidos para detectar posibles intentos de intrusión.

Procedimiento para la instalación de software

- Se designará un equipo o persona responsable de evaluar y aprobar la instalación de nuevo software en los sistemas del instituto.
- Antes de la instalación, se realizarán pruebas de compatibilidad y seguridad para garantizar que el software no represente riesgos para la infraestructura existente.
- Se documentarán los pasos de instalación, incluyendo la configuración adecuada y la asignación de permisos de acceso.

Procedimiento para la gestión de parches y actualizaciones

- Se establecerá un calendario regular para la aplicación de parches y actualizaciones de seguridad en todos los sistemas del Instituto InterAmerican.
- Antes de aplicar los parches, se realizarán pruebas en un entorno de prueba para garantizar que no causen problemas de funcionamiento.
- Se documentarán todas las actualizaciones aplicadas, incluyendo detalles como la fecha, el tipo de actualización y los sistemas afectados.

Procedimiento para la gestión de incidentes de seguridad

- Se designará un equipo de respuesta a incidentes para manejar cualquier incidente de seguridad que se produzca.
- Los incidentes serán reportados de inmediato al equipo de seguridad, que investigará y tomará medidas correctivas adecuadas.
- Se mantendrá un registro de todos los incidentes reportados, incluyendo detalles como la naturaleza del incidente, las acciones tomadas y las lecciones aprendidas.

Procedimiento para la gestión de dispositivos móviles

- Se implementará una política de uso de dispositivos móviles que establezca los requisitos de seguridad para los dispositivos que acceden a los recursos del instituto.
- Los dispositivos móviles serán configurados con medidas de seguridad apropiadas, como la encriptación de datos y el bloqueo remoto en caso de pérdida o robo.
- Se llevará a cabo un seguimiento regular de los dispositivos móviles conectados a la red del instituto para garantizar su cumplimiento con las políticas de seguridad.

Procedimiento para la gestión de accesos

- Se establecerán roles de usuario con privilegios específicos, y se asignarán estos roles según las responsabilidades de cada empleado.
- Se llevará a cabo una revisión periódica de los derechos de acceso para garantizar que sean apropiados y estén actualizados.
- Se documentarán los cambios en los accesos de usuario, incluyendo quién realizó el cambio y la justificación para el mismo.