INFORME SOBRE LA IMPLEMENTACIÓN DE CIBERSEGURIDAD EN LA EMPRESA

Realizado por: Karol Vanessa Nuñez Vera

Dirigido a: Angela Patricia Marroquín

Técnico en Control de la Seguridad Digital

SENA

Ficha: 2930435

Fecha: 24/01/2025

Tabla de contenido

1. Introducción

El programa realizado en PHP utilizado por la empresa es un sistema integral que gestiona aspectos clave de la operación, incluyendo bases de datos, diagramas, contabilidad, y otros sectores críticos e importantes. Este programa es utilizado de manera extensiva, lo que presenta varios riesgos relacionados con la seguridad digital. A pesar de la importancia del sistema, actualmente no se han implementado medidas adecuadas de ciberseguridad, lo que podría exponer a la empresa a amenazas y vulnerabilidades.

El presente informe tiene como objetivo establecer un plan para integrar medidas de ciberseguridad que garanticen la protección de la infraestructura digital de la empresa, especialmente en lo relacionado con el manejo de contraseñas, control de acceso, mantenimiento de los servidores y otros aspectos cruciales para el funcionamiento seguro del sistema.

2. Medidas de Protección en el Programa PHP

2.1 Encriptación de Contraseñas

El sistema actual presenta deficiencias en la encriptación de contraseñas, lo que representa un riesgo significativo en caso de un ataque o acceso no autorizado. Para mitigar este riesgo, se recomienda implementar algoritmos de encriptación modernos y seguros como bcrypt, scrypt o Argon2, los cuales son diseñados específicamente para proteger las contraseñas de los usuarios.

Se debe garantizar que las contraseñas se almacenan utilizando técnicas de "salting" y "hashing" para asegurar que no puedan ser recuperadas ni siquiera en caso de acceso a la base de datos. Además, el uso de algoritmos de encriptación robustos garantiza que las contraseñas sean resistentes ante ataques de diccionario o de fuerza bruta.

2.2 Control de Acceso

Se recomienda la implementación de autenticación multifactor (MFA). Esto reducirá la probabilidad de que un atacante obtenga acceso a áreas críticas del sistema, incluso si logra obtener una contraseña válida.

3. Fallo / Mantenimiento en Servidores y Ciberseguridad

3.1 Redundancia y Respaldo

Para garantizar la continuidad del servicio y la disponibilidad de la información crítica en caso de fallos, se implementarán copias de seguridad periódicas de las bases de datos y archivos importantes. Estas copias de seguridad deben almacenarse en ubicaciones separadas (tanto en servidores locales como en la nube) y deben ser cifradas para proteger la información en caso de un acceso no autorizado.

Además, se utilizarán tecnologías de alta disponibilidad (HA), como la replicación de bases de datos, que permitirán que el sistema continúe funcionando en caso de que un servidor falle. Esto garantizará la mínima interrupción de las operaciones, incluso en situaciones críticas.

3.2 Manejo de Vulnerabilidades

Durante las sesiones de mantenimiento, es esencial aplicar de manera sistemática parches y actualizaciones de seguridad a todos los componentes del servidor, incluidos el sistema operativo, el servidor web y el programa PHP. De igual manera, se recomienda la utilización de herramientas de escaneo de vulnerabilidades para detectar debilidades en la infraestructura del servidor y corregir cualquier hallazgo de manera prioritaria.

Cada vulnerabilidad identificada debe ser evaluada en función de su gravedad, y las actualizaciones deben implementarse lo antes posible para reducir los riesgos de un posible ataque.

3.3 Monitoreo Constante

Se debe implementar un sistema de monitoreo de servidores que permita la detección inmediata de fallos en los servicios o actividades sospechosas. Herramientas de monitoreo avanzadas alertarán en tiempo real sobre intentos de acceso no autorizado, tráfico inusual o cualquier otro comportamiento que pueda indicar la presencia de un ataque cibernético.

El monitoreo debe incluir el análisis constante de los registros del servidor, buscando patrones anómalos que puedan indicar intentos de intrusión, modificación no autorizada de datos o abusos de privilegios.

3.4 Mantenimiento con Seguridad

Es necesario establecer una política de "mínimos privilegios" para el personal encargado del mantenimiento de los servidores, asegurando que cada usuario tenga acceso únicamente a los recursos necesarios para llevar a cabo su trabajo. El acceso al servidor debe restringirse a los administradores y personal autorizado, y todo acceso remoto debe realizarse a través de métodos seguros, como VPN y autenticación multifactor (MFA).

Durante las tareas de mantenimiento, se deben evitar prácticas que puedan comprometer la seguridad, como compartir contraseñas o dejar configuraciones inseguras por error. También es importante que el acceso a la infraestructura crítica se realice bajo estrictos controles de seguridad.

3.5 Recuperación Ante Desastres (DRP)

Un plan de recuperación ante desastres (DRP) detallado debe ser implementado y probado regularmente para asegurar que el sistema pueda ser restaurado rápidamente en caso de un fallo grave. Este plan debe incluir procedimientos claros para la restauración de datos a partir de las copias de seguridad y la puesta en marcha de los servicios lo más rápido posible.

El DRP debe ser probado de manera periódica, tanto en un entorno de pruebas como en el entorno de producción, para asegurar su efectividad y que no existan fallos durante su ejecución.

3.6 Cifrado

Todo el tráfico de datos entre los servidores y los dispositivos de los empleados debe ser cifrado utilizando protocolos seguros como HTTPS, SSH o VPN. De esta manera, se garantizará que la información no pueda ser interceptada por actores maliciosos durante su transmisión.

Asimismo, los datos sensibles almacenados en los servidores, como las contraseñas y otra información personal, deben ser cifrados utilizando algoritmos robustos, como AES-256, para proteger la información en caso de acceso no autorizado o robo de datos.

3.7 Control de Acceso

El acceso a los servidores y a la infraestructura crítica debe estar estrictamente controlado. Se deben implementar herramientas de gestión de identidad y acceso (IAM) para asignar roles y permisos de manera eficiente. La autenticación multifactor (MFA) debe ser obligatoria para todos los accesos privilegiados, asegurando que solo los administradores y personal autorizado tengan acceso a recursos críticos.

4. Evaluación de Riesgos y Amenazas

4.1 Análisis de Riesgos

Se debe realizar un análisis de riesgos detallado, identificando las amenazas potenciales más relevantes para el sistema, incluyendo:

- **Amenazas externas**: ataques de hackers, phishing, malware, etc.
- **Amenazas internas**: accesos no autorizados por empleados, fallos humanos, robo de datos internos, etc.
- **Riesgos asociados a la infraestructura**: fallos en el hardware, interrupciones de la red, problemas de energía, etc.

Este análisis permitirá priorizar las acciones de seguridad y asignar recursos de manera eficiente.

4.2 Evaluación de Impacto

La evaluación del impacto de los riesgos ayudará a determinar la gravedad de un posible ataque o fallo. Identificar qué sistemas, procesos y datos son más críticos para la operativa de la empresa permitirá establecer prioridades para la protección de estos elementos.

5. Plan de Capacitación en Ciberseguridad para los Empleados

5.1 Concientización y Formación

Es fundamental incluir un programa de capacitación en ciberseguridad para los empleados. Este programa debe incluir temas como:

- **Buenas prácticas de seguridad**: creación de contraseñas seguras, uso de MFA, y prevención de ataques de phishing.
- **Uso seguro de dispositivos**: precauciones al acceder a redes públicas o dispositivos personales.
- **Simulacros de ciberseguridad**: ejercicios prácticos de respuesta a incidentes de seguridad.

5.2 Evaluación Continua del Conocimiento

Además de la capacitación inicial, se debe implementar un sistema de evaluación continua para asegurar que el personal esté actualizado con las últimas amenazas y técnicas de defensa.

6. Integración con Otras Herramientas de Seguridad

6.1 Firewall y Sistemas de Prevención de Intrusiones (IPS)

La implementación de un firewall avanzado y un sistema de prevención de intrusiones (IPS) ayudará a monitorear y bloquear ataques en tiempo real.

6.2 Soluciones Antivirus y Antimalware

Todos los dispositivos de los empleados deben tener soluciones antivirus y antimalware actualizadas para protegerse contra software malicioso.

7. Cumplimiento Normativo y Estándares de Seguridad

7.1 Cumplimiento de Normativas y Regulaciones

La empresa debe verificar que cumpla con las normativas de seguridad y privacidad de datos vigentes, tales como GDPR, la Ley de Protección de Datos Personales, o estándares internacionales como ISO 27001.

7.2 Auditorías Regulares de Seguridad

Las auditorías periódicas garantizarán que las políticas y medidas de seguridad se mantengan efectivas.

8. Plan de Respuesta a Incidentes

8.1 Procedimientos de Respuesta a Incidentes de Seguridad

Debe detallarse un protocolo claro sobre cómo reaccionar ante un incidente de seguridad. Esto incluye la detección temprana, aislamiento del incidente, y recuperación.

8.2 Equipo de Respuesta a Incidentes

Es recomendable establecer un equipo especializado en respuesta a incidentes de seguridad (CSIRT) disponible 24/7.

9. Evaluación y Mejora Continua

9.1 Revisiones Periódicas del Plan de Seguridad

La ciberseguridad debe ser revisada y mejorada constantemente para adaptarse a nuevas amenazas.

9.2 Feedback de los Usuarios

El personal debe proporcionar retroalimentación sobre las políticas y medidas de seguridad, ayudando a identificar áreas de mejora.

10. Conclusión

Este informe presenta un enfoque integral para abordar la ciberseguridad dentro del programa PHP de la empresa. Implementar las medidas descritas protegerá los sistemas y datos de la empresa, garantizará la continuidad del negocio y el cumplimiento de las normativas vigentes. La capacitación continua, la respuesta proactiva ante incidentes y el monitoreo constante son elementos clave para mantener una postura de seguridad efectiva.