Universidad Nacional Autónoma de México

Secretaría de Desarrollo Institucional

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Lineamientos de Seguridad de la Información en Sitios Web de la UNAM

Diciembre de 2022

Contenido

Lineamientos de Seguridad de la Información en Sitios Web de la UNAM

Introducción

En 2021, la Comisión Especial de Seguridad (CES) del H. Consejo Universitario en su sesión ordinaria del 1° de diciembre del 2021, aprobó el Plan Maestro de Seguridad UNAM 2021-2024, el cual fue emitido por la Secretaría de Prevención, Atención y Seguridad Universitaria (SPASU) y como resultado de un esfuerzo impulsado por la CES y el Rector, en conjunto con la SPASU.

El Plan Maestro de Seguridad UNAM 2021-2024 tiene como misión, establecer los ejes rectores, programas y líneas de acción en materia de seguridad universitaria, protección civil, movilidad y transporte para el conjunto de entidades académicas, dependencias universitarias y zonas comunes de la UNAM, con el propósito de salvaguardar a la comunidad universitaria, el patrimonio universitario, el territorio, las actividades y el prestigio de la Universidad, a través del desarrollo y fortalecimiento de las capacidades institucionales y la configuración de políticas para tales propósitos.

En el Eje Rector 1 del Plan Maestro de Seguridad UNAM 2021-2024, línea de acción 20, establece como un objetivo, el fortalecer la seguridad de las redes sociales y las páginas oficiales de la Universidad.

Es por ello que la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) emite estos lineamientos técnicos para que cada entidad académica y dependencia universitaria implemente acciones que robustezcan la seguridad de sus sitios web.

Capítulo I

Disposiciones Generales

1. El presente documento tiene como propósito establecer lineamientos y recomendaciones en seguridad de la información aplicables al desarrollo, operación y/o actualización de sitios web institucionales y que están a cargo de las entidades y dependencias universitarias de la Universidad Nacional Autónoma de México (UNAM) a fin de robustecer la seguridad de los sitios web universitarios.
2. El alcance de los lineamientos y recomendaciones es aplicable a los sitios web institucionales de la UNAM. Están dirigidos al personal universitario que interviene en el proceso de instalación, configuración, desarrollo, operación, actualización y/o mantenimiento de sitios web institucionales.
3. Los presentes lineamientos y recomendaciones son aplicables por los responsables de los sitios web institucionales de la UNAM y las áreas vinculadas de manera directa o indirecta con los servicios, activos de información, aplicaciones e infraestructura que los soportan.
4. Los presentes lineamientos son de carácter obligatorio, mientras que las recomendaciones se sugieren para que sean adoptadas por las entidades y dependencias universitarias de acuerdo con sus necesidades y recursos disponibles.
5. Se recomienda al menos una revisión anual de la implementación de los presentes lineamientos y cada vez que haya cambios significativos en el sistema operativo, servidor web y/o sitio web de las entidades y dependencias universitarias.
6. El responsable TIC debe participar en la implementación o supervisión de los presentes lineamientos.

7. Para los efectos de los presentes Lineamientos, se entenderá por:

I. **Control de acceso:** Asegurar que el acceso a los activos esté autorizado y restringido de acuerdo con los requerimientos de seguridad y de las entidades y dependencias universitarias.

II. **Contraseña:** Una cadena protegida/privada de letras, números y/o caracteres especiales utilizados para autenticar una identidad o para autorizar el acceso a los datos.

III. **Respaldo:** Una copia de los archivos y programas realizados para facilitar su recuperación en caso de ser necesario.

IV. **Entidades y Dependencias universitarias**: Todas aquellas áreas universitarias que realizan actividades de docencia, investigación, difusión, extensión universitaria y gestión, como son facultades, escuelas, unidades multidisciplinarias, institutos y centros de investigación, áreas de extensión universitaria, así como dependencias de apoyo y de servicios.

V. **Responsable TIC**. Responsable del área de informática, cómputo o afín que tiene a su cargo las funciones de tecnología de información y comunicación, designado(a) por el o la titular de la entidad o dependencia universitaria y que funge como representante ante la Red de Responsables de TIC (REDTIC).

VI. **HTTPS**: Es el Protocolo seguro de transferencia de hipertexto (en inglés, Hypertext Transfer Protocol Secure) es un protocolo de aplicación basado en el protocolo HTTP, con el objetivo de realizar la transferencia segura de datos de hipertexto, y es la versión segura de HTTP.

VII. **Política de contraseñas seguras**. Comprende un mínimo de ocho caracteres que incluyan letras mayúsculas y minúsculas, caracteres especiales y que no sean palabras de diccionario.

VIII. **Privilegios**: Un permiso que se asigna a un individuo, programa o proceso.

IX. **Sitios web institucionales**: Son los portales y/o páginas web institucionales pertenecientes a la UNAM cuyo propósito es apoyar las funciones sustantivas que tienen a su cargo las entidades académicas o dependencias administrativas.

X. **Vulnerabilidad**: Debilidad en un control o activo que puede ser explotada por una o más amenazas provocando un impacto negativo en la confidencialidad, la integridad o la disponibilidad.

Capítulo II

Seguridad en el sistema operativo del servidor web

8. Con el objetivo de mejorar la seguridad del sistema operativo contra amenazas y ataques, es necesario apegarse a los siguientes lineamientos durante la instalación, configuración y mantenimiento del sistema operativo.

I. Los sistemas operativos deben estar actualizados para corregir vulnerabilidades conocidas.

II. Se debe mantener desconectado el servidor de redes innecesarias, conectarlo únicamente a redes aseguradas por medidas de protección perimetral.

III. Eliminar o deshabilitar del sistema operativo todos los servicios y aplicaciones que no sean utilizados.

IV. Instalar la versión mínima del sistema operativo y posteriormente agregar o eliminar servicios y aplicaciones como sea necesario.

V. Eliminar o deshabilitar los grupos y cuentas de usuario instalados de forma predeterminada que no se requieran.

VI. Cambiar los nombres y contraseñas de los grupos y cuentas predeterminadas que se requieran en el sistema operativo.

VII. Establecer una política de contraseñas seguras.

VIII. Implementar tecnologías de encriptación en la autenticación como el Secure Sockets Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH) o Virtual Private Network (VPN) para mantener la seguridad de la información transmitida.

IX. Configurar bajo un conjunto mínimo de privilegios los accesos individuales para archivos, directorios, dispositivos y otros recursos computacionales.

X. Asignar control de acceso para permisos de lectura, escritura y ejecución a los recursos del sistema operativo.

XI. Instalar y configurar programas antimalware, antivirus, antispyware y detectores de rootkit.

XII. Instalar y configurar firewalls para proteger al servidor de accesos no autorizados.

XIII. Instalar y configurar programas (software) que protejan la integridad de los archivos críticos del sistema operativo.

XIV. Instalar y configurar los programas (software) que monitoreen los recursos del sistema operativo.

Capitulo III

Seguridad en el servidor web

9. La seguridad del servidor web incluye las acciones necesarias para mantener la integridad, disponibilidad y confidencialidad de la información del sitio web y del propio servidor.

I. Instalar los parches y actualizaciones para corregir vulnerabilidades conocidas.

II. Crear una partición lógica o física dedicada para el contenido web.

III. Separar el contenido web de la aplicación del servidor web.

IV. Eliminar o deshabilitar los servicios instalados por el servidor web que no son requeridos.

V. Eliminar o deshabilitar todas las cuentas de usuario creadas de forma predeterminada por la instalación del servidor web.

VI. Eliminar del servidor web toda la documentación del fabricante o restringir el acceso a la misma.

VII. Eliminar todos los archivos de ejemplo o de prueba del servidor, incluidos los scripts y código ejecutable.

VIII. Reconfigurar el banner del servicio HTTP y cualquier otro para no proporcionar información sobre el servidor web, el sistema operativo y la versión.

IX. Considerar una instalación del servidor web con nombres y ubicación de directorios y archivos no estándar.

X. Controlar los accesos a los archivos de configuración de la aplicación web, de almacenamiento del hash de contraseñas, los que contienen información de la autenticación, de llaves criptográficas, archivos de bitácoras y registros de auditoría y de contenido web.

XI. Configurar los procesos de servicio para ejecutarse por un usuario con un conjunto estrictamente limitado de privilegios.

XII. Permitir o denegar la carga de archivos a través de la aplicación web, de acuerdo con el propósito del sitio.

XIII. Asignar un límite de espacio en disco duro para las cargas o subidas de archivos.

XIV. Asignar una partición específica para almacenar los archivos que se suben a través de la aplicación web.

XV. Limitar el tamaño de los archivos que se suben a través de la aplicación web dependiendo de las necesidades de la organización y de los recursos disponibles para el almacenamiento de los mismos.

XVI. Asegurar que los archivos cargados por la aplicación web no sean leídos por el servidor web hasta que se utilice algún proceso manual o automático de revisión para examinarlos.

XVII. Asegurar que las bitácoras están almacenadas en una partición con suficiente espacio y que haya una rotación periódica de las mismas.

XVIII. Configurar un número máximo de procesos del servidor web y de las conexiones de red que serán permitidas.

XIX. Limitar el acceso a la aplicación del servidor web a un conjunto de recursos computacionales.

Capítulo IV

Administración del servidor web

10. En esta sección, se describen las prácticas relacionadas con el desarrollo, operación y mantenimiento de los sitios web, que deben ser implementadas por las entidades y dependencias universitarias para mantener la seguridad de la información:

I. Implementar un conjunto mínimo de privilegios y deshabilitar cuentas y permisos innecesarios.

II. Cambiar todos los nombres de usuario y contraseñas instalados por defecto en el servidor web.

III. Establecer una política de contraseñas seguras.

IV. Asignar los permisos mínimos necesarios para la operación de la aplicación web.

V. Verificar el límite apropiado de la entrada de datos por parte de los usuarios.

VI. Actualizar a la versión libre de vulnerabilidades las herramientas utilizadas en la aplicación web incluyendo el servidor web.

VII. Descargar las aplicaciones y/o herramientas de sitios web oficiales.

VIII. Mantener el código fuente lo más simple posible.

IX. Restringir las acciones de escritura, lectura y ejecución de los programas fuente a las mínimas necesarias.

X. Restringir la interacción de los programas fuente únicamente con programas o aplicaciones necesarias.

XI. Determinar una lista de caracteres permitidos para ingresar en los formularios y filtrar aquellos no permitidos antes de procesar el formulario. Es recomendable el uso de expresiones regulares.

XII. Mantener en todo momento la aplicabilidad del criterio de la confidencialidad y la protección a los datos personales y sensibles al solicitar y publicar información.

XIII. Atender las regulaciones y controles en materia de tratamiento de datos personales y/o sensibles. Especialmente el “Acuerdo por el que se establecen los Lineamientos para la Protección de Datos Personales en posesión de la Universidad Nacional Autónoma de México” y las “Normas complementarias sobre medidas de seguridad técnicas, administrativas y físicas para la protección de datos personales en posesión de la Universidad“.

XIV. Identificar los tipos de bitácoras que existen en el servidor web y el formato que manejan.

XV. Seleccionar los tipos de bitácoras y el formato convenientes para contar con información útil para el análisis de eventos.

XVI. Habilitar el registro de bitácoras con los datos correctos relacionados con el servidor web, con la información del sistema operativo y de la red.

XVII. Monitorear las bitácoras del sitio web para detectar eventos de seguridad o accesos indebidos.

XVIII. Contar con procedimientos y herramientas para procesar y analizar las bitácoras y revisar las alertas y notificaciones.

XIX. Monitorear el tamaño de las bitácoras, archivando y eliminándolas periódicamente y/o reduciendo su nivel de detalle.

XX. Considerar el almacenamiento de las bitácoras por un tiempo determinado acorde a las necesidades de la organización, a requerimientos legales, al tamaño de los archivos, al valor de los datos del servicio web y al nivel de amenaza.

XXI. Definir en la política de respaldos las aplicaciones web que abarca, frecuencia y tipo de respaldos, tiempo de retención y eliminación segura de los respaldos. Los respaldos pueden ser completos, incrementales o diferenciales según sea necesario.

XXII. Mantener los respaldos en un entorno seguro y físicamente distinto al servidor que aloja la aplicación web.

XXIII. Realizar procedimientos sobre la realización y restauración de respaldos que especifique las actividades y la secuencia en que estas se deben llevar a cabo.

Capítulo V

Recomendaciones

Seguridad en el sistema operativo del servidor web

11. Los siguientes puntos si bien no son obligatorios, ayudan a complementar los lineamientos y es recomendable aplicarlos para proteger en mayor medida el sistema operativo.

I. Configurar el sistema operativo para prevenir la adivinación/predicción de las contraseñas denegando el acceso a un cierto número de equivocaciones de contraseña.

II. Forzar a que la contraseña expire cada seis meses y que no se pueda reutilizar.

III. Instalar y configurar programas de detección y prevención de intrusos para detectar ataques realizados contra el servidor web, incluidos los ataques DoS.

IV. Dedicar el sistema operativo al servidor web únicamente (un solo propósito, idealmente).

V. Implementar firewalls de aplicaciones web (WAF).

Seguridad en el servidor web

12. Se recomienda las siguientes acciones a fin de proteger el servidor web.

I. Instalar el servidor web en un servidor dedicado.

II. Limitar el acceso a los usuarios a través de controles adicionales.

Administración del servidor web

13. Se sugiere realizar las siguientes en la administración del servidor web.

I. Aplicar autenticación multifactor para los inicios de sesión u otras transacciones a través de las cuentas de usuario que sean accesibles desde internet, priorizando aquellas que tienen accesos privilegiados.

II. Implementar una política que determine qué tipo de información se puede publicar abiertamente, qué información publicar con acceso restringido y qué información se debe omitir de un sitio web público.

III. Verificar periódicamente el código fuente ya que podría contener información confidencial o sensible u otros detalles acerca del servidor web y/o sistema operativo.

IV. Reducir o eliminar el uso de cookies de sesión.

V. Personalizar el contenido del sitio web a la imagen institucional de la dependencia universitaria de acuerdo con los “Lineamientos para sitios web institucionales de la UNAM”.

VI. Almacenar las bitácoras en un servidor distinto al servidor web, con el propósito de permitir operaciones de búsqueda históricas de anomalías.

VII. Utilizar una solución de respaldos que realice copias de seguridad automáticas y continuas de los datos críticos y configuraciones del sitio web.

VIII. Implementar una solución de redundancia para los respaldos.

IX. Probar escenarios de recuperación ante desastres.

X. Mantener un servidor web en ambiente de pruebas a fin de probar en éste los nuevos parches y actualizaciones, los nuevos desarrollos y contenidos y las nuevas configuraciones, así como mantener el funcionamiento de programas y aplicaciones necesarias para la operación del ambiente de pruebas.

XI. Auditar y reforzar las configuraciones en función de listas de verificación de seguridad específicas para cada aplicación (por ejemplo, Apache, MySQL) en el sistema.

XII. Utilizar aplicaciones web que permitan listar y deshabilitar módulos o funciones que proporcionen funcionalidades que no son necesarias para las necesidades de la organización.

XIII. Implementar protecciones de secuencias de comandos entre sitios (Cross-Site Scripting, XSS) y falsificación de solicitudes entre sitios (Cross Site Request Forgery, CSRF) para los usuarios y para el sitio web.

XIV. Instalar los parches de todas las vulnerabilidades críticas y altas dentro de los 15 y 30 días, respectivamente. Buscar vulnerabilidades de configuración y de software y corregirlas.

XV. Identificar y remediar los 10 riesgos de seguridad más críticos en aplicaciones web y posterior a ello continuar con las vulnerabilidades menos críticas. (Consultar OWASP Top 10 para obtener una lista de los riesgos de seguridad de aplicaciones web más críticos).

Créditos

Rector
Dr. Enrique Luis Graue Wiechers

Secretaria de Desarrollo Institucional
Dra. Patricia Dolores Dávila Aranda

Director General de Cómputo y de Tecnologías de Información y Comunicación
Dr. Héctor Benítez Pérez

Coordinación DGTIC, UNAM
Dra. Ana Yuri Ramírez Molina
M. en C. María de Lourdes Velázquez Pastrana
Mtro. Juan Manuel Castillejos Reyes

Elaboración DGTIC, UNAM
M. en C. Carlos Raúl Tlahuel Pérez
M.T.I.A Esther Lugo Rojas
M.I. Adriana Cruz García

Revisión técnica
Ing. Arturo Bahena Armas – DGAPA, UNAM
M.T.I.A Esther Lugo Rojas – DGTIC, UNAM
Mtro. Jesús Ojeda Arévalo – DGCP. UNAM
Ing. Luis Armando Sánchez Ruiz – SG, UNAM

Revisión jurídica
Mtra. Elizabeth Rangel Gutiérrez – DGTIC, UNAM
Lic. José Luis Chávez Sánchez – DGTIC, UNAM

Revisión estructural y publicación en NormaTIC
Mtra. Ma. Teresa Ventura Miranda – DGTIC, UNAM
L.A. Heidi Alejandra Pérez Vera – DGTIC, UNAM