e

**Informe de pruebas de seguridad al sitio web ${SITIO\_WEB}**

${MES} ${ANIO}

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

[Resumen ejecutivo 4](#_Toc62577337)

[Objetivos 5](#_Toc62577338)

[Alcance 5](#_Toc62577339)

[Estado actual de Seguridad 6](#_Toc62577340)

[Recomendaciones generales 7](#_Toc62577341)

[Anexo A. Recomendaciones específicas 8](#_Toc62577342)

[Anexo B. Hallazgos por activo de información 11](#_Toc62577343)

[Anexo C. Common Vulnerability Scoring System version 3 16](#_Toc62577344)

# Resumen ejecutivo

En atención a la solicitud recibida el pasado DD de MM de AAAA, la Coordinación de Seguridad de la Información UNAM-CERT (CSI/UNAM-CERT) llevó a cabo pruebas de penetración y análisis de vulnerabilidades los días DD al DD de MM de AAAA al sitio web ${SITIO\_WEB}, 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.

Como resultado de las pruebas se identificaron seis hallazgos, uno de impacto medio, uno de impacto bajo y cuatro sin impacto según la calificación establecida a través del Common Vulnerability Scoring System Versión 3 (Anexo C).

La siguiente tabla muestra la cantidad de hallazgos identificados por activo.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID ACTIVO | sitio | CRITICOS | ALTO | MEDIO | BAJO | SIN IMPACTO |
| **ACT01** | ${SITIO\_WEB} | ${c\_critico} | ${c\_alto} | ${c\_medio} | ${c\_bajo} | ${c\_ni} |

Ingresa en esta sección a qué se deben los tipos de hallazgos encontrados por nivel.

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

* Obtener la mayor cantidad de información de los servicios proporcionados en el sitio definido en el alcance, mediante la aplicación de técnicas y ejecución de pruebas de penetración que permitan conocer su nivel de exposición.
* 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.
* Intentar explotar las debilidades encontradas en las pruebas de penetración, a fin de determinar el impacto potencial que tendría sobre la infraestructura tecnológica.
* Verificar la mitigación de las vulnerabilidades preliminares reportadas.
* Emitir recomendaciones para la mitigación de los hallazgos identificados.

# Alcance

Realizar 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, los días DD al DD de MM de AAAA.

| **ID activo** | **Descripción** | **Dirección IP** |
| --- | --- | --- |
| **ACT01** | **${SITIO\_WEB}** | **${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. Para más información sobre la metodología consultar el Anexo C.

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** |
| --- | --- | --- | --- | --- |
| **ACT 01** | ${ACTIVO} | ${nombre\_hallazgo} | **REC${rec\_id}** | **${nivel\_impacto\_n}**  **${nivel\_impacto}** |

# 

# 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 | ${url\_hallazgo} |
| CVSS versión 3.1 | **${nivel\_impacto\_n} ${nivel\_impacto}**  Vector  **${cvss\_hallazgo}** |

${/TABLA\_H}

# Anexo B. Hallazgos por activo de información

**ACT01** **${SITIO\_WEB} / ${DIR\_IP}**

**${ANEXOB}**

|  |  |
| --- | --- |
| **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}

**${/ANEXOB}**

# Anexo C. Common Vulnerability Scoring System version 3.1

El *Common Vulnerability Scoring System* (CVSS) toma las principales características técnicas de vulnerabilidades en *software, hardware* y *firmware.* El resultado es un valor numérico que indica la severidad de una vulnerabilidad en relación con otras vulnerabilidades.

CVSS está compuesta por tres grupos de métricas: Base, Temporales y Entorno. La calificación Base refleja la severidad de una vulnerabilidad de acuerdo con sus características intrínsecas, las cuales son constantes a lo largo del tiempo y asume el peor escenario a través de diferentes ambientes. Las métricas Temporales modifican la severidad de la Base de una vulnerabilidad basado en factores que cambian conforme pasa el tiempo, tales como la disponibilidad del código de un *exploit*. Las métricas de Entorno modifican la severidad de las Base y Temporales para un ambiente especifico, éstas consideran factores tales como la presencia de mitigantes en ese ambiente.

Las calificaciones Base son generadas por la organización que mantiene el producto vulnerable, o un tercero. Es típico solo publicar la métrica Base, debido a que no cambia con el tiempo y es común a todos los ambientes. Los usuarios del CVSS deben complementar la calificación Base con la calificación Temporal y de Entorno del producto vulnerable para obtener una severidad más exacta de acuerdo con el ambiente de la organización. Los usuarios del CVSS pueden utilizarlo como entrada para un proceso de gestión de vulnerabilidades que consideren factores que no son parte del CVSS en orden de clasificar las amenazas a su infraestructura tecnológica y tomar decisiones sobre la remedición. Tales factores pueden incluir: número de clientes en una línea de productos, amenazas contra la propiedad o la vida, pérdidas monetarias debido a una brecha o el sentir público para una vulnerabilidad divulgada extensamente. Estos están fuera del alcance del presente documento del CVSS.

Los beneficios del CVSS incluyen la provisión de un proveedor estandarizado y una metodología que califica las vulnerabilidades para todas las plataformas. Es un marco abierto, que proporciona transparencia a las características individuales y la metodología utilizada para obtener una calificación.

# Grupos de métricas

CVSS está compuesta por tres grupos de métricas: Base, Temporales y Entorno, cada una consiste en un conjunto de métricas como se muestra en la Imagen 1.

**Grupo de Métricas Base**

Métricas de Explotación Métricas de Impacto

Vector de Ataque

Impacto a la   
Confidencialidad

Complejidad de Ataque

Impacto a la   
Integridad

**Confidencialidad**

Impacto a la   
Disponibilidad

**Confidencialidad**

Privilegios Requeridos

Interacción del  
Usuario

**Alcance**

**Confidencialidad**

**Grupo de Métricas Temporales**

Nivel de Maduración de la Explotación

Nivel de Remediación

Reporte de Confianza

**Grupo de   
Métricas de Entorno**

Requerimiento de Confidencialidad

Requerimiento de Integridad

Requerimiento de Disponibilidad  
Requerida

Métricas Base Modificadas

Imagen 1. Grupos de métricas de CVSS v3.1.0

Los grupos de métricas pueden describirse como:

* **Métricas Base**: representan las características intrínsecas de una vulnerabilidad que es constante a lo largo del tiempo y entorno del usuario. Se compone de tres métricas: Métricas de Explotación, Métricas de Impacto y Métrica de Alcance.
  + **Métricas de Explotación** reflejan las características técnicas necesarias y facilidad de explotación de una vulnerabilidad. *Representa la parte que es vulnerable,* es decir, el *componente vulnerable*.
  + **Métricas de Impacto** hacen referencia a las consecuencias de un ataque exitoso. Representa la *parte que sufre el impacto*, es decir, *el componente impactado*.
  + **Métrica de Alcance** permite reflejar si la vulnerabilidad afecta a un componente en específico (componente vulnerable) o podría afectar a otros elementos (componente impactado) diferentes al componente vulnerable.
* **Métricas temporales**: muestra las particularidades de una vulnerabilidad que podrían cambiar a lo largo del tiempo, pero no debido al entorno donde se encuentre. Por ejemplo, la existencia de un *exploit* para la vulnerabilidad aumenta la calificación CVSS, mientras que la creación de una actualización oficial debería disminuirla.
* **Métricas de entorno**: define las propiedades de una vulnerabilidad que son relevantes y únicas para el entorno particular de un usuario u organización. Estas métricas permiten considerar los controles existentes que podrían mitigar cualquier consecuencia de un ataque exitoso, así como promover o denotar la importancia de la vulnerabilidad de acuerdo con el riesgo de la organización.

# La calificación CVSS

Cuando a las Métricas Base se les asignan valores, la ecuación calcula una calificación que va de 0 a 10 y genera una cadena de texto que contiene los valores asignados a cada métrica. La cadena de texto se utiliza para indicar cómo se deriva la puntuación de su respectiva vulnerabilidad, a esta cadena se le denomina **vector** y debe mostrarse con la calificación de la vulnerabilidad.

La calificación **Base** puede ser modificada por las calificaciones de las **Métricas** **Temporales** y **Entorno** con el fin de obtener mayor exactitud del riesgo que produce una vulnerabilidad dentro del entorno de la organización donde se presenta. Las calificaciones de métricas Temporales y Entorno no son requeridas, pero es recomendable que se evalúen para mayor precisión.

Por lo general, el grupo de **Métricas Base y Temporales** son especificadas en boletines de seguridad o por parte de los proveedores de productos de seguridad, quienes cuentan con más información sobre las características de una vulnerabilidad. El grupo de **Métricas de Entorno** es especificado por los usuarios pertenecientes a la organización afectada, debido a que tienen un mejor entendimiento acerca del posible impacto que pueda generar la vulnerabilidad en sus organizaciones.

Todas las métricas son evaluadas bajo la consideración de que un atacante ha identificado la vulnerabilidad.

# Métricas base

Las Métricas Base evalúan características de una vulnerabilidad constante en el tiempo y en el entorno del usuario.

# Métricas de explotación

Reflejan las características del dispositivo vulnerable, al cual nos referimos como el *componente vulnerable.* Por lo tanto, cada métrica de explotación listada a continuación debe ser calificado con relación al componente vulnerable, y reflejar las propiedades de la vulnerabilidad que conducen a un ataque exitoso.

Al evaluar las Métricas Base, se debe asumir que el atacante tiene un conocimiento de las debilidades del sistema objetivo, incluyendo configuraciones generales y mecanismos de protección predeterminados (*firewalls* integrados, límites de velocidad de transferencia, política de tráfico de la red). Por ejemplo, explotar una vulnerabilidad con resultados repetibles, debería ser considerada con un valor de Complejidad de Ataque bajo, independiente de los conocimientos o capacidades del atacante. Además, mitigaciones de impacto en el objetivo atacado (por ejemplo, filtrado especifico en el *firewall*, listas de control de acceso) deben ser reflejados en las métricas de Entorno.

Configuraciones especificas deberían no impactar a cualquier atributo de la calificación Base del CVSS, es decir, si una configuración especifica es necesaria para que un ataque sea exitoso, el componente vulnerable debería ser evaluado asumiendo que se tiene esa configuración.

# Vector de ataque (AV)

Esta métrica refleja el contexto por el cual la explotación de una vulnerabilidad es posible. El valor de esta métrica (y consecuentemente la calificación Base) deberá ser mayor si es posible la explotación vía **Red** del componente vulnerable a que la explotación sea **Local** o **Física**. Esta suposición deriva del número de potenciales atacantes para la vulnerabilidad, la cual aumenta si esta puede ser explotada a través de la red y de esa manera tener un valor mayor en la calificación Base, y la calificación disminuye debido a la posibilidad de que se tenga acceso físico al dispositivo afectado. Los posibles valores son listados en la Tabla 1.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Red (N) | El componente vulnerable está ligado a la red y el conjunto de posibles atacantes se extienda más allá de las opciones listadas a continuación, incluyendo la internet. Dicha vulnerabilidad se denomina “remotamente explotable” y el ataque puede ser a nivel de protocolo o través de una o varias redes, por ejemplo, a través de uno o más ruteadores. Un ejemplo de un ataque de red es una denegación de servicio (DoS) enviando un paquete TCP especialmente diseñado a través de la red pública, Internet (ejemplo de lo anterior es el CVE-2004-0230). |
| Adyacente (A) | El componente vulnerable está ligado a la red, pero el ataque está limitado a nivel de protocolo a una *red adyacente.* Esto significaque el ataque debe ser lanzado desde el mismo espacio físico (por ejemplo, Bluetooth, IEEE 802.11), o una red lógica (por ejemplo, una subred local), o desde un dominio administrativo o limitado (ejemplo es una MPLS, una VPN a una zona de red administrativa). Un Ejemplo de un ataque adyacente son ARP (IPv4) o la inundación excesiva durante un descubrimiento (IPv6) para generar una negación de servicio en el segmento local. Ver también CVE-2013-6014. |
| Local (L) | El componente vulnerable no está ligado a la red y la vía de ataque es a través de la capacidad de lectura/escritura/ejecución del componente. Ya sea:   * El ataque explota la vulnerabilidad accediendo al sistema objetivo localmente (por ejemplo: teclado, consola) o remotamente (ejemplo, SSH) , o * El ataque depende en la interacción del usuario por otra persona para realizar las acciones requeridas para explotar la vulnerabilidad (por ejemplo, utilizar técnicas de ingeniería social para engañar a un usuario legitimo a abrir un documento malicioso). |
| Físico(P) | El ataque requiere *acceso físico* que pueda manipular el componente vulnerable. La interacción física puede ser breve o continua. Un ejemplo de tal ataque es el ataque de reinicio de plataforma, el cual permite a un atacante ganar acceso a las llaves de cifrado de disco. Otros ejemplos son los ataques a periféricos a través de *Firewire*/USB. |

Tabla 1. Evaluación de Vector de Ataque (AV).

Guía de evaluación: Cuando se decida entre Red y Adyacente, si un ataque puede ser lanzado a través de un WAN o desde fuera de una red lógica adyacente, utilizar Red. Red debería ser usado incluso si el ataque requiere estar en la misma intranet para explotar el sistema vulnerable (por ejemplo, el atacante solo puede explotar la vulnerabilidad desde dentro de una red corporativa).

# Complejidad de ataque (AC)

Describe las condiciones que un atacante requiere para explotar una vulnerabilidad. Tales condiciones podrían requerir, reunir una mayor información acerca del objetivo o excepciones computacionales. Algo importante a mencionar es que esta métrica excluye todos los requisitos para la interacción con el usuario, debido a que tales condiciones se evalúan en la Métrica Interacción del Usuario. Si una configuración especifica es requerida para que el ataque sea exitoso, las métricas Base deberían ser calificadas asumiendo que el componente vulnerable está en esa configuración (lo anterior no aplica a configuraciones que están explícitamente contraindicadas). La calificación Base es más grande para ataques con menos complejidad. Los posibles valores para esta métrica se listan en la Tabla 2.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Baja (L) | No existen condiciones especiales de acceso o circunstancias extenuantes. Un atacante puede explotar de manera exitosa el componente vulnerable en repetidas ocasiones. |
| Alta (H) | Un ataque exitoso depende de ciertas condiciones, más allá del control del componente vulnerable por parte del atacante, es decir, requiere que el atacante invierta tiempo en la preparación y ejecución antes de explotar alguna vulnerabilidad contra el componente vulnerable. Por ejemplo, un ataque exitoso depende de que se cumpla alguna de las siguientes condiciones:   * El atacante debe reunir información acerca del ambiente en el cual el objetivo/componente vulnerable existe. Por ejemplo, recolectar detalles de las configuraciones del objetivo, secuencia de números, secretos compartidos, entre otros. * El atacante debe preparar el objetivo para tener una explotación exitosa. Por ejemplo, explotaciones continuas para obtener una condición de carrera o el uso de *exploits* avanzados. * El atacante debe introducirse dentro de la red lógica entre el objetivo y los recursos de la víctima con el fin de leer y/o modificar las comunicaciones de red (por ejemplo, el ataque de hombre en medio MitM). |

Tabla 2. Evaluación de Complejidad del Ataque (AC).

Como se describe en la sección de *Métricas de explotación*, conocimiento detallado del componente vulnerable esta fuera de la Complejidad de ataque. Referirse a esta sección cuando se tengan mitigantes para evaluar la complejidad de ataque.

# Privilegios requeridos (PR)

La métrica describe el nivel de privilegios que un atacante debe poseer antes de explotar exitosamente la vulnerabilidad. La calificación Base es mayor si no se requieren privilegios. Los posibles valores están listados en la Tabla 3.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Ninguno(N) | El atacante no está autorizado antes del ataque, y por lo tanto no requiere algún acceso a configuraciones o archivos del sistema vulnerable para llevar a cabo el ataque. |
| Bajo (L) | El atacante requiere privilegios que permiten capacidades básicas, las cuales sólo podrían afectar configuraciones y archivos del usuario. Alternativamente, un atacante con privilegios mínimos sólo puede acceder a recursos no sensibles. |
| Alto (H) | El atacante requiere privilegios que podrían afectar las configuraciones y archivos del componente vulnerable. Por ejemplo, privilegios administrativos. |

Tabla 3. Evaluación de Privilegios Requeridos (PR).

Guía de evaluación: Privilegios Requeridos es usualmente Ninguno para vulnerabilidades de credenciales en el código o vulnerabilidades que requieren ingeniería social (por ejemplo, *Cross Site Scripting* reflejado, *Cross Request Forgery*, o vulnerabilidad de análisis de archivo en un lector de PDF).

# Interacción del usuario (UI)

Esta métrica considera al usuario real, no al atacante, en la participación de un ataque satisfactorio al componente vulnerable. Esta métrica determina si la vulnerabilidad puede ser explotada únicamente a voluntad del atacante, o si un usuario (o proceso iniciado por un usuario) debe participar de alguna manera. La calificación Base será mayor, cuando no se requiera interacción del usuario. Los posibles valores están listados en la Tabla 4.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Ninguno (N) | El sistema vulnerable puede ser explotado sin la interacción de algún usuario. |
| Requerido (R) | Se requiere que un usuario realice alguna acción antes de que la vulnerabilidad sea explotada. Por ejemplo, la explotación exitosa puede ser posible durante la instalación de algún aplicativo con privilegios administrativos. |

Tabla 4. Evaluación de Interacción del Usuario (UI).

# Métrica Alcance (S)

La métrica de Alcance determina si una vulnerabilidad en un componente vulnerable impacta los recursos de componentes más allá de su alcance de seguridad.

Formalmente, una autoridad de seguridad es un mecanismo (por ejemplo, una aplicación, un sistema operativo, firmware, un ambiente controlado) que define y hace cumplir el control de acceso en términos de como ciertos sujetos y actores (usuarios, procesos) pueden acceder a ciertos objetos/recursos restringidos de una manera controlada (por ejemplo, archivos, CPU, memoria) . Todos los sujetos y objetos bajo la jurisdicción de una simple autoridad de seguridad son considerados bajo el mismo alcance de seguridad. Si una vulnerabilidad en un componente vulnerable puede afectar un componente en una alcance de seguridad diferente al componente vulnerable, un Cambio en el Alcance ocurre. Intuitivamente, cada vez que el impacto de una vulnerabilidad viola un límite de seguridad/confianza e impacta componentes fuera del alcance de seguridad en el que reside el componente vulnerable, se produce un Cambio en el Alcance.

El alcance de seguridad de un componente engloba otros componentes que proporcionan funcionalidad solamente a ese componente, incluso si esos otros componentes tienen su propia autoridad de seguridad. Por ejemplo, una base de datos utilizada solamente por una aplicación es considerada parte de un alcance de seguridad para esa aplicación incluso si la base de datos tiene su propia autoridad de seguridad, ejemplo de lo anterior es un mecanismo que controla el acceso a los registros de la base de datos en función de los usuarios de la base de datos y los privilegios asociados a la base de datos.

La calificación Base de la vulnerabilidad será mayor cuando el Alcance cambie. Los posibles valores están listados en la Tabla 5.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Sin cambios (U) | Al explotar la vulnerabilidad solamente se afectan recursos administrados por la misma autoridad. En este caso el componente vulnerable y el componente impactado son el mismo o ambos son manejados por la misma autoridad de seguridad. |
| Cambio(C) | Al explotar la vulnerabilidad se pueden afectar recursos fuera de los privilegios autorizados previstos para el componente vulnerable. En este caso, el componente vulnerable y el componente impactado son diferentes y administrados por diferentes autoridades de seguridad. |

Tabla 5. Evaluación de Alcance (S).

# Métricas de impacto

Las métricas de impacto reflejan los efectos de una explotación exitosa a una vulnerabilidad, sobre el componente que sufre el peor resultado de manera directa y previsiblemente con el ataque. Se deben limitar los impactos a aquellos que sean razonables a poder ser alcanzables por un atacante.

Solo el incremento en accesos, privilegios obtenidos u otras consecuencias negativas como resultado de la explotación deberían ser considerados cuando se evalúan las métricas de impacto de una vulnerabilidad. Por ejemplo, considerare una vulnerabilidad que requiere permisos de solo lectura antes de poder explotar la vulnerabilidad. Después de una explotación exitosa, el atacante mantiene los mismos permisos de lectura, y obtiene permisos de escritura. En este caso, solo la métrica de impacto en la Integridad debería ser calificada, y las métricas de Confidencialidad y Disponibilidad deberían ser calificadas a Ninguno.

Notar que cuando se observa un cambio en la delta de impacto, el impacto final debería ser usado. Por ejemplo, si un atacante inicia con accesos parciales para información restringida (Confidencialidad Baja) y una explotación exitosa de la vulnerabilidad resulta en la pérdida total de la confidencialidad (Confidencialidad Alta), entonces el resultado de la calificación Base de CVSS debería hacer referencia al resultado final del valor de la métrica de impacto (Confidencialidad Alta).

Si un cambio de Alcance no ha sucedido, las métricas de impacto deberían reflejar el impacto de la confidencialidad, integridad y disponibilidad al *componente vulnerable*. Sin embargo, si el cambio de Alcance sucede, entonces las métricas de impacto deberían reflejarse para cualquier componente vulnerable o componente afectado, reflejando el valor más severo en el impacto de la confidencialidad, integridad y disponibilidad.

# Impacto a la confidencialidad (C)

Esta métrica califica el impacto a la confidencialidad de la información del recurso administrado por el componente después de la explotación exitosa de una vulnerabilidad. La confidencialidad se refiere a limitar el acceso y divulgación de la información solamente a usuarios autorizados, así como evitar el acceso o divulgación de información a personas no autorizadas. La calificación Base aumenta cuando la pérdida del componente impactado es más alta. Los posibles valores para esta métrica son listados en la Tabla 6.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Alto (H) | Hay una pérdida total de la confidencialidad, resultando en el acceso a toda la información por parte del atacante. Alternativamente, el acceso a alguna información restringida es posible, pero la información obtenida presenta un serio impacto. Por ejemplo, el atacante obtiene contraseñas administrativas o llaves privadas de un servidor web. |
| Bajo (L) | Hay una cierta pérdida de la confidencialidad. Es posible el acceso a cierta información, pero el atacante no tiene control sobre lo que puede obtener, o la pérdida es limitada. La información divulgada no presenta un impacto serio al componente. |
| Ninguno (N) | No hay pérdida de confidencialidad del componente afectado. |

Tabla 6. Evaluación de Confidencialidad (C).

# Impacto a la integridad (I)

Esta métrica califica el impacto a la integridad después de la explotación exitosa de una vulnerabilidad. La integridad se refiere a la veracidad y confiabilidad de la información. La calificación Base aumenta cuando la pérdida del componente impactado es más alta. Los valores posibles para esta métrica están listados en la Tabla 7.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Alto (H) | Hay una pérdida total de la integridad, o una completa pérdida de la protección. Por ejemplo, el atacante puede modificar cualquiera/todos los archivos del componente afectado. Alternativamente, sólo algunos archivos pueden ser modificados, pero con consecuencias importantes en el componente afectado. |
| Bajo (L) | La modificación de datos es posible, pero el atacante no tiene control en las modificaciones o la cantidad de modificaciones es reducida. La modificación de datos no tiene un impacto importante sobre el componente afectado. |
| Ninguno (N) | No hay pérdida de la integridad del componente afectado. |

Tabla 7. Evaluación de Integridad (I).

# Impacto a la disponibilidad (A)

Esta métrica califica el impacto a la disponibilidad después de la explotación exitosa de una vulnerabilidad. Esta métrica se refiere a la pérdida de disponibilidad del componente impactado, tal como servicios de red (por ejemplo, sitios web, bases de datos o correos electrónicos). La disponibilidad se refiere a la accesibilidad de los recursos de información, ataques que consumen ancho de banda, ciclos de procesador, o espacio en disco que impacten la disponibilidad del componente afectado. La calificación Base aumenta cuando la pérdida del componente impactado es más alta. Los valores posibles para esta métrica son listados en la Tabla 8.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Alto (H) | Hay una interrupción total de la disponibilidad, dando como resultado la denegación de acceso al recurso del componente afectado; esta pérdida de acceso se mantiene (mientras el atacante continúa realizando el ataque) o es persistente (la condición continúa incluso después de que el ataque ha sido completado). Alternativamente, el atacante tiene la habilidad de denegar cierta disponibilidad, pero la pérdida de disponibilidad presenta una seria consecuencia al componente afectado (por ejemplo, el atacante no puede interrumpir las conexiones existentes, pero puede evitar nuevas conexiones; el atacante puede explotar de manera repetida una vulnerabilidad, que cada vez que sea exitosa provoca la fuga una pequeña cantidad de memoria, pero después de repetidas explotaciones causa que el servicio se encuentre completamente indisponible). |
| Bajo (L) | Hay una reducción en el rendimiento o interrupciones en la disponibilidad del recurso. Incluso si se explota de manera repetida la vulnerabilidad, el atacante no tiene la posibilidad de completar la negación de servicio a usuarios legítimos. Los recursos en el componente afectado se encuentran parcialmente disponibles o indisponibles durante algún tiempo, pero no hay consecuencias directas al componente afectado. |
| Ninguno (N) | No hay impacto a la disponibilidad del componente afectado. |

Tabla 8. Evaluación de Disponibilidad (A).

# Métricas Temporales

Las métricas temporales miden el estado actual de las técnicas de explotación o código disponible, la existencia de alguna actualización de seguridad o solución temporal, o la confianza que se tiene en la descripción de la vulnerabilidad.

# Nivel de maduración de la explotación (E)

Esta métrica mide la probabilidad de que la vulnerabilidad sea explotada, las técnicas de explotación conocidas, *exploit* disponible o explotación activa en Internet. La existencia de un *exploit* público y fácil de usar, incrementa el número de atacantes potenciales, incluyendo aquéllos que no cuentan con experiencia en su uso, por lo tanto, incrementa la severidad de la vulnerabilidad. Los posibles valores para esta métrica están listados en la Tabla 9. Mientras menor dificultad tenga explotar una vulnerabilidad, mayor es su calificación.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| No definida (X) | Asignar este valor indica que no se cuenta con información suficiente para seleccionar otro valor, y no tiene impacto en la calificación general de la métrica Temporal, es decir, tiene el mismo efecto que asignar el valor Alto. |
| Alto (H) | No se requiere la existencia de código funcional o *exploit* y los detalles de la explotación se encuentran ampliamente disponibles. El *exploit* funciona en todos los escenarios o es empleado de manera activa a través de un gusano o un virus. Los sistemas conectados a la red presentan intentos de explotación y escaneos. El *exploit* desarrollado ha alcanzado el nivel de confiabilidad en donde es utilizado en herramientas automatizadas. |
| Funcional (F) | El código funcional del *exploit* está disponible y funciona en diversos escenarios donde la vulnerabilidad existe. |
| Prueba de concepto (P) | Una prueba de concepto del *exploit* o una demostración del ataque que no es práctica para muchos sistemas se encuentra disponible. El código o técnica no es funcional en todos los escenarios y puede requerir modificaciones sustanciales por un atacante experimentado. |
| No probada (U) | No hay código funcional del *exploit* disponible o el *exploit* es conceptual. |

Tabla 9. Evaluación de Nivel de Maduración de la Explotación (E).

# Nivel de remediación (RL)

El nivel de remediación de una vulnerabilidad es un factor importante para priorizar. Correcciones provisionales pueden ofrecer una solución temporal hasta que una actualización oficial se publique. Cada una de estas etapas modifica la calificación de las métricas temporales, reflejando la disminución de esta en cuanto la solución es definitiva. Los valores posibles para esta evaluación están listados en la Tabla 10. Mientras no sea oficial o permanente una solución, más alta será la calificación.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| No definida (X) | Asignar este valor indica que no se cuenta con información suficiente para seleccionar otro valor, y no tiene impacto en la calificación general de la métrica Temporal, es decir, tiene el mismo efecto que asignar el valor No disponible. |
| No disponible (U) | No hay una solución disponible o es imposible de aplicar. |
| Solución provisional (W) | Hay disponible una solución no oficial de un tercero. En algunos casos, los usuarios con la tecnología afectada pueden generar una corrección o proveer alguna guía para mitigar la vulnerabilidad. |
| Solución temporal (T) | Hay una solución oficial pero temporal. Incluye los casos donde el proveedor emite una corrección temporal, herramienta o solución. |
| Solución oficial (O) | Existe una solución completa de un proveedor, el vendedor ha publicado una corrección oficial o una actualización se encuentra disponible. |

Tabla 10. Evaluación de Nivel de Remediación (RL).

# Reporte de confianza (RC)

Esta métrica evalúa el grado de confianza en la existencia de la vulnerabilidad y la credibilidad de los detalles técnicos conocidos de la misma. Algunas veces la existencia de la vulnerabilidad es publicada, pero sin detalles técnicos o puede ser incluso corroborada y confirmada por el autor o proveedor de la tecnología. Esta métrica también sugiere el nivel de conocimiento que tienen los atacantes al respecto. Los valores posibles están listados en la Tabla 11. La calificación será mayor cuando una vulnerabilidad es validada por un proveedor u otras fuentes de buena reputación.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| No definida (X) | Asignar este valor indica que no se cuenta con información suficiente para seleccionar otro valor, y no tiene impacto en la calificación general de la métrica Temporal, es decir, tiene el mismo efecto que asignar el valor Confirmada. |
| Confirmada (C) | Existen reportes detallados de la vulnerabilidad, es reproducible, y existen *exploits*. Código fuente se encuentra disponible para confirmar lo mencionado por el investigador o el proveedor confirma la existencia de la vulnerabilidad |
| Razonable(R) | Existen publicaciones, pero los investigadores no tienen una completa certeza de la principal causa de la vulnerabilidad o no tiene acceso al código fuente que les permita confirmarla. Sin embargo, la vulnerabilidad es reproducible o existe una prueba de concepto de esta. Un ejemplo es un reporte de investigación de la vulnerabilidad en la cual se da una explicación (posiblemente ofuscada) que da la certeza de cómo reproducirla. |
| Desconocido(U) | Existen reportes que indican que la vulnerabilidad existe. Los reportes no indican que causa la vulnerabilidad o son contradictorios. Un ejemplo es el reporte de una falla donde se menciona una intermitencia por un cierre inesperado, pero no reproducible, la evidencia de corrupción de memoria sugiere una negación de servicio o posiblemente impacto más severo puede resultar. |

Tabla 11. Evaluación de Reporte de Confianza (RC).

# Métricas de entorno

Estas métricas permiten ajustar la calificación CVSS, dependiendo de la importancia del activo de TI afectado dentro de la organización y evaluando los controles de seguridad alternativos/complementarios aplicados. Estas métricas son el equivalente modificado de las métricas base y las calificaciones son asignadas de acuerdo con el lugar que el componente tiene dentro de la organización.

# Requerimientos de seguridad (CR, IR, AR)

Permiten ajustar la calificación CVSS dependiendo de la importancia del activo de TI dentro de la organización, evaluando en términos de confidencialidad, integridad y disponibilidad. Esto es, si un activo de TI admite un área de negocio para el que la disponibilidad es más importante, se puede asignar un mayor valor, en comparación con la confidencialidad e integridad. Cada requerimiento de seguridad tiene cuatro posibles valores: “Bajo”, “Medio”, “Alto” y “No Definido”.

El efecto total en una evaluación del entorno está determinado por sus correspondientes modificadores de métricas base. Esto es, las métricas modifican la calificación del entorno, ponderando el impacto de las métricas modificadas de confidencialidad, integridad y disponibilidad. Por ejemplo, el impacto a la métrica de Confidencialidad Modificada (MC) se incrementa si la Confidencialidad Requerida (CR) es alta. Igualmente, el impacto a la métrica de Confidencialidad Modificada disminuye si el Requerimiento de Confidencialidad es bajo. El impacto a la métrica de Confidencialidad Modificada no se ve afectado si el Requerimiento de Confidencialidad es medio. El mismo proceso es aplicado para el Requerimiento de Integridad y Disponibilidad.

Es importante mencionar que el Requerimiento de Confidencialidad no deberá afectar la calificación de entorno si el impacto de la Métrica Base Modificada de Confidencialidad es asignado a No definido. También, incrementar el Requerimiento de Confidencialidad de medio a alto no cambiará la calificación de entorno cuando el impacto de la Métrica de Base Modificada sea colocado en alto. Esto es debido a que el impacto de la sub-calificación del impacto (parte de la calificación de la base modificada que calcula el impacto) se encuentra en su valor máximo de 10.

Los posibles valores para los requerimientos de seguridad están listados en la Tabla 12. La misma tabla es usada para las tres métricas: Requerimiento de Confidencialidad (CR), Requerimiento de Integridad (IR) y Requerimiento de Disponibilidad (AR). Mientras mayor sea el requerimiento de seguridad, más alta es la calificación, de manera predeterminada se considera el valor de “Medio”.

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| No definido (ND) | Asignar este valor a la métrica no influye en la calificación. Esto indica a la ecuación que debe saltarse esta métrica. |
| Alto (H) | Es posible que la pérdida de [confidencialidad | integridad | disponibilidad] muestre un efecto catastrófico y adverso en la organización o a las personas vinculadas con la organización (ejemplos: empleados, clientes). |
| Medio (M) | Es factible que la pérdida de [confidencialidad | integridad | disponibilidad] muestre un efecto serio y adverso en la organización o a las personas vinculadas con la organización (ejemplos: empleados, clientes). |
| Bajo (L) | Es posible que la pérdida de [confidencialidad | integridad | disponibilidad] tenga un efecto limitado y adverso en la organización o a las personas vinculadas con la organización. |

Tabla 12. Evaluación de los Requerimientos de Seguridad (CR, IR, AR).

# Métricas Base modificadas

Estas métricas permiten anular las métricas Base de manera individual, basado en características específicas del entorno del usuario. Características que afectan la Explotación, Alcance o Impacto pueden ser reflejadas adecuadamente a través de una modificación de la calificación de Entorno.

El efecto total de la calificación del entorno es determinado por la métrica Base correspondiente. Es decir, estas métricas modifican la calificación del entorno mediante la reasignación de los valores de métrica Base. Por ejemplo, la configuración predeterminada para un componente vulnerable podría ser la ejecución de un servicio con privilegios administrativos, por lo que un compromiso podría otorgar a un atacante confidencialidad, integridad y disponibilidad con impacto alto. A pesar de todo, en el entorno interno, el mismo servicio puede ser ejecutado con privilegios reducidos; en ese caso, el Modificador de Confidencialidad, Modificador de Integridad y Modificador de Disponibilidad son asignados con calificación baja.

Para reducir el documento, solo las métricas Base Modificadas son mencionadas. Cada métrica de entorno modificado tiene el mismo valor que su correspondiente en métricas Base, más el del valor No Definido. No Definido es la valor predeterminado y el valor asociado a la métrica Base.

La intención de esta métrica es definir la mitigación presente en determinados entornos internos. Es aceptable usar la métrica Modificador para describir situaciones que incrementa la calificación Base. Por ejemplo, la configuración predeterminada de un componente puede requerir privilegios elevados para acceder a una función en particular, pero en el análisis de entorno interno, puede no requerir los privilegios. Se puede establecer privilegios requeridos como Alto y Modificador de Privilegios Requeridos a Ninguno para reflejar mayor seriedad a la condición de su entorno.

En la Tabla 13 se mencionan los posibles valores que pueden tomar estas métricas:

|  |  |
| --- | --- |
| Valor de la métrica | Descripción |
| Modificador de Vector de Ataque (MAV) | Los mismos valores que el correspondiente a las **Métricas Base**, consideran de manera predeterminada el valor de “No definidas”. |
| Modificador de Complejidad de Ataque (MAC) |
| Modificador de Privilegios Requeridos (MPR) |
| Modificador de Interacción del Usuario (MUI) |
| Modificador de Alcance (MS) |
| Modificador de Confidencialidad (MC) |
| Modificador de Integridad (MI) |
| Modificador de Disponibilidad (MA) |

Tabla 13. Métricas base modificadas

# Escala de severidad

El *Common Vulnerability Scoring System* (CVSS) trabaja con una escala de puntuación del 0 al 10, y considera valores cualitativos para señalar el impacto sobre cada uno de los requerimientos de seguridad (confidencialidad, integridad y disponibilidad).

A continuación, en la Tabla 14 se muestran la equivalencia entre el valor y las métricas CVSS que se pueden obtener, así como una breve descripción donde se especifica la gravedad de la afectación sobre cada uno de los requerimientos de seguridad.

|  |  |  |
| --- | --- | --- |
| Valor CVSS | Valor de la métrica | Descripción |
| 0.0 | **Sin impacto** | No existe una posible pérdida de confidencialidad, integridad y disponibilidad, sobre la organización, activos de información o personas. |
| 0.1 – 3.9 | **Bajo** | Es posible que la pérdida de [confidencialidad | integridad | disponibilidad] sólo tenga un efecto limitado y adverso en la organización o las personas vinculadas con la organización. |
| 4.0 – 6.9 | **Medio** | Es factible que la pérdida de [confidencialidad | integridad | disponibilidad] muestre un efecto serio y adverso en la organización o las personas vinculadas con la organización. |
| 7.0 – 8.9 | **Alto** | Es probable que la pérdida de [confidencialidad | integridad | disponibilidad] tenga un efecto catastrófico y adverso en la organización o las personas vinculadas con la organización. |
| 9.0-10 | **Crítico** | Es probable que la pérdida de [confidencialidad | integridad | disponibilidad] tenga un efecto catastrófico y adverso en la organización o las personas relacionadas con ella. Y requiere ser mitigado de manera inmediata. |

Tabla 14. Rangos de valores de la escala de CVSS.

# Vector

El vector CVSS v3.1.1 es una representación de una cadena de texto de un conjunto de métricas del CVSS. Es comúnmente utilizada para registrar y mencionar la métrica del CVSS de una forma concisa.

Para la versión 3.1 el vector empieza con el texto “CVSS” y un valor numérico que representa la versión actual (“3.1”). Cada métrica en el vector consiste en el nombre abreviado de la métrica, seguida por “:”, y por su valor de métrica abreviado. El vector muestra estas métricas en un orden predeterminado, usando el “/” para separarlas. Si una métrica temporal no es usada, se le da un valor de “ND” (No definida).

Los vectores **Base**, **Temporales** y **Entorno** se muestran en la Tabla 15.

|  |  |  |
| --- | --- | --- |
| Métrica | Nombre | Posibles valores |
| Base | Vector de Ataque, AV Complejidad de Ataque, AC Privilegios Requeridos, PR Interacción del Usuario, UI Alcance, S Confidencialidad, C Integridad, I Disponibilidad, A | [N,A,L,P] [L,H] [N,L,H] [H,L] [U,C] [H,L,N] [H,L,N] [H,L,N] |
| Temporales | Nivel de maduración de la explotación, E Nivel de remediación, RL Reporte de Confianza, RC | [X,H,F,P,U] [X,U,W,T,O] [X,C,R,U] |
| De Entorno | Req. de Confidencialidad, CR Req. de Integridad, IR Req. de Disponibilidad, AR Mod. de Vector de Ataque, MAV Mod. de Complejidad de Ataque, MAC Mod. de Privilegios Requeridos, MPR Mod. de Interacción del Usuario, MUI Mod. de Alcance, MS Mod. de Confidencialidad, MC Mod. de Integridad, MI Mod. de Disponibilidad, MA | [X,H,M,L] [X,H,M,L] [X,H,M,L] [X,N,A,L,P] [X,L,H] [X,N,L,H] [X,H,L] [X,U,C] [X,H,L,N] [X,H,L,N] [X,H,L,N] |

Tabla 15. Vectores base, temporales y de entorno.

Por ejemplo, una vulnerabilidad con los valores de las métricas base de “Vector de Ataque: Red, Complejidad del Ataque: Bajo, Privilegios requeridos: Ninguno, Interacción del Usuario: Ninguno, Alcance: Cambio, Impacto a la Confidencialidad: Bajo, Impacto a la Integridad: Bajo, Impacto a la Disponibilidad: Bajo”, tiene el siguiente vector base:

“CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L”.

# Niveles de métricas

Cada valor de la métrica tiene uno constante asociado, el cual es usado en las fórmulas, definidos en la tabla 16.

|  |  |  |
| --- | --- | --- |
| Métrica | Valor de la Métrica | Valor numérico |
| Vector de ataque / Vector de ataque modificado | Red  Red Adyacente  Local Físico | 0.85  0.62  0.55  0.2 |
| Complejidad de ataque / Complejidad de ataque modificado | Bajo  Alto | 0.77  0.44 |
| Privilegios Requeridos / privilegios requeridos modificados | Ninguno  Bajo  Alto | 0.85  0.62 (0.68 si alcance/Alcance modificado es cambiado)  0.27 (0.50 si alcance/Alcance modificado es cambiado) |
| Interacción de usuario / Interacción de usuario modificado | Ninguno  Requerido | 0.85  0.62 |
| C,I,A Impacto / Modificado C,I,A Impacto | Alto  Bajo  Ninguno | 0.56  0.22  0 |
| Explotación de madurez de código no definida | Alto Funcional Prueba de Concepto Sin probar | 1  0.97  0.94  0.91 |
| Nivel de remediación | No definido  No disponible  Solucionado Corrección temporal  Corrección oficial | 1  1   0.97  0.96  0.95 |
| Reporte de confianza | No definido 1   Confirmado 1   Razonable  Desconocido | 1  1  0.96  0.92 |
| Requerimientos de confianza– C,I,A Requerimientos (CR) | No definido   Alto Medio Bajo | 1  1.5  1  0.5 |

Tabla 16. Niveles de Métricas.