e

**Informe de seguimiento a pruebas de seguridad a sitios de Ingresar aquí nombre de grupo**

${MES} ${ANIO}

|  |  |
| --- | --- |
| Elaboración de Documento | |
| Pentester | ${PENTESTER}  ${nombre\_pentester}  ${/PENTESTER} |
| Revisión | ${nombre\_revisor} |
| Visto Bueno | ${nombre\_visto\_bueno} |

[Resumen ejecutivo 4](#_Toc62745446)

[Objetivos 5](#_Toc62745447)

[Alcance 5](#_Toc62745448)

[Estado actual de Seguridad 6](#_Toc62745449)

[Recomendaciones generales 7](#_Toc62745450)

[Anexo A. Recomendaciones específicas 8](#_Toc62745451)

[Anexo B. Hallazgos por activo de información 10](#_Toc62745452)

# Resumen ejecutivo

En atención a la solicitud recibida el ddd de MMM de AAA y en seguimiento al “Informe de pruebas de seguridad al sitio ${SITIO\_WEB}”, la Coordinación de Seguridad de la Información UNAM-CERT (CSI/UNAM-CERT) llevó a cabo seguimiento a pruebas de penetración y análisis de vulnerabilidades a los sitios web XXXX, alojado en el centro de datos de la DGTIC.

Las pruebas consistieron en la identificación y análisis de vulnerabilidades, que bajo ciertas condiciones podrían ser aprovechadas para provocar alguna afectación en la confidencialidad, integridad o disponibilidad de los activos de información. En el presente informe se documentan los resultados de las pruebas y, con base en ellos, se emiten recomendaciones que incluyen acciones correctivas y preventivas orientadas a fortalecer el esquema de seguridad actual.

De la verificación de atención de recomendaciones se resumen los resultados en la siguiente tabla:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Hallazgos Mitigados de la revisión previa | | | | | | |
| **ID ACTIVO** | **DOMINIIO** | **CRITICOS** | **ALTO** | **MEDIO** | **BAJO** | **SIN IMPACTO** |
| **ACT${id\_activoR1}** | ${SITIO\_WEB} | ${c\_criticoP} | ${c\_altoP} | ${c\_medioP} | ${c\_bajoP} | ${c\_niP} |

Como resultado de las pruebas se identificó que persisten tres hallazgos, uno de impacto bajo y dos sin impacto según la calificación establecida a través del Common Vulnerability Scoring System Version 3.1. Es importante mencionar que uno de los hallazgos persistente fue atendido de manera parcial, pero persiste debido a que parte del hallazgo continua.

De la verificación de atención de recomendaciones se resumen los resultados en la siguiente tabla:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Hallazgos persistentes detectados durante la verificación | | | | | | |
| **ID ACTIVO** | **DOMINIO** | **CRITICOS** | **ALTO** | **MEDIO** | **BAJO** | **SIN IMPACTO** |
| **ACT${id\_activoR2}** | ${SITIO\_WEB} | ${c\_critico} | ${c\_alto} | ${c\_medio} | ${c\_bajo} | ${c\_ni} |

El hallazgo de impacto bajo se refieren a que el aplicativo es susceptible a ataques de fuerza bruta. En el caso de los hallazgos clasificados sin impacto se presentan debido a la ausencia de encabezados de seguridad y a la exposición de versiones.

A partir de los resultados de las pruebas de penetración y los hallazgos documentados, los administradores del sitio deberán evaluar la aplicación de las recomendaciones emitidas en el presente informe e implementar las que considere pertinentes, verificando que la medida correctiva adoptada no genere problemas en la operación de los servicios.

# Objetivos

* Identificar y documentar el estado actual de seguridad en la infraestructura tecnológica del sistema, para evaluar su impacto asociado a los hallazgos encontrados durante las pruebas.
* Verificar la mitigación de las vulnerabilidades preliminares reportadas.
* Emitir recomendaciones para la mitigación de los hallazgos identificados.

# Alcance

Realizar seguimiento a pruebas de seguridad de tipo caja negra (no se contó con información acerca del código o lógica con la que fue programado) al objetivo que se presentan en la Tabla 1, el dd de mmmm de aaa.

| **ID activo** | **Descripción** | **Dirección IP** |
| --- | --- | --- |
| **ACT${id\_activoA}** | **${SITIO\_WEB}** | **${dir\_IP}** |

Tabla 1. Alcance de las pruebas de seguridad.

# Estado actual de Seguridad

A continuación, se presentan los hallazgos encontrados durante las pruebas de seguridad, ejecutándose desde la Coordinación de Seguridad de la Información.

Se asocia al activo un nivel de impacto en función de la complejidad y las condiciones que deben presentarse para que un evento de esta naturaleza ocurra. Para determinar el impacto se utilizó una puntuación basada en *Common Vulnerability Scoring System* (CVSS v3.1), la cual es una metodología para el puntaje de vulnerabilidades de TI utilizada a nivel internacional. La calificación obtenida ayuda a priorizar la atención de vulnerabilidades identificadas en activos de TI con base en las características de esta respecto a la afectación potencial en la confidencialidad, integridad o disponibilidad de la información, en los sistemas y/o en la infraestructura, en caso de que sea explotada.

En la primera columna de la tabla se encuentra el identificador del activo, posteriormente su dirección IP. Los hallazgos se documentan en la columna Hallazgo/Vulnerabilidad, la siguiente columna representa el identificador de la recomendación que se asocia con el hallazgo o vulnerabilidad, la descripción detallada de las recomendaciones se encuentra en el Anexo A. En la columna restante se presenta el impacto asociado el cual fue calculado utilizando el CVSS. Los detalles de los hallazgos se describen en Anexo B.

| **ID activo** | **Dirección IP /**  **URL** | **Hallazgo/**  **Vulnerabilidad** | **ID**  **REC** | **Impacto** | **Estatus** |
| --- | --- | --- | --- | --- | --- |
| **ACT${id\_activoE}** | ${ACTIVO} | ${nombre\_hallazgo} | **${rec\_id}** | **${nivel\_impacto\_n}**  **${nivel\_impacto}** | **${estatus}** |

# 

# Recomendaciones generales

Se debe evaluar el impacto de las medidas correctivas asociadas a cada recomendación para no afectar la continuidad de los servicios que ofrece la infraestructura. En caso necesario, se sugiere evaluar otras formas de mitigar el impacto identificado para el activo de información.

Las recomendaciones más relevantes que se desprenden de los hallazgos obtenidos de las pruebas son:

${RECOMENDACIONES}

* ${recomendación\_general\_h}

${/RECOMENDACIONES}

# Anexo A. Recomendaciones específicas

${TABLA\_H}

|  |  |
| --- | --- |
| ID | ${REC} |
| Hallazgo / vulnerabilidad | **${nombre\_hallazgo}** |
| Descripción | ${descripcion\_hallazgo} |
| Solución | ${recomendacionG\_hallazgo} |
| Referencias | ${url\_hallazgo} |
| CVSS versión 3.1 | **${DETALLES\_H}**  **${nivel\_impacto\_n} ${nivel\_impacto}**  Vector  **${cvss\_hallazgo}**  **${DETALLES\_H}** |

${/TABLA\_H}

# Anexo B. Hallazgos por activo de información

**${ANEXOB}**

**ACT${idSitio} ${URL\_SITIO} / ${DIR\_IP}**

**${HALLAZGOB}**

|  |  |
| --- | --- |
| **Descripción** | **CVSS v3.1** |
| **${nombre\_hallazgo}** | **${nivel\_impacto\_n}**  **${nivel\_impacto}** |

${descripcion\_hallazgo}

${descripcion\_hall\_rev}

**Algunos recursos afectados:**

${RECURSOS}

* ${recurso\_afectado}

${RECURSOS}

${IMAGENES}

${imagen}

Imagen ${contadorImg}. ${descripcion\_img}

${IMAGENES}

**${HALLAZGOB}**

**${/ANEXOB}**