SEP

SECRETARÍA DE
EDUCACION PUBLICA

Marco de Gestión de Seguridad de la Información (MGSI)

PROGRAMA DE GESTIÓN DE VULNERABILIDADES

Ing. Leonardo Rafael Sánchez Ferreiro
Coordinador General del Centro Nacional de Cálculo
Responsable de la Seguridad de Información Institucional

Mtro. Axel Avilés Pallares
Director de Cómputo y Comunicaciones

Enero, 2024

PROGAMA DE GESTIÓN DE VULNERABILIDADES

Nombre del documento	**Programa de Gestión de Vulnerabilidades**		
Elaboración:	Ing. César Ramón Hernández Portillo Ingeniero del Departamento de Seguridad Informática		
Revisión:	Ing. Roberto Muñoz Castro Jefe del Departamento de Seguridad Informática Ing. Federico Juárez de la Fuente Coordinador Técnico de la CG del CENAC Ricardo Sánchez Payán Líder implementador del Marco de Gestión de Seguridad de la Información		
Aprobación:	Mtro. Axel Avilés Pallares Director de Cómputo y Comunicaciones		
Autorización:	Ing. Leonardo Rafael Sánchez Ferreiro Coordinador General del CENAC Responsable de la Seguridad de Información Institucional		
Fecha de elaboración:	15/01/2023	**Fecha de aprobación:**	15/01/2024

CONTROL DE VERSIONES

Fecha	Versión	Observaciones/Comentarios	Autor
15/01/2024	1.0	Primera Versión	Ing. César Ramón Hernández Portillo

CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVOS 5
3. ALCANCE 5
4. PROGRAMA DE ANÁLISIS DE VULNERABILIDADES 6
5. FASES DEL PROGRAMA DE GESTIÓN DE VULNERABILIDADES 8
6. MARCO NORMATIVO 10

PROGRAMA DE GESTIÓN DE VULNERABILIDADES

1. INTRODUCCIÓN.

Con base en el **ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal**, publicado en el Diario Oficial de la Federación el **6 de septiembre de 2021**; y de conformidad con:

CAPÍTULO VI

Seguridad de la Información

Artículo 75.- Las Instituciones deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI) alineado a la política general de SI, que procure los máximos niveles de confidencialidad, integridad y disponibilidad de la información generada, recibida, procesada, almacenada y compartida por dichas Instituciones, a través de sus sistemas, aplicaciones, infraestructura y personal; dicho MGSI deberá contribuir al cumplimiento de los objetivos institucionales, de TIC, regulatorios, organizacionales, operativos y de cultura de la seguridad de la información.

Artículo 76.- El MGSI deberá conformarse, al menos por los siguientes elementos:

a) El establecimiento de objetivos alineados a la política general de seguridad de la información;

....

e) **Programa de gestión de vulnerabilidades**, que incluya su identificación, evaluación y corrección. La identificación de las mismas deberá partir de un análisis de vulnerabilidades al interior de la Institución, así como de las alertas o investigaciones de seguridad divulgadas por fuentes externas;

El "Programa de gestión de vulnerabilidades" está orientado a garantizar certidumbre en la disponibilidad, confidencialidad e integridad de la información institucional y a fortalecer la seguridad de la información de los Sistemas Críticos Institucionales y los activos esenciales que los soportan.

El presente documento contiene los objetivos, fases y formatos, que derivan de este Programa de Gestión de Vulnerabilidades y que funciona paralelamente con el Procedimiento de Análisis de Vulnerabilidades.

2. OBJETIVOS

Objetivo General:

Establecer el proceso del Programa de Gestión de Vulnerabilidades, que realizará el Departamento de Seguridad Informática a los activos definidos como críticos Institucionales.

Objetivos Específicos:

- Realizar la gestión de la programación de la evaluación de los análisis de vulnerabilidades de los sistemas, aplicaciones o sitios web Institucionales para identificar, evaluar y tratar las vulnerabilidades halladas.
- Evitar incidentes de seguridad al detectar posibles fallas de configuración para evitar su explotación.
- Determinar las medidas de seguridad adecuadas para mitigar o reducir las vulnerabilidades en los activos Institucionales.

3. ALCANCE

El "Programa de Gestión de Vulnerabilidades" forma parte de las actividades de implementación del Marco de Gestión de Seguridad de la Información y es de observancia obligatoria en el Instituto Politécnico Nacional, y aplica a los Sistemas Críticos Institucionales y a todos los activos esenciales que soporten dichos sistemas críticos.

Como parte de los esfuerzos institucionales en materia de seguridad de la información, la implementación de un Programa de Gestión de Vulnerabilidades permite reducir los riesgos de materialización de incidentes cibernéticos al realizar análisis periódicos calendarizados a los Sistemas Críticos Institucionales y su infraestructura de soporte, así como por alertas de vulnerabilidades que afecten a los elementos que soportan a los servicios, publicados en los boletines de ciberseguridad y alertas. El contar con configuraciones seguras, parches de seguridad actualizados y software y firmware en sus últimas versiones reduce la superficie de ataque y la exposición de nuestros Sistemas Críticos Instituciones, fundamentales para la operación diaria en el Instituto Politécnico Nacional.

4. PROGRAMA DE ANÁLISIS DE VULNERABILIDADES

El programa de análisis de vulnerabilidades consistirá en la evaluación programada de forma trimestral para los siguientes Activos Críticos Institucionales (ACI):

- Sistema de Correo Electrónico Institucional
- Sistema de Administración Escolar
- Sistema de Recursos Humanos y Nómina

El control de la evaluación de los análisis de vulnerabilidades estará a cargo del Departamento de Seguridad Informatica; la ejecución de este programa se constituirá acorde a las diferentes fases definidas en el apartado 5 del presente documento.

PROGRAMA DE ANÁLISIS DE VULNERABILIDADES (PAdV) PARA "APLICACIONES, SITIOS WEB O ACTIVOS CRÍTICOS INSTITUCIONALES (ACI)"

Sistema de Correo Electrónico Institucional

Trimestre	Actividad	Fecha Programada para AdV	Responsable	Fecha de Cumplimiento de Remediación de Vulnerabilidades	Responsable
1er. Trimestre	Ejecución de análisis de vulnerabilidades en plataforma de correo electrónico	02/02/2024	Departamento de Seguridad Informatica	12/02/2024	Área de correo electrónico Institucional
2do. Trimestre	Ejecución de análisis de vulnerabilidades en plataforma de correo electrónico	06/05/2024	Departamento de Seguridad Informatica	13/05/2024	Área de correo electrónico Institucional
3er. Trimestre	Ejecución de análisis de vulnerabilidades en plataforma de correo electrónico	26/08/2024	Departamento de Seguridad Informatica	02/09/2024	Área de correo electrónico Institucional
4to. Trimestre	Ejecución de análisis de vulnerabilidades en plataforma de correo electrónico	04/11/2024	Departamento de Seguridad Informatica	11/12/2024	Área de correo electrónico Institucional

Sistema de Administración Escolar					
Trimestre	**Actividad**	**Fecha Programada para AdV**	**Responsable**	**Fecha de Remediación y Seguimiento de Vulnerabilidades**	**Responsable**
1er. Trimestre	Ejecución de Análisis de vulnerabilidades en los SAES de las diferentes Unidades Académicas Institucionales	06/02/2024	Departamento de Seguridad Informatica	29/02/2024	Administrador(es) SAES
2do. Trimestre	Ejecución de Análisis de vulnerabilidades en los SAES de las diferentes Unidades Académicas Institucionales	13/05/2024	Departamento de Seguridad Informatica	14/06/2024	Administrador(es) SAES
3er. Trimestre	Ejecución de Análisis de vulnerabilidades en los SAES de las diferentes Unidades Académicas Institucionales	02/09/2024	Departamento de Seguridad Informatica	30/09/2024	Administrador(es) SAES
4to. Trimestre	Ejecución de Análisis de vulnerabilidades en los SAES de las diferentes Unidades Académicas Institucionales	12/11/2024	Departamento de Seguridad Informatica	16/12/2024	Administrador(es) SAES

Sistema de Recursos Humanos y Nómina					
Trimestre	**Actividad**	**Fecha Programada para AdV**	**Responsable de AdV**	**Fecha de Remediación de Vulnerabilidades**	**Responsable de Remediación**
1er. Trimestre	Análisis de Vulnerabilidades en los Sistemas de RH y Nomina Institucional	04/03/2024	Departamento de Seguridad Informática	14/03/2024	Área de Sistemas de RH y Nomina Institucional
2do. Trimestre	Análisis de Vulnerabilidades en los Sistemas de RH y Nomina Institucional	27/05/2024	Departamento de Seguridad Informática	10/06/2024	Área de Sistemas de RH y Nomina Institucional
3er. Trimestre	Análisis de Vulnerabilidades en los Sistemas de RH y Nomina Institucional	23/09/2024	Departamento de Seguridad Informática	07/10/2024	Área de Sistemas de RH y Nomina Institucional
4to. Trimestre	Análisis de Vulnerabilidades en los Sistemas de RH y Nomina Institucional	09/12/2024	Departamento de Seguridad Informática	18/12/2024	Área de Sistemas de RH y Nomina Institucional

5. FASES DEL PROGRAMA DE GESTIÓN DE VULNERABILIDADES

5.1. Detección

En esta fase se identificarán y mapearan los activos que intervienen en el procedimiento de análisis de vulnerabilidades para su ejecución con la coordinación y participación de los encargados involucrados de TI de los activos críticos Institucionales para su correcta evaluación.

Para esta fase es indispensable identificar los puntos de exposición de la superficie de ataque, asimismo, para obtener una visibilidad completa se deberá escanear todo aquello que conforma el ecosistema como son, servidor(es), sitio(s) o aplicación(es) web, dominio(s), dirección(es) IP que correspondan, así como a los elementos de infraestructura que soportan a los diferentes activos críticos.

Las actividades de esta fase corresponden en los numerales 1 al 9 de la descripción del proceso del Anexo A "Procedimiento de Análisis de Vulnerabilidades".

5.2. Planificación y Evaluación

La evaluación del análisis de vulnerabilidades se programará y notificará vía correo electrónico para realizar la ejecución del escáner de vulnerabilidades de acuerdo al procedimiento del análisis de vulnerabilidades del Anexo A; en la fecha y horario acordado por el Departamento de Seguridad Informática y el responsable del activo a evaluar, para que no exista afectación en la disponibilidad de los servicios.

La evaluación del análisis de vulnerabilidades será efectuada por la herramienta de escaneo que cubre el rango de las familias de vulnerabilidades del top 10 de OWASP. Asimismo, el ambiente de pruebas será dentro de la Red Interna Institucional.

5.3. Clasificación y Priorización

La herramienta de análisis de vulnerabilidades clasifica estas con los siguientes niveles de riesgo: informativo, bajo, medio, alto y crítico. Del resultado de la evaluación vulnerabilidades del activo Institucional se generará un informe de la herramienta donde aparecerán las vulnerabilidades clasificadas por el nivel de riesgo.

Al realizar los escaneos y obtener los resultados correspondientes, como se indica en el procedimiento de análisis de vulnerabilidades (Anexo A), dependiendo si son halladas vulnerabilidades de nivel de severidad crítica, alta, media o baja se elaborará el documento "Reporte de Análisis de Vulnerabilidades"; en éste se describirán las vulnerabilidades halladas (CWE, CERT, OWASP, CISA, CVE) y en su caso, la correspondiente solución para la mitigación de la vulnerabilidad.

Ante el panorama actual de constantes ataques y amenazas, el administrador del activo deberá dar prioridad para realizar la remediación de las vulnerabilidades de nivel crítico, alto, que cuenten con un exploit (independiente del nivel de riesgo) o posean una actividad de alcance o impacto alto; estas serán indicadas en el documento "Reporte de Análisis de Vulnerabilidades", y se establecerá un tiempo de número horas de remediación, una vez hecho el conocimiento de la misma.

El Departamento de Seguridad Informática enviará los resultados vía correo electrónico del escáner realizado a los activos para su corregir las vulnerabilidades descubiertas.

Las actividades de esta fase corresponden a los numerales 10.1 al 10.5. de la descripción del proceso del Anexo A "Procedimiento de Análisis de Vulnerabilidades.

5.4. Corrección

Una vez recibido los resultados y el reporte del análisis correspondiente, el administrador del activo realizará las acciones correspondientes para la mitigación, de las vulnerabilidades reportadas, asegurando que las vulnerabilidades de mayor riesgo se mitiguen inicialmente. Una vez que se hayan mitigado las vulnerabilidades, el administrador del activo, avisará mediante correo electrónico al Ingeniero de Servicio del Departamento de Seguridad han sido resueltas, asimismo indicará la fecha y horario posible para realizar nuevamente el escaneo de vulnerabilidades para la verificación de la corrección de la(s) vulnerabilidad(es).

Las actividades de esta fase corresponden al numeral 11 de la descripción del proceso del Anexo A "Procedimiento de Análisis de Vulnerabilidades.

5.5. Validación

El ingeniero de servicio notificara mediante correo electrónico la fecha y horario de la nueva evaluación del análisis de vulnerabilidades para verificar la remediación de las vulnerabilidades reportadas.

Si el resultado del análisis indica que se han mitigado las vulnerabilidades es decir si es satisfactorio, se notificará mediante correo electrónico que han sido solventadas las vulnerabilidades al Administrador del activo; en caso contrario, si la vulnerabilidad persiste o la acción de remediación ha generado nuevas vulnerabilidades, se notifica nuevamente al Administrador, para que tome las acciones necesarias para la correcta remediación.

Las actividades de esta fase corresponden a los numerales 12 al 16 de la descripción del proceso del Anexo A "Procedimiento de Análisis de Vulnerabilidades.

5.6. Monitoreo y Escaneo Continuo

El Departamento de Seguridad Informática, realizará el escaneo continuo de los activos evaluados acorde al Programa de Análisis de Vulnerabilidades, integrado por los Formatos de Registro de Análisis de Vulnerabilidades (FRAdV), asimismo, cuando se presenten amenazas emergentes y/o vulnerabilidades riesgosas que amenacen o pongan en un riesgo alto a los servicios de los activos Institucionales, o cuando ameriten llevar a cabo esta actividad por la solicitud del administrador del activo, dado que haya realizado un cambio, actualización u otro.

Para los elementos que soportan a los diferentes activos críticos identificados en la fase número uno (Detección), el Departamento de Seguridad Informática aplicará una inspección de forma continua en la lista de información registrada sobre vulnerabilidades de seguridad conocidas (CVE) de severidad crítica, para evaluar el estado de riesgo en que puedan encontrarse los activos señalados. Los resultados de la inspección se harán llegar a los responsables de TI de los activos correspondientemente.

Las actividades de esta fase corresponden en los numerales a 1 al 7 de la descripción del Anexo B "Procedimiento de Monitoreo de Vulnerabilidades Criticas a Elementos de Infraestructura Institucionales".

6. MARCO NORMATIVO

6.1. Constitución

6.1.1. Constitución Política de los Estados Unidos Mexicanos en su última reforma vigente.

6.2. Leyes

6.2.1. Ley Orgánica de la Administración Pública Federal vigente.

6.2.2. Ley Orgánica del Instituto Politécnico Nacional vigente.

6.2.3. Ley de Firma Electrónica Avanzada vigente.

6.2.4. Ley General de Transparencia y Acceso a la Información Pública vigente

6.2.5. Ley Federal de Transparencia y Acceso a la Información vigente.

6.2.6. Ley General de Responsabilidades Administrativas vigente.

6.2.7. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados vigente.

6.2.8. Ley General de Archivo vigente.

6.3. Reglamentos

6.3.1. Reglamento de la Ley de Firma Electrónica Avanzada vigente.

6.3.2. Reglamento Orgánico del Instituto Politécnico Nacional vigente.

6.4. Decretos

6.4.1. Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaría en el ejercicio del gasto público, así como, para la modernización de la Administración Pública Federal vigente.

6.5. Acuerdos

6.5.1. ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal. D.O.F. 6 de septiembre de 2021.

6.5.2. Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal vigente.

6.6. Políticas

6.6.1. Política Institucional de Seguridad de la Información v5, Instituto Politécnico Nacional, marzo 2023

6.6.2. Política Institucional de Uso Aceptable de las Tecnologías de Información y Comunicaciones, Instituto Politécnico Nacional, marzo 2023

6.7. Lineamientos

6.7.1. Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal vigente.

6.7.2. Lineamientos para la Operación, Funcionalidad, Comunicación y Seguridad de los Sistemas Automatizados de Control de Gestión vigente. Secretaría de Hacienda y Crédito Público.

6.7.3. Lineamientos de Protección de Datos Personales vigente.

6.8. Plan Nacional de Desarrollo

6.8.1. Plan Nacional de Desarrollo 2018-2024.

6.9. Estándares, normas y documentos

6.9.1. Recomendaciones en materia de seguridad de datos personales, vigente. D.O.F.

6.9.2. Acta de Instalación del Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI).

6.9.3. Documento de Integración del Grupo Estratégico del Marco de Gestión de Seguridad de la Información (GEMGSI).

6.9.4. ISO/IEC 27001:2022 Requerimientos del Sistema de Gestión de Seguridad de la Información

6.9.5. ISO/IEC 27002:2022 Controles de Seguridad de la Información
6.9.6. ISO/IEC 27005:2022 Gestión de Riesgos de Seguridad de la Información
6.9.7. ISO/IEC 27035:2023 Gestión de Incidentes de Seguridad de la Información, Parte 1 y 2
6.9.8. ISO 22301:2019 Requerimientos del Sistema de Gestión de la Continuidad del Negocio
6.9.9. ISO/TS 22317 Guía para el Análisis de Impacto al Negocio
6.9.10. Procedimiento de Análisis de Vulnerabilidades