SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

TOMÉ, 28 OCTUBRE 2025

VISTOS:

Considerando el Decreto Fuerza Ley N° 01/24.04.2006 del MINSAL; el D.F.L. N° 29/2004 sobre Estatuto Administrativo; la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos; la Resolución N° 6/2019 de Contraloría sobre exención de toma de razón en materias de personal; los Decretos Supremos de Salud N° 140/2005 y N° 38/2005 que aprueban los Reglamentos Orgánicos de los Servicios de Salud y de los Establecimientos de Salud de Menor Complejidad; la Resolución Exenta N° 2778/2023 del SSThno; la Resolución Exenta N° 1251/2023 que aprueba la Política General de Seguridad de la Información del Hospital de Tomé; el COMGES 2025; y el Ordinario N° 943/2025 del Subsecretario de Redes Asistenciales sobre implementación de controles críticos de seguridad de la información según ISO/IEC 27001:2022; que, conforme al D.S. N° 285/2022 y la Ley N° 21.663 de Ciberseguridad, el Hospital de Tomé se encuentra incluido en la lista preliminar de **Operadores de Importancia Vital (OIV)**; y que, mediante la Providencia N° DHT-6553 y el oficio N° 0106 clasificado como secreto, se instruye evacuar un Informe Técnico Fundado respecto del cumplimiento de los criterios del artículo 4° del D.S. N° 285/2022, se da curso a la presente comunicación.

CONSIDERANDO:

1. Que la adecuada gestión de vulnerabilidades en los activos de información es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información del Hospital de Tomé.
2. Que el Hospital de Tomé requiere establecer procedimientos claros para identificar, clasificar, analizar, tratar y verificar vulnerabilidades, asegurando la mitigación de riesgos de explotación y fortaleciendo la postura de seguridad de la organización.
3. Que la correcta aplicación de este procedimiento asegura el cumplimiento de normativas nacionales, estándares internacionales ISO/IEC 27001:2022 e ISO/IEC 27002:2013, y demás requerimientos legales relacionados con la seguridad de la información y ciberseguridad.
4. Que este procedimiento aplica a todos los activos de información propiedad de, o bajo la responsabilidad de, Hospital de Tomé, incluyendo infraestructura de red, sistemas operativos, aplicaciones, bases de datos, dispositivos móviles y otros activos tecnológicos.
5. Que la implementación de este procedimiento contribuye a formalizar roles y responsabilidades, coordinar análisis de vulnerabilidades, definir planes de remediación y mitigación, monitorear el estado de los activos y generar reportes periódicos a la alta dirección.

RESUELVE EXENTA N° 2121

1. **APRÚEBASE** el Procedimiento de Gestión de Vulnerabilidades del Hospital de Tomé, que establece lineamientos, responsabilidades, flujos de trabajo y mecanismos de control para la identificación, clasificación, análisis, tratamiento, verificación y seguimiento de vulnerabilidades en todos los activos de información de la organización, en concordancia con normas nacionales, estándares internacionales y buenas prácticas de seguridad de la información.

SERVICIO DE SALUD TALCAHUANO
SUBDIRECCIÓN ADMINISTRATIVA
ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
HOSPITAL DE TOMÉ

2. **DISPÓNGASE** que todos los colaboradores, personal a honorarios y proveedores externos que operen en el Hospital de Tomé cumplan estrictamente con los lineamientos establecidos en este procedimiento, incluyendo:

   a) Identificación y reporte de vulnerabilidades mediante escaneos automatizados, pruebas de penetración, auditorías y fuentes de inteligencia de amenazas.

   b) Clasificación y puntuación de vulnerabilidades usando CVSS y evaluación de riesgos asociados a activos críticos.

   c) Implementación de medidas de tratamiento, incluyendo remediación, mitigación, aceptación o transferencia de riesgos, según corresponda.

   d) Planificación, documentación y seguimiento de acciones de tratamiento de vulnerabilidades.

   e) Verificación de la efectividad de remediaciones mediante re-escaneos y pruebas complementarias.

   f) Monitoreo continuo de vulnerabilidades y amenazas emergentes.

   g) Generación de informes periódicos para la alta dirección y propietarios de activos.

   h) Cumplimiento con la Política General de Seguridad de la Información del Hospital de Tomé y normativas asociadas.

3. **ENCÁRGUESE** al Responsable de Ciberseguridad, Equipo de Operaciones de TI, Equipo de Desarrollo, Analistas de Seguridad y Propietarios de Activos la supervisión, aplicación, monitoreo y control del cumplimiento de este procedimiento, así como la gestión de incidentes, auditorías, remediaciones y medidas correctivas en caso de incumplimiento.
4. **DEJASE CONSTANCIA** que todo funcionario, colaborador o proveedor que interactúe con activos tecnológicos del Hospital de Tomé deberá conocer y adherir al presente procedimiento, asegurando la correcta gestión de vulnerabilidades y la protección de los activos de información.
5. **ESTABLÉCESE** que la presente resolución entra en vigor a partir de su publicación, y cualquier modificación futura deberá efectuarse mediante resolución exenta de la autoridad competente, asegurando la coherencia con las normativas legales y estándares internacionales aplicables.

"ANÓTESE Y COMUNÍQUESE"

LEC/CCU/ccu
N° INT. 06/28.10.2025
DISTRIBUCIÓN:

- Subdirección Administrativa H. Tomé
- Subdirección Médica H. Tomé
- Oficina de Partes Hospital de Tomé
- CR. Apoyo Diagnóstico
- Área Recurso Físicos
- Área Gestión y Desarrollo de las Personas
- CR. Atención Cerrada
- CR. Atención Abierta
- CR. Emergencia

Firmado por Aníbal Antonio Cea Henríquez
Fecha 28/10/2025 15:08:55 CLST

PUEDE VALIDAR ESTE DOCUMENTO CON EL SIGUIENTE CODIGO:309304-51730
EN LA SIGUIENTE URL: https://sstalcahuano.cl/validador_panel

PROC03-25-0003

PROCEDIMIENTO GESTIÓN DE VULNERABILIDADES

Sistema de Gestión de Seguridad de la Información – Hospital de Tomé

Versión Oficial Actual 1 – julio 2025

Contenido

1 PROPÓSITO

Este procedimiento define los pasos a seguir para identificar, clasificar, analizar, tratar y verificar las vulnerabilidades de seguridad en los activos de información del Hospital de Tomé, con el objetivo de minimizar el riesgo de explotación y garantizar la confidencialidad, integridad y disponibilidad de la información.

2 ALCANCE

Este procedimiento aplica a todos los activos de información propiedad de, o bajo la responsabilidad de, Hospital de Tomé, incluyendo:

- Infraestructura de red (servidores, routers, switches, firewalls, etc.).
- Sistemas operativos (servidores, estaciones de trabajo).
- Aplicaciones (internas, externas, web, móviles).
- Bases de datos.
- Dispositivos móviles corporativos.
- Otros activos de TI que procesen almacenen o transmitan información.

3 TERMINOLOGÍA

- **Amenaza:** Un evento o acción que tiene el potencial de comprometer la seguridad del sistema, como un ataque malicioso, un fallo del sistema o desastres naturales.
- **Análisis de Riesgos:** El proceso de evaluar los riesgos potenciales en un sistema, identificando vulnerabilidades y amenazas, y determinando la probabilidad e impacto de su explotación.
- **Análisis de Vulnerabilidades**: Identificación y evaluación de debilidades en sistemas y redes que podrían ser explotadas por amenazas. Tiene por objetivo el identificar y corregir vulnerabilidades antes de que sean aprovechadas.
  - Análisis de Código Dinámico: Evaluación del comportamiento de una aplicación mientras se está ejecutando. Se realiza mediante pruebas y monitoreo en tiempo real durante la ejecución de un programa, identificando posibles vulnerabilidades y problemas de seguridad que podrían surgir en situaciones de uso reales.
  - Análisis de Código Estático: Evaluación que se realiza sin ejecutar el programa. Consiste en examinar el código fuente de una aplicación para identificar posibles vulnerabilidades, errores de programación y prácticas inseguras.
- **Controles de Seguridad**: Medidas implementadas para proteger activos de información, como firewalls, cifrado, autenticación, y políticas de acceso.
- **Scanner de seguridad:** También conocido como scanner de vulnerabilidades, es un proceso automatizado mediante el cual se examinan sistemas informáticos, redes, aplicaciones o dispositivos en busca de posibles debilidades y vulnerabilidades que podrían ser explotadas por amenazas maliciosas. Se lleva a cabo utilizando herramientas especializadas y/o pruebas manuales que buscan activamente vulnerabilidades conocidas, configuraciones incorrectas o debilidades en la seguridad.
- **Incidente de Seguridad:** Un evento que indica una posible violación de la seguridad de la información, como un acceso no autorizado, pérdida de datos, o interrupción del servicio.
- **Informe de Análisis de Vulnerabilidades**: Presenta los resultados del análisis de vulnerabilidades llevado a cabo en un sistema, red, aplicación o entorno específico. El objetivo principal de este análisis es identificar posibles debilidades y riesgos de seguridad que puedan comprometer la integridad, confidencialidad o disponibilidad de la información. La implementación de las recomendaciones propuestas en este informe

contribuirá significativamente a reducir los riesgos y fortalecer la postura de seguridad de la organización.

- **Pen-Testing**: Una evaluación activa de la seguridad de un sistema mediante la simulación de ataques para identificar vulnerabilidades y evaluar la efectividad de las medidas de seguridad existentes.
- **Política de Seguridad:** Un conjunto de reglas y directrices que definen cómo deben manejarse y protegerse los activos de información en un sistema o sitio web.
- **Riesgo de Seguridad:** La probabilidad de que una amenaza explote una vulnerabilidad y cause un impacto no deseado en el sistema.
- **Vulnerabilidad**: Una debilidad en el sistema o en un componente que podría ser explotada para comprometer la seguridad del sistema.
- **CVE (Common Vulnerabilities and Exposures):** Diccionario público de nombres para vulnerabilidades de seguridad conocidas.
- **CVSS (Common Vulnerability Scoring System):** Estándar de la industria para asignar una puntuación de gravedad a las vulnerabilidades.
- **Tratamiento de la Vulnerabilidad:** Acción tomada para mitigar el riesgo asociado a una vulnerabilidad (remediación, mitigación, aceptación, transferencia).
- **Remediación:** Acción para corregir la vulnerabilidad (aplicación de parches, actualización de software, reconfiguración).

4 DOCUMENTOS APLICABLES

Dentro de la normativa, marcos de trabajo y documentos relacionados, y que son aplicables al presente procedimiento, se asocian los siguientes:

- ISO/IEC 27001:2022 - Sistemas de gestión de la seguridad de la información: Este procedimiento se basa en los siguientes controles específicos de la norma ISO/IEC 27001:2022, que proporcionan un marco para la gestión de riesgos de seguridad de la información, incluyendo la gestión de vulnerabilidades:
    - A.5.15 Información de inteligencia sobre amenazas: Establece la necesidad de recopilar y analizar información sobre amenazas de seguridad de la información para comprender las amenazas actuales y emergentes y el panorama de amenazas.
    - A.5.16 Gestión de vulnerabilidades: Requiere el desarrollo e implementación de un proceso para gestionar las vulnerabilidades de seguridad de la información. Esto incluye la identificación, evaluación y tratamiento de las vulnerabilidades.
    - A.5.17 Planificación de la continuidad de negocio: (En relación con la mitigación de impactos de vulnerabilidades explotadas).
    - A.5.18 Planes de recuperación de desastres: (En relación con la recuperación de sistemas afectados por la explotación de vulnerabilidades).
    - A.6.1 Gestión de activos: (Para identificar y valorar los activos susceptibles a vulnerabilidades).
    - A.8.8 Gestión de vulnerabilidades técnicas: Se centra específicamente en la gestión de vulnerabilidades en sistemas de información y software.
    - A.8.9 Pruebas de seguridad: Incluye la realización de pruebas de penetración y otras evaluaciones de seguridad para identificar vulnerabilidades.
    - A.8.12 Protección contra software malicioso: (Como una medida para prevenir la explotación de ciertas vulnerabilidades).
    - A.8.16 Monitorización de seguridad: (Para detectar actividades sospechosas que podrían indicar la explotación de vulnerabilidades).

5 ROLES Y RESPONSABILIDADES

- **Responsable de Ciberseguridad**: responsable general de la gestión de vulnerabilidades, incluyendo la definición de políticas, la supervisión del proceso y la comunicación con la alta dirección.
- **Equipo de Operaciones de TI**: responsable de la implementación de parches y otras medidas de remediación en la infraestructura de TI.
- **Equipo de Desarrollo**: responsable de la corrección de vulnerabilidades en las aplicaciones.
- **Analistas de Seguridad**: responsables de la identificación, clasificación, análisis y seguimiento de las vulnerabilidades.
- **Propietarios de Activos**: responsables de comprender los riesgos asociados a las vulnerabilidades en sus activos y de aprobar las decisiones de tratamiento.

6 PROCEDIMIENTO

6.1 Identificación de Vulnerabilidades:

- **Escaneo de Vulnerabilidades:** Realizar escaneos de vulnerabilidades periódicos (programados y ad-hoc) utilizando herramientas automatizadas en la infraestructura de red, sistemas operativos y aplicaciones. La frecuencia de los escaneos debe basarse en el riesgo del activo.
- Pudiendo solicitar escaneo al Minsal a través de un correo a mds@minsal.cl, con copia a la casilla seguridadtic@minsal.cl, adjuntando el "Formulario de solicitud de scanner de seguridad" o solicitar scan a la ANCI a la casilla ayuda@anci.gob.cl a través de formulario exigido por esta organización.
- **Pruebas de Penetración (Pentesting):** Realizar pruebas de penetración periódicas por personal interno o externo para identificar vulnerabilidades que los escaneos automatizados podrían no detectar.
- **Auditorías de Seguridad:** Incorporar la revisión de vulnerabilidades como parte de las auditorías de seguridad internas y externas.
- **Gestión de Parches:** Monitorear y analizar los boletines de seguridad de los proveedores de software y hardware para identificar vulnerabilidades y la disponibilidad de parches.
- **Inteligencia de Amenazas:** Utilizar fuentes de inteligencia de amenazas para identificar vulnerabilidades emergentes y activamente explotadas.
- **Reportes Internos:** Fomentar la notificación interna de posibles vulnerabilidades por parte del personal, esto incluye incidentes internos que puedan ser evaluador por el Grupo de Seguridad de la Información.

6.2 Clasificación y Puntuación de Vulnerabilidades:

- **Análisis Inicial:** El analista de seguridad revisará los resultados de las herramientas de escaneo, pruebas de penetración y otras fuentes para identificar las vulnerabilidades.
- **Puntuación CVSS:** Asignar una puntuación de gravedad a cada vulnerabilidad utilizando el sistema CVSS (Common Vulnerability Scoring System).
- **Clasificación del Riesgo:** Evaluar el riesgo asociado a cada vulnerabilidad considerando:
  - **Gravedad de la Vulnerabilidad (CVSS):** Puntuación base de la vulnerabilidad.
  - **Explotabilidad:** Facilidad con la que la vulnerabilidad puede ser explotada.
  - **Impacto:** Consecuencias potenciales de la explotación (confidencialidad, integridad, disponibilidad).
  - **Valor del Activo:** Importancia del activo afectado para la organización.
  - **Controles de Seguridad Existentes:** Controles implementados que podrían mitigar el riesgo.
  - **Exposición:** Si el activo es accesible desde redes externas.

- **Niveles de Riesgo:** Clasificar las vulnerabilidades en niveles de riesgo (ej. Crítico, Alto, Medio, Bajo) basándose en la evaluación del riesgo. Definir los criterios específicos para cada nivel.

6.3 Análisis de Vulnerabilidades:

- **Análisis Técnico Detallado:** Investigar la naturaleza de la vulnerabilidad, su posible impacto y las posibles formas de explotación.
- **Validación:** Verificar la existencia de la vulnerabilidad en el entorno del Hospital de Tomé.
- **Identificación de Activos Afectados:** Determinar todos los activos que son susceptibles a la vulnerabilidad.
- **Priorización:** Priorizar el tratamiento de las vulnerabilidades basándose en su nivel de riesgo y la criticidad de los activos afectados.

6.4 Tratamiento de Vulnerabilidades:

- **Selección del Tratamiento:** Para cada vulnerabilidad priorizada, seleccionar la acción de tratamiento apropiada:
  - **Remediación:** Aplicar parches, actualizar software, reconfigurar sistemas.
  - **Mitigación:** Implementar controles compensatorios (ej. reglas de firewall, segmentación de red, controles de acceso adicionales).
  - **Aceptación:** Documentar la decisión de aceptar el riesgo (solo para vulnerabilidades de bajo riesgo o cuando la remediación/mitigación no es factible a corto plazo). Requiere la aprobación del Propietario del Activo y del Responsable de Ciberseguridad.
  - **Transferencia:** Considerar la transferencia del riesgo (ej. seguro cibernético) como parte de una estrategia general de gestión de riesgos.
- **Planificación de la Implementación:** Desarrollar un plan de implementación para las acciones de tratamiento, incluyendo responsables, plazos y recursos necesarios.
- **Implementación:** Ejecutar las acciones de tratamiento según el plan.
- **Documentación:** Documentar todas las decisiones de tratamiento y las acciones implementadas.

6.5 Verificación de la Remediación:

- **Re-escaneo:** Realizar un nuevo escaneo de vulnerabilidades después de la implementación de la remediación para verificar que la vulnerabilidad ha sido corregida.
- **Pruebas:** Realizar pruebas manuales o automatizadas para confirmar la efectividad de la remediación o mitigación.
- **Validación:** El analista de seguridad validará que la vulnerabilidad ha sido tratada correctamente.

6.6 Seguimiento y Monitoreo:

- **Seguimiento de Vulnerabilidades Pendientes:** Mantener un registro actualizado de todas las vulnerabilidades identificadas y su estado de tratamiento.
- **Monitoreo de Nuevas Vulnerabilidades:** Mantenerse al tanto de las nuevas vulnerabilidades y amenazas a través de fuentes de inteligencia y alertas de seguridad.
- **Revisiones Periódicas:** Revisar periódicamente el proceso de gestión de vulnerabilidades para identificar áreas de mejora.
- **Informes:** Generar informes periódicos sobre el estado de las vulnerabilidades a la alta dirección y a los propietarios de los activos.

7 REGISTROS

- Formulario de solicitud de scanner de seguridad
- Informe de Análisis de Vulnerabilidades

8 DIFUSION

La comunicación del presente documento se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Portal Mesa de Servicio TI, Sección Ayuda, Seguridad
- Correo Informativo.

9 REVISION

El presente procedimiento deberá ser revisado cada dos años o cuando ocurran cambios significativos para garantizar que:

- Sigue siendo adecuado para su propósito y preciso.
- Refleja los cambios en las tecnologías.
- Está alineado con la legislación vigente, los estándares internacionales y las mejores prácticas.

10 EXCEPCIONES AL CUMPLIMIENTO

En situaciones excepcionales, el Jefe de Departamento TIC, el CISO o el Comité de Seguridad de la Información tendrán la facultad de evaluar y establecer condiciones específicas para la excepción al cumplimiento de las directrices establecidas en esta política, siempre que tales excepciones no infrinjan la legislación vigente ni comprometan la seguridad de la información.

Cada excepción deberá ser debidamente documentada, y se deberá iniciar un proceso de revisión de la política en el que se determinará si es necesario incorporar directrices adicionales o realizar modificaciones específicas.

11 CONTROL DE VERSIONES

Versión	Fecha	Creado por	Pág. o Sección modificada	Descripción de la modificación

12 ANEXO A: MATRICES

Explotabilidad

NIVEL	DESCRIPCIÓN	EJEMPLOS
Alta (3)	Puede explotarse con facilidad, sin requerir conocimientos avanzados o herramientas especializadas	Malware genérico, phishing básico, puertos abiertos sin autenticación.
Media (2)	Requiere algunos conocimientos técnicos, herramientas específicas o acceso intermedio	Ataques que requieren scripts especializados, manipulación de configuración
Baja (1)	Requiere conocimientos avanzados, acceso físico o condiciones muy específicas.	Ataques de ingeniería inversa, explotación de hardware, necesidad de insider.

Impacto

NIVEL	DESCRIPCIÓN	EJEMPLOS
Alto (3)	Compromete confidencialidad, integridad y disponibilidad de datos críticos o servicios esenciales.	Robo de datos de pacientes, indisponibilidad de sistemas clínicos, ransomware.
Medio (2)	Impacta parcialmente la operación o datos no críticos.	Interrupción temporal de un sistema administrativo, pérdida de datos no sensibles.
Bajo (1)	Impacto menor y fácilmente recuperable.	Fallo en una estación de trabajo aislada, pérdida de datos temporales no críticos.

Controles de Seguridad Existentes (Mitigación)

NIVEL	DESCRIPCIÓN	EJEMPLOS
Bajos (3)	No existen controles relevantes o son fácilmente eludibles.	Sin antivirus, sin parches, sin firewall efectivo.
Medios (2)	Controles presentes, pero no cubren todas las posibilidades	Antivirus básico, políticas parciales, segmentación de red incompleta.
Altos (1)	Controles robustos y actualizados, difícil de evadir.	EDR avanzado, segmentación estricta, bloqueo de redes no autorizadas.

Exposición (Accesibilidad del activo)

NIVEL	DESCRIPCIÓN	EJEMPLOS
Alta (3)	Accesible desde Internet o redes públicas sin restricción.	Servidor web público, equipo con IP pública.
Media (2)	Accesible solo desde la red interna, pero sin segmentación.	Servidor interno sin firewall interno, estaciones conectadas a VLAN general.
Baja (1)	Accesible solo desde segmentos restringidos o aislados.	Servidor en VLAN aislada, equipo sin conexión externa.

Mapeo de Riesgo

PUNTAJE	NIVEL RIESGO	DESCRIPCIÓN	ACCIÓN
9-12	Crítico	La vulnerabilidad representa un riesgo inaceptable y puede comprometer gravemente datos y servicios esenciales del hospital.	Corrección inmediata: abrir gestión de problemas prioritaria, aplicar mitigaciones urgentes y, si es necesario, retirar el activo de producción hasta remediación. Escalar a Comité de Seguridad.
7-8	Alto	Puede ser explotada con relativa facilidad y producir un impacto alto sobre datos o servicios críticos.	Gestionar de forma prioritaria: iniciar gestión de problemas, asignar responsable y plazo corto (ej. ≤ 15 días hábiles). Monitorear hasta cierre.
4-6	Medio	Requiere más esfuerzo para explotar o el impacto sería moderado.	Planificación controlada: registrar en backlog de seguridad, programar corrección en ciclo de mantenimiento o proyecto. Revisar controles preventivos.
1-3	Bajo	Baja probabilidad de explotación y/o impacto menor.	Monitorear y documentar: mantener bajo observación. Corregir solo si se realizan cambios mayores o se detecta aumento de exposición.

13 Anexo B – Metodología de Cálculo CVSS 3.1 – Base Score

Objetivo:

Este anexo describe el método para determinar la puntuación base (Base Score) de una vulnerabilidad de acuerdo con el estándar Common Vulnerability Scoring System (CVSS) v3.1, y define cómo interpretar cada métrica para su uso en la gestión de vulnerabilidades del Hospital.

Descripción General

El CVSS 3.1 es un sistema estándar internacional que permite cuantificar la severidad de una vulnerabilidad de manera objetiva, entregando un puntaje que oscila entre 0.0 (nula) y 10.0 (crítica).

La Puntuación Base (Base Score) se calcula considerando características intrínsecas de la vulnerabilidad que no cambian con el tiempo ni dependen del entorno específico.

Para facilitar el cálculo y estandarizar criterios, se utilizará la calculadora oficial disponible en: https://www.cvss.pentest.cl

Métricas de la Puntuación Base

Cada vulnerabilidad debe evaluarse en función de las siguientes métricas:

Vector de Ataque (Attack Vector – AV)

Indica la distancia y accesibilidad necesaria para explotar la vulnerabilidad.

- Red (Network – N): Explotable de forma remota a través de red o Internet.
- Adyacente (Adjacent – A): Requiere estar en la misma red o segmento local.
- Local (Local – L): Requiere acceso físico o lógico al sistema.
- Físico (Physical – P): Requiere interacción física directa con el dispositivo.

Complejidad del Ataque (Attack Complexity – AC)

Describe las condiciones fuera del control del atacante que deben cumplirse.

- Bajo (Low – L): No requiere condiciones especiales.
- Alto (High – H): Requiere condiciones poco comunes o difíciles de cumplir.

Privilegios Requeridos (Privileges Required – PR)

Nivel de permisos que el atacante debe tener antes de explotar la vulnerabilidad.

- Ninguno (None – N): No requiere autenticación previa.
- Bajo (Low – L): Requiere permisos limitados de usuario.
- Alto (High – H): Requiere privilegios elevados (administrador/root).

Interacción del Usuario (User Interaction – UI)

Si la explotación requiere la acción de una persona legítima.

- Ninguna (None – N): No requiere participación del usuario.
- Requerida (Required – R): Necesita que un usuario ejecute una acción (ej.: abrir archivo, hacer clic).

Alcance (Scope – S)

Si la vulnerabilidad afecta sólo el componente vulnerable o puede impactar otros.

- Directo (Unchanged – U): El impacto se limita al mismo sistema.
- Indirecto (Changed – C): Puede afectar otros sistemas o componentes distintos.

Impacto en la Confidencialidad (Confidentiality – C)
Grado en que se ven comprometidos datos e información.

- Ninguno (None – N): Sin impacto.
- Bajo (Low – L): Acceso parcial o limitado.
- Alto (High – H): Pérdida total o exposición completa.

Impacto en la Integridad (Integrity – I)
Grado en que pueden alterarse datos o procesos.

- Ninguno (None – N)
- Bajo (Low – L)
- Alto (High – H)

Impacto en la Disponibilidad (Availability – A)
Grado en que se interrumpe el servicio o recurso.

- Ninguno (None – N)
- Bajo (Low – L)
- Alto (High – H)

Escala de Severidad
De acuerdo con el puntaje calculado, la clasificación es:

- 0.0: Ninguna
- 0.1 – 3.9: Baja
- 4.0 – 6.9: Media
- 7.0 – 8.9: Alta
- 9.0 – 10.0: Crítica

Procedimiento de Uso
- Identificar la vulnerabilidad y recopilar la información técnica.
- Evaluar cada métrica según las definiciones de la sección Métricas Puntuación Base.
- Ingresar los valores en la calculadora oficial: https://www.cvss.pentest.cl
- Registrar el puntaje obtenido y su vector CVSS (ejemplo: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
- Clasificar la severidad según la sección Escala de Severidad.
- Incorporar el resultado al registro de vulnerabilidades (Ticket de Incidencia) y al plan de remediación.

Observaciones
Este anexo aplica exclusivamente para la determinación de la Puntuación Base del CVSS 3.1. No incluye métricas temporales ni contextuales, las cuales pueden ser consideradas en etapas posteriores para priorización de tratamiento.

El cálculo debe realizarse siempre con la calculadora oficial para asegurar consistencia y trazabilidad.