Análisis forense y profesionalización en ciberseguridad

Breve descripción:

La profesionalización en la ciberseguridad, es clave para garantizar que los especialistas cuenten con la formación, certificaciones y competencias técnicas y éticas necesarias para desarrollar su labor con efectividad y rigor. Además, la gestión de riesgos y la actualización constante son elementos críticos para enfrentar las amenazas en un entorno digital en constante evolución. Esta combinación fortalece la seguridad organizacional y promueve la confianza en los usuarios finales.

Agosto de 2025

Tabla de contenido

Introducción

Este componente aborda de manera integral, el análisis forense digital y la profesionalización en ciberseguridad, explicando el proceso metodológico para la identificación, recolección, preservación, análisis y presentación de evidencia digital, garantizando su integridad y validez en procesos legales. Además, se presenta la evolución histórica y el contexto actual del campo de la ciberseguridad, destacando el crecimiento exponencial de la demanda de profesionales y la diversificación de perfiles, desde técnicos especializados hasta roles estratégicos de liderazgo.

Para comprender la importancia del contenido y los temas abordados, se recomienda acceder al siguiente video:

Video 1. Análisis forense y profesionalización en ciberseguridad

Enlace de reproducción del video

Video 1. Síntesis del video: Análisis forense y profesionalización en ciberseguridad
En este componente se aborda el análisis forense digital como una disciplina clave dentro de la ciberseguridad, enfocándose en la investigación y recuperación de evidencia digital tras incidentes y ataques cibernéticos. Se explica el proceso metodológico para la identificación, preservación, análisis y presentación de pruebas digitales, fundamentales para esclarecer hechos y apoyar procesos legales. Además, se examina la creciente profesionalización de la ciberseguridad, destacando la importancia de contar con expertos capacitados y acreditados, así como con certificaciones reconocidas internacionalmente que garanticen el rigor y la ética en la investigación forense y la defensa cibernética. También se analizan las habilidades técnicas, legales y éticas que forman parte del perfil profesional del analista forense, y cómo esta especialización contribuye a fortalecer la seguridad organizacional y la confianza en los entornos digitales. Finalmente, se presenta la relevancia de la colaboración interdisciplinaria y la actualización continua en un campo que evoluciona rápidamente, haciendo un llamado a la profesionalización como un pilar indispensable para proteger activos digitales y responder con eficacia ante incidentes. Este componente invita a comprender el análisis forense y la profesionalización en ciberseguridad como piezas esenciales para un entorno digital seguro y confiable, donde la calidad del talento humano es tan importante como la tecnología empleada.

1. Análisis de evidencia digital

Para dar contexto a lo que se refiere el análisis de evidencia digital, se invita a que analice los siguientes dos casos que se presentan por medio de estos videos:

Caso # 1

Video 2. Análisis forense y profesionalización de la ciberseguridad Caso No.1

Enlace de reproducción del video

Video 2. Síntesis del video: Análisis forense y profesionalización de la ciberseguridad Caso No.1
Imagina que un detective recibe un celular sospechoso durante una investigación. Lo primero que hace es asegurarse de que nadie use el dispositivo para

no alterar la información. Con mucho cuidado, lo lleva al laboratorio, donde crea una copia exacta de todos los datos, sin tocar el original.

Luego, usando herramientas avanzadas, explora mensajes, fotos, llamadas y aplicaciones buscando pistas importantes. También revisa si alguien intentó borrar información o si hubo accesos inusuales.

Cada hallazgo se documenta detalladamente en un informe claro y ordenado, que luego puede usarse como prueba ante un juez. Así, el análisis de evidencia digital combina tecnología y método para descubrir lo que realmente ocurrió.

Caso # 2

Video 3. Análisis forense y profesionalización de la ciberseguridad Caso No.2

Enlace de reproducción del video

Video 3. Síntesis del video: Análisis forense y profesionalización de la ciberseguridad Caso No.2
Imagina que la policía investiga un robo y encuentra una computadora en la escena. El análisis de evidencia digital comienza cuando un experto apaga y transporta cuidadosamente el computador al laboratorio, asegurándose de no alterar los datos. Allí, el especialista crea una copia “espejo” del disco, para no modificar la información original. Luego, usando programas especiales, busca archivos eliminados, correos, fotos y registros de actividad. Analiza si hay conexiones a dispositivos externos, accesos a cuentas sospechosas o rastros de programas maliciosos. Finalmente, el experto organiza la información hallada en un informe claro y fácil de entender, que servirá como prueba confiable ante la justicia. Así, paso a paso, el análisis de evidencia digital ayuda a descubrir la verdad sobre el delito.

1.1 Conceptos fundamentales del análisis forense digital

El análisis forense digital es una disciplina encargada de identificar, recolectar, preservar, analizar y presentar evidencia digital de manera que garantice su integridad y utilidad en procesos legales o investigaciones de seguridad. Implica el uso de técnicas especializadas para evitar la alteración de los datos y su correcto procesamiento, con el objetivo de reconstruir hechos, descubrir actividades sospechosas y aportar información válida ante las autoridades.

A continuación, se relacionan los conceptos fundamentales del análisis forense digital:

Tabla 1. Conceptos del análisis forense digital

Concepto	Descripción breve
Identificación.	Localiza posibles fuentes de evidencia digital, como discos duros, correos o dispositivos móviles.
Recolección.	Obtiene la evidencia resguardando su integridad, siguiendo procedimientos que eviten la alteración de datos.
Preservación.	Garantiza que los datos recolectados permanezcan intactos y auténticos durante todo el proceso.
Análisis.	Examina de manera detallada la evidencia, usando herramientas forenses para descubrir, recuperar y correlacionar información relevante.
Documentación.	Registra de manera cronológica y precisa todos los pasos realizados, generando informes claros y verificables.
Presentación.	Exhibe los hallazgos de forma comprensible y útil en juicios o auditorías, respetando normas legales.

Concepto	Descripción breve
Cadena de custodia.	Registra de manera formal que se asegure y documente cada transferencia o manipulación de la evidencia para mantener su validez.

A continuación, se relacionan algunos ejemplos:

- **Identificación**
  - ✓ Encontrar un disco duro externo conectado a una computadora involucrada en un delito.
  - ✓ Localizar correos electrónicos sospechosos en la bandeja de entrada de un usuario.
  - ✓ Detectar tráfico de red anormal en un servidor empresarial.
- **Recolección**
  - ✓ Clonar el contenido de un smartphone, usando herramientas forenses.
  - ✓ Extraer archivos de un servidor utilizando técnicas que evitan modificar los datos originales.
  - ✓ Recolectar registros de acceso de una base de datos.
- **Preservación**
  - ✓ Guardar una copia de los datos recolectados en un dispositivo de solo lectura.

- ✓ Sellar y almacenar un disco duro en una bolsa antiestática.
- ✓ Mantener los precintos de seguridad y etiquetas intactas durante el traslado de la evidencia.

- **Análisis**

  - ✓ Buscar archivos eliminados en un disco con software especializado.
  - ✓ Analizar los metadatos de fotos para determinar fechas y ubicaciones.
  - ✓ Examinar logs de actividad para identificar accesos no autorizados.

- **Documentación**

  - ✓ Anotar cada paso realizado durante el análisis en un cuaderno o sistema digital.
  - ✓ Tomar capturas de pantalla de hallazgos relevantes.
  - ✓ Escribir un informe que describa procedimientos, herramientas utilizadas y resultados.

- **Presentación**

  - ✓ Exponer los hallazgos en un juicio utilizando gráficos o resúmenes visuales.
  - ✓ Explicar en lenguaje sencillo los resultados y la importancia de la evidencia encontrada.
  - ✓ Responder preguntas de abogados o jueces sobre la validez de las pruebas.

- **Cadena de custodia**

  - ✓ Firmar un registro cada vez que alguien recibe o entrega la evidencia.

- ✓ Archivar un documento que detalle fechas, horas y nombres de quienes manipularon la evidencia.
- ✓ Utilizar sellos de seguridad numerados para verificar que no ha habido alteraciones.

1.2 Proceso forense en ciberseguridad organizacional

El proceso forense en ciberseguridad organizacional, es un conjunto de procedimientos estructurados para identificar, contener, analizar y remediar incidentes de seguridad, asegurando la validez y la integridad de la evidencia digital.

Al respecto, se destacan los siguientes:

1. **Procedimientos 1**

- **Detección del incidente**: todo comienza cuando un sistema de monitoreo alerta sobre una actividad anormal, como múltiples intentos de acceso fallidos o transferencia de grandes volúmenes de datos.
- **Activar el protocolo forense**: el equipo de respuesta a incidentes (CSIRT o DFIR) inicia el protocolo forense, delimitando responsabilidades y asegurando que cada paso quede documentado desde el principio.
- **Preservación de escena**: los sistemas afectados se aíslan para evitar que la amenaza se propague o que la evidencia sea manipulada.
- **Notificación interna**: se comunican los hechos relevantes a los responsables de seguridad, TI, legales y, si corresponde, a la alta dirección.
- **Identificación de evidencia**: se localizan los dispositivos críticos: servidores, estaciones, correos, logs, dispositivos móviles, backups y registros en la nube.

2. **Procedimientos 2**

- **Recolección de evidencia**: se efectúan copias forenses bit a bit de discos duros, memoria RAM, registros de red y cualquier dato potencialmente útil, asegurando la cadena de custodia.
- **Etiquetado y documentación**: cada evidencia se archiva y etiqueta meticulosamente, detallando fecha, hora, responsable y condiciones de recolección.
- **Verificación de integridad**: se usan hash criptográficos (MD5, SHA-1, SHA-256) para garantizar que la evidencia no sea alterada durante el análisis.
- **Análisis preliminar**: se visualizan logs iniciales buscando actividad sospechosa (inicios de sesión, conexiones externas, eliminación de archivos).
- **Hipótesis de ataque**: el equipo desarrolla hipótesis sobre cómo ocurrió el incidente: vía externa, interna, malware, ingeniería social, etc.

3. **Procedimientos 3**

- **Análisis profundo**: herramientas forenses especializadas que permiten recuperar archivos borrados, analizar vectores de ataque y rastrear movimientos laterales dentro de la red.
- **Correlación de eventos**: se unen evidencias de distintos sistemas para reconstruir la cronología del ataque o fuga de datos.
- **Identificación de responsables**: en la medida de lo posible, se atribuye la acción a usuarios internos, externos o cuentas comprometidas.

- **Medidas contemporáneas**: se recomiendan y, si es posible, implementan controles para detener el ataque y evitar su repetición inmediata.
- **Remediación**: se limpia el entorno, reestableciendo sistemas, restaurando backups seguros e instalando parches.

4. **Procedimientos 4**

- **Recuperación**: los sistemas vuelven a la normalidad bajo monitorización continua.
- **Evaluación de daños**: se analiza el alcance del incidente: impacto financiero, operativo, de reputación y legal.
- **Reporte forense**: se elabora un informe detallado, claro y entendible, que incluya cronología, técnicas usadas, descubrimientos, evidencia documental y conclusiones.
- **Validación legal**: si procede, se consulta con asesores legales para asegurar que la evidencia pueda usarse en juicios.
- **Presentación de evidencia**: la información se expone ante directivos, auditores, reguladores o autoridades judiciales si es necesario.

5. **Procedimientos 5**

- **Retroalimentación y mejora**: el equipo revisa y documenta lecciones aprendidas, actualiza políticas y procedimientos.
- **Capacitación y concienciación**: se refuerzan entrenamientos internos sobre ciberseguridad y respuesta a incidentes.
- **Simulacros forenses**: se programan ejercicios regulares para mantener la eficacia del proceso.

- **Actualización de herramientas**: se evalúan y actualizan constantemente las soluciones de monitoreo y análisis.
- **Integración con gestión de riesgos**: los hallazgos se usan para ajustar el mapa de riesgos de la organización.

6. **Procedimientos 6**

- **Seguimiento**: se monitorean posibles repercusiones, como intentos de represalia o campañas de desinformación.
- **Cumplimiento normativo**: se revisa y garantiza el cumplimiento de normativas como GDPR, LFPDPPP o PCI DSS.
- **Reportes externos**: si el incidente es mayor, se informa a autoridades regulatorias o sectoriales según obliga la ley.
- **Soporte a investigaciones externas**: se colabora con entes externos si el incidente involucra cibercrimen organizado.
- **Cierre formal**: una vez finalizados todos los pasos, se documenta el cierre y el aprendizaje obtenido, asegurando la trazabilidad del proceso.

Ahora bien, imagine una empresa en pleno funcionamiento cuando, de repente, suena una alarma: el equipo de monitoreo detecta movimientos sospechosos en uno de sus servidores críticos. Inicia entonces la siguiente historia de detectives digitales:

- El primer héroe en actuar es el especialista del equipo forense, que activa el protocolo de emergencia. Rápidamente aísla los sistemas afectados para que el atacante no siga avanzando ni borre sus huellas.

- Corren mensajes por la empresa: el área de ciberseguridad alerta a TI, legal y a la dirección. Todos saben que, a partir de ese momento, cada acción cuenta y debe ser documentada.
- El equipo localiza las posibles fuentes de evidencia: servidores, correos, respaldos y hasta registros en la nube. Todo se recolecta siguiendo estrictas normas, haciendo copias exactas de los dispositivos y calculando “huellas digitales” (hashes) para demostrar que nada se ha alterado.
- La sala se llena de pantallas mostrando registros y gráficos. Los analistas comienzan a revisar los logs, buscan patrones inusuales, conexiones extrañas y archivos borrados recientemente. Surge la hipótesis: el atacante usó credenciales internas y pasó de un sistema a otro buscando información sensible.
- Al descubrir cómo entró y qué información tocó, el equipo elabora un mapa de lo ocurrido y prepara recomendaciones inmediatas: cerrar accesos vulnerados, restaurar sistemas de un respaldo seguro y reforzar la protección.
- Mientras tanto, todo queda perfectamente documentado en informes: desde el primer aviso hasta la última acción de remediación. Cada pieza de evidencia tiene su etiqueta, cada copia su respaldo. Si la gravedad lo exige o la ley lo indica, el reporte se comparte con directivos o autoridades legales.
- Finalmente, una junta reúne al equipo. Se repasan errores, aciertos y se actualizan los procedimientos para estar mejor preparados la próxima vez.

Así, este ciclo de investigación deja enseñanzas y fortalece la cultura de seguridad digital en la organización.

De esta forma, el proceso forense, contado como una historia, se convierte en el escudo invisible que protege a la empresa contra amenazas y le da la capacidad de aprender, adaptarse y seguir adelante.

1.3 Normativa aplicable en el análisis de evidencia digital

El análisis de evidencia digital se rige por diversas normativas internacionales y nacionales, así como por estándares técnicos, ampliamente reconocidos en el ámbito forense. Estos marcos normativos buscan garantizar la validez, integridad y admisibilidad de la evidencia en procesos legales o administrativos. Los principales son:

- **Normas ISO/IEC**
  - ✓ **ISO/IEC 27037:2012**: establece directrices para la identificación, recolección, adquisición y preservación de evidencia digital, asegurando un tratamiento adecuado desde el inicio del proceso.
  - ✓ **ISO/IEC 27042:2015**: proporciona lineamientos específicos para el análisis e interpretación de evidencia digital, asegurando que los resultados sean trazables y reproducibles.
  - ✓ **ISO/IEC 27043:2015**: detalla los principios y procesos para la investigación de incidentes de seguridad de la información, incluyendo el análisis forense.
  - ✓ **ISO/IEC 27041:2015**: establece directrices sobre la garantía de idoneidad y eficacia de los métodos y herramientas utilizadas en investigaciones digitales.

- **Regulaciones y estándares tecnológicos:**
  - ✓ **RFC 3227**: recoge directrices para la recopilación de evidencia digital, especialmente sobre el orden de adquisición y la integridad de los datos.
  - ✓ **Protocolos institucionales**: muchas organizaciones y entidades gubernamentales desarrollan protocolos internos basados en estas normas internacionales, adaptados a su contexto legal y operativo.
- **Marco legal nacional (ejemplo Colombia y países hispanoamericanos):**
  - ✓ **Leyes de Comercio Electrónico, Ley de Protección de Datos, Código Procesal Penal y disposiciones sobre delitos informáticos**: contemplan reglas para la obtención y valoración de evidencia digital en procesos judiciales.
  - ✓ **Cadena de custodia**: registros formales y procedimientos para documentar, transportar y manipular la evidencia digital conforme a la ley y a estándares reconocidos.

2. Gestión de riesgos de seguridad de la información

La gestión de riesgos de seguridad de la información, es una disciplina esencial que toda persona y empresa debe comprender para proteger adecuadamente sus activos más valiosos. El riesgo, en este contexto, se define como la posibilidad de que una amenaza explote una vulnerabilidad, ocasionando un impacto negativo sobre los recursos informáticos, ya sean datos, servicios o infraestructura. Una correcta gestión, lleva los siguientes pasos:

1. **Identificación**

   Comienza con la identificación de los activos críticos: información confidencial, sistemas financieros, bases de datos de clientes o dispositivos de red.

2. **Reconocimiento y análisis**

   Posteriormente, se reconocen y analizan las amenazas que podrían afectar estos activos, como malware, ataques de phishing, errores humanos, desastres naturales o acciones internas malintencionadas.

3. **Evaluación**

   Finalmente, se realiza una evaluación sistemática de vulnerabilidades; esto abarca desde brechas en el software, hasta malas configuraciones e insuficiente capacitación del personal.

El análisis de riesgos, implica cruzar amenazas y vulnerabilidades, para estimar la probabilidad de ocurrencia y el posible impacto asociado, lo que permite priorizar los riesgos más significativos. Una vez priorizados, se diseña un plan de tratamiento, que

puede incluir la implementación de controles técnicos (cortafuegos, cifrado, autenticación multifactor), organizativos (políticas, normas, campañas de concienciación) y procedimientos de respuesta ante incidentes.

La gestión de riesgos es un proceso continuo, no un esfuerzo aislado. Los riesgos evolucionan por cambios tecnológicos, amenazas emergentes y nuevos marcos regulatorios, por lo que requiere revisiones y actualizaciones periódicas. El marco internacional más reconocido para estructurar esta gestión es la norma ISO/IEC 27005, que promueve un ciclo de mejora continua: identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos.

La toma de decisiones debe estar documentada y alineada con los objetivos globales del negocio y el cumplimiento normativo. Involucrar a todas las áreas de la organización, desde la alta dirección hasta los usuarios finales, es clave para crear una cultura de seguridad.

2.1 Identificación, evaluación y tratamiento de riesgos

A continuación, se detallan estas etapas con sus respectivas explicaciones y su orden de aplicación en la gestión de seguridad de la información:

- **Identificación de riesgos**

  Se inicia con el reconocimiento sistemático de activos, amenazas y vulnerabilidades que pueden afectar el funcionamiento o confidencialidad, integridad y disponibilidad de los sistemas. Este paso implica mapear los activos críticos, identificar fuentes potenciales de riesgo (internas y externas), así como las debilidades que podrían ser explotadas, usando

técnicas como entrevistas, revisión documental y análisis de incidentes previos.

- **Evaluación de riesgos**

  Luego, se cuantifica o cualifica la probabilidad de que una amenaza explote una vulnerabilidad y el impacto que esto tendría en la organización. Se utilizan metodologías formales para ponderar la criticidad y priorizar los riesgos, normalmente empleando matrices de riesgo, análisis de escenarios o cálculos probabilísticos, considerando aspectos técnicos, operativos y de negocio.

- **Tratamiento o mitigación del riesgo**

  Finalmente, se seleccionan y aplican controles o medidas que reduzcan el riesgo a niveles aceptables, mediante acciones como evitar el riesgo, reducirlo con controles técnicos u organizativos (firewalls, cifrado, capacitación), transferirlo (seguro) o aceptarlo cuando no se justifica una inversión mayor. Este proceso debe ser documentado, con planes de acción claros, indicadores para evaluar la eficacia de las medidas y procesos de revisión continua, asegurando la alineación con los objetivos estratégicos y cumplimiento normativo de la organización.

Estas etapas conforman un ciclo iterativo y dinámico para mantener la seguridad y resiliencia frente a amenazas cambiantes en sistemas de información.

2.2 Relación entre análisis forense y gestión de riesgos

La relación entre el análisis forense digital y la gestión de riesgos de seguridad de la información es estrecha y complementaria, pues ambos buscan proteger de manera

integral los activos digitales y minimizar el impacto de incidentes de seguridad en las organizaciones.

Al respecto, se dan las siguientes diferenciaciones:

- **Gestión de riesgos**

  Mientras la gestión de riesgos se enfoca en identificar, evaluar y tratar las amenazas y vulnerabilidades para prevenir incidentes.

- **Análisis forense**

  El análisis forense interviene cuando un incidente ya ha ocurrido, proporcionando mecanismos técnicos y metodológicos para la adquisición, preservación, análisis y presentación de la evidencia digital, con el fin de entender el suceso y atribuir responsabilidades.

El análisis forense aporta información valiosa para la gestión de riesgos, ya que sus hallazgos permiten validar o ajustar las hipótesis de amenazas, identificar nuevas vulnerabilidades explotadas y evaluar la efectividad de los controles existentes.

De esta manera se retroalimenta el ciclo de mejora continua de la seguridad organizacional, fortaleciendo las defensas y reduciendo la probabilidad y el impacto de futuros ataques. Además, la gestión de riesgos define protocolos y políticas de actuación que aseguran que el análisis forense se realice respetando la integridad y cadena de custodia de la evidencia, lo que es fundamental para que los resultados sean admisibles en procesos legales o auditorías. En un contexto organizacional, ambos procesos deben estar integrados en los planes de respuesta a incidentes y en las

estrategias de seguridad para garantizar una reacción rápida, coordinada y eficaz frente a las amenazas.

Por ejemplo, la identificación temprana de riesgos mediante evaluaciones, permite preparar y capacitar equipos forenses que actúen eficientemente tras un incidente; a su vez, los informes forenses detallados facilitan la toma de decisiones sobre qué riesgos priorizar y qué controles implementar o mejorar. La integración de análisis forense y gestión de riesgos, también contribuye a la resiliencia organizacional al permitir aprender de incidentes pasados, detectar patrones y anticipar tendencias de ataques. Así, la gestión de riesgos y el análisis forense se complementan en la protección y recuperación de los sistemas de información, reflejando un enfoque proactivo y reactivo necesario para la seguridad integral en entornos digitales modernos.

Analice la siguiente historia para tener mayor claridad sobre estas dos acciones:

1. Imagine una ciudad digital donde todos los datos son tesoros guardados en cofres electrónicos, protegidos día y noche por un sistema de vigilancia: la gestión de riesgos.
2. Este equipo vigila de cerca los posibles peligros: ladrones virtuales, tormentas de malware, accidentes internos, identificando por dónde podrían entrar, qué vulnerabilidades existen y qué medidas hay que reforzar antes de que ocurra un desastre.
3. Su trabajo es anticipar amenazas y levantar escudos: cortafuegos, sistemas de detección y reglas claras para todos los habitantes digitales.
4. Pero un día, pese a todo el esfuerzo, una amenaza logra burlar las defensas y roba información valiosa.

5. Aquí entra en acción el equipo de análisis forense digital, los detectives expertos. Llegan al lugar del incidente, preservan cuidadosamente cada evidencia, reconstruyen paso a paso lo sucedido y descifran cómo el atacante logró avanzar. Su investigación revela no solo qué se perdió, sino también qué falló y por qué.
6. Este hallazgo es crucial para la gestión de riesgos, que toma nota de las técnicas usadas por los atacantes y de las debilidades expuestas.
7. El aprendizaje del incidente sirve para ajustar controles, fortalecer protocolos y estar mejor preparados para el futuro. Así, ambos equipos se complementan: la gestión de riesgos prepara y previene, el análisis forense investiga y enseña tras lo ocurrido.
8. Juntos, mantienen la ciudad digital resiliente, aprendiendo de los errores y reforzando continuamente sus defensas frente a amenazas siempre cambiantes.

2.3 Herramientas y marcos para la gestión de riesgos (NIST, ISO/IEC 27005)

La gestión de riesgos en el ámbito de la seguridad de la información, requiere marcos y herramientas sólidas que permitan a las organizaciones identificar, analizar, tratar y monitorear posibles amenazas. Dos de los marcos más reconocidos internacionalmente son el NIST Risk Management Framework (RMF) y la norma ISO/IEC 27005. A continuación, la explicación de cada uno:

- **Marco NIST RMF**

  Es ampliamente utilizado en los Estados Unidos, especialmente en organismos federales y empresas que requieren altos estándares de

seguridad. Consta de seis pasos esenciales: preparación, categorización del sistema, selección de controles de seguridad, implementación de controles, evaluación de controles, autorización del sistema y monitoreo continuo. El proceso parte desde la categorización de los sistemas en función de su impacto potencial, seleccionando controles apropiados basados en publicaciones especializadas como NIST SP 800-37 o SP 800-53, hasta la implementación y supervisión constante de la eficacia de los mismos. Esta estructura fomenta una aproximación adaptable y escalable, facilitando la gestión proactiva del riesgo y la toma de decisiones informadas desde la alta dirección hasta el personal operativo.

- **Norma ISO/IEC 27005**

  Es una norma internacional dedicada a la gestión de riesgos de seguridad de la información y está alineada con la ISO/IEC 27001, la cual establece los requisitos para los Sistemas de Gestión de Seguridad de la Información (SGSI). ISO/IEC 27005 proporciona directrices para un proceso continuo y estructurado que incluye la definición del contexto, la identificación, análisis y evaluación de riesgos, así como su tratamiento, revisión y comunicación. El establecimiento del contexto implica comprender el entorno organizacional, sus objetivos y parte interesada. Posteriormente, se identifican los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información, se analizan las probabilidades y consecuencias, y se comparan con los criterios de aceptación establecidos. En el tratamiento de riesgos, se pueden emplear estrategias como la mitigación, transferencia, aceptación o eliminación del riesgo, mientras que el monitoreo y la revisión aseguran la mejora continua del sistema.

Uno de los principales aportes de la ISO/IEC 27005, es su enfoque flexible, apto para cualquier tipo y tamaño de organización. También enfatiza la interrelación entre los diversos métodos de evaluación de riesgos, permitiendo aproximaciones cualitativas, cuantitativas o semicuantitativas según las necesidades y recursos de la entidad. A diferencia del NIST, que provee listas de controles sugeridos, ISO/IEC 27005 se centra en el marco metodológico, dejando que cada organización adapte los controles y criterios a sus circunstancias particulares, siempre en coherencia con los requisitos de la ISO/IEC 27001.

Ambos marcos impulsan una cultura de gestión de riesgos, promueven la responsabilidad y concientizan a todos los niveles dentro de la organización sobre la importancia de la seguridad de la información. Facilitan la integración de los procesos de gestión de riesgos con otros enfoques empresariales y ofrecen una plataforma para la mejora continua, la automatización de tareas, la generación de reportes y el seguimiento de acciones correctivas.

Por lo tanto, el NIST RMF como la ISO/IEC 27005, representan pilares fundamentales en la administración de riesgos, destacándose cada uno en lo siguiente:

- **NIST RMF**

  Posee un enfoque práctico y detallado en los controles de seguridad.

- **ISO/IEC 27005**

  Ofrece una guía metodológica robusta y adaptable.

La elección o combinación de estos marcos, dependerá del contexto regulatorio, el sector y las necesidades específicas de cada organización. Implementarlos

correctamente contribuye a reducir amenazas, cumplir normativas y sustentar la confianza digital en los procesos, productos y servicios de la entidad.

Para tener una mayor claridad sobre lo explicado anteriormente, se relaciona la siguiente tabla que detalla los puntos clave que diferencian y relacionan el NIST RMF y la ISO/IEC 27005, en el contexto de la gestión de riesgos en seguridad de la información:

Tabla 2. Marcos y herramientas para la gestión de riesgo

Aspecto	**NIST Risk Management Framework (RMF)**	**ISO/IEC 27005**
Origen.	Estados Unidos (NIST).	Internacional (ISO/IEC).
Aplicación principal.	Entes gubernamentales y empresas.	Organizaciones de cualquier sector y tamaño.
Propósito.	Gestión de riesgos de seguridad de sistemas.	Gestión de riesgos de la información.
Estructura.	6 pasos: preparación, categorización, selección, implementación, evaluación, monitoreo.	Proceso continuo: contexto, identificación, análisis, evaluación, tratamiento,

Aspecto	NIST Risk Management Framework (RMF)	ISO/IEC 27005
		monitoreo y comunicación.
Enfoque.	Práctico y detallado, controles prescriptivos.	Metodológico, flexible y adaptable.
Relación con otras normas.	Basado en NIST SP 800-37 y SP 800-53.	Alineado con ISO/IEC 27001.
Controles de seguridad.	Lista específica de controles sugeridos.	Definición metodológica, controles elegidos por la organización.
Métodos de valoración.	Normalmente cualitativo, con algunos cuantitativos.	Permite enfoques cualitativos, cuantitativos y semicuantitativos.
Mejora continua.	Énfasis en monitoreo y revisión.	Énfasis en revisión continua y mejora.
Adaptabilidad.	Escalable y adaptable a diferentes escenarios.	Altamente flexible y adaptable.

Aspecto	NIST Risk Management Framework (RMF)	ISO/IEC 27005
Cultura organizacional.	Promueve responsabilidad y concientización.	Promueve cultura de gestión de riesgos.
Automatización y soporte.	Facilita reportes y seguimiento automatizados.	Admite integración con herramientas y automatización.
Decisión de controles.	Basado en impacto y categorización.	Basado en contexto y criterios propios.
Compatibilidad.	Integrable con otros marcos NIST.	Integra con otros estándares ISO.
Regulatorio.	Requerido en gobierno federal de EE. UU.	Recomendado internacionalmente.

3. Enfoques profesionales en la ciberseguridad

La ciberseguridad como carrera ha experimentado una transformación profunda a lo largo de las décadas recientes, impulsada por la evolución tecnológica y la sofisticación de las amenazas digitales. Por lo anterior, se relaciona lo más destacado en las siguientes etapas cronológicas, las cuales destacan su proceso evolutivo:

- **Década de 1980**

  Durante los años 80, los enfoques profesionales en ciberseguridad eran muy limitados y se centraban en roles técnicos básicos. Este periodo estuvo marcado por la aparición de los primeros virus informáticos y el surgimiento de los primeros antivirus, lo que sentó las bases iniciales de la disciplina. La mayoría de los especialistas provenían de áreas como la informática o las telecomunicaciones y actuaban de forma reactiva frente a los incidentes de seguridad. Los perfiles eran generalistas, principalmente administradores de sistemas, técnicos en redes y desarrolladores que adquirían conocimientos en seguridad de manera autodidacta.

- **Década de 1990**

  Con la masificación del internet, el crecimiento del comercio electrónico y la acelerada digitalización empresarial durante los años 90, surgieron nuevas necesidades en materia de protección de datos y sistemas. Esto impulsó la creación de los primeros programas académicos y certificaciones específicas en ciberseguridad, como CISSP (1994). Aun así, la carrera no era ampliamente conocida y la demanda laboral, aunque en aumento, no alcanzaba la magnitud que tiene en la actualidad.

- **Década de 2000**

  Durante la primera década de los 2000, la expansión del internet, la consolidación del comercio electrónico y el crecimiento de las amenazas cibernéticas, impulsaron una mayor especialización en ciberseguridad. Surgieron certificaciones más avanzadas, como CEH (2003) y comenzaron a aparecer carreras universitarias y programas de posgrado dedicados exclusivamente a la seguridad informática. La demanda laboral aumentó considerablemente y los perfiles profesionales evolucionaron desde roles generalistas hacia funciones más específicas, como analistas de seguridad, especialistas en pruebas de penetración y administradores de seguridad de redes.

- **Actualidad (2025)**

  La ciberseguridad es reconocida como una de las carreras más demandadas y estratégicas a nivel global. El mercado laboral enfrenta una enorme brecha de talento: se estima que actualmente se tiene hasta 3.5 millones de vacantes sin cubrir. Los perfiles profesionales se han diversificado enormemente, abarcando desde técnicos especializados (analistas, ingenieros, pentesters, analistas forenses) hasta estrategas (CISO, consultores, auditores, responsables de cumplimiento normativo).

Además, la formación es mucho más accesible y especializada: existen grados universitarios, másteres, programas de formación profesional y una vasta oferta de certificaciones reconocidas mundialmente. Se requieren conocimientos no solo técnicos, sino también en gestión de riesgos, normativas internacionales, derecho digital e incluso comunicación y liderazgo.

A nivel de oportunidades, las salidas profesionales se multiplican en todos los sectores: banca, salud, gobierno, industria, tecnología, etc. El trabajo remoto, la movilidad internacional y los salarios altos son características habituales. Existen altísimas tasas de empleabilidad, lo que convierte a la ciberseguridad en una carrera con futuro seguro y crecimiento sostenido.

De cara al futuro, la ciberseguridad se proyecta como una profesión fundamental en la sociedad digital. Las tendencias apuntan hacia:

- **Automatización e IA**

  Mayor automatización y uso de inteligencia artificial tanto en ataques como en defensa.
- **Crecimiento de roles híbridos**

  Expertos en seguridad con foco en IA, big data, protección de infraestructuras críticas, seguridad de IoT, cloud, blockchain, etc.
- **Necesidad de habilidades blandas**

  Liderazgo, toma de decisiones, resiliencia, pensamiento crítico y capacidad de adaptación constante.
- **Enfoque en formación continua**

  Los profesionales deberán actualizarse permanentemente ante la rápida evolución tecnológica y regulatoria.
- **Relevancia estratégica**

  Los expertos en ciberseguridad serán fundamentales no solo en la parte técnica, sino como agentes clave en la toma de decisiones empresariales, en la protección de la democracia y en la economía digital.

En conclusión, la ciberseguridad ha pasado de ser un campo técnico marginal a convertirse en una de las carreras más prometedoras del mundo actual y futuro, con demanda creciente, alto impacto social, excelente proyección salarial y un papel cada vez más relevante en todas las organizaciones y países.

3.1 Panorama del mercado profesional de la ciberseguridad

El mercado profesional de la ciberseguridad en la actualidad atraviesa un momento de auge sin precedentes, caracterizado por una demanda creciente de talento, salarios atractivos y enormes oportunidades de desarrollo profesional. Este sector se consolida como uno de los más dinámicos y estratégicos dentro del ecosistema digital global, impulsado por la acelerada transformación digital, la sofisticación de las amenazas y la obligatoriedad regulatoria en múltiples industrias.

Alta demanda y brecha de talento

La escasez de profesionales, es uno de los retos más destacados en la actualidad: como se mencionó previamente, la brecha global alcanza los 3.5 millones de vacantes sin cubrir, según reportes de la industria. El incremento de ataques cibernéticos —en particular ransomware y amenazas avanzadas a infraestructuras críticas— ha hecho que la protección digital sea una prioridad, incluso para pequeñas y medianas empresas, sectores financieros, sanitarios y gobiernos. Esta situación convierte la ciberseguridad en una carrera de futuro casi garantizado, con enorme proyección de empleabilidad y altos niveles de estabilidad laboral.

Perfiles y habilidades más demandados

Las empresas buscan perfiles variados y cada vez más especializados, entre los que destacan:

1. **Chief Information Security Officer (CISO)**

   Estratega encargado de liderar la política de seguridad y la protección de los activos informáticos.

2. **Ingeniero de ciberseguridad**

   Responsable del diseño e implementación de infraestructuras seguras.

3. **Analista de ciberseguridad**

   Especialista en detección y mitigación de vulnerabilidades, y respuesta ante incidentes.

4. **Auditor de ciberseguridad / hacker ético**

   Encargado de poner a prueba los sistemas y validar la robustez de las defensas.

5. **Data Protection Officer (DPO)**

   Supervisor del cumplimiento normativo en privacidad y protección de datos.

Especialidades emergentes incluyen expertos en automatización, inteligencia artificial aplicada a la seguridad, IoT, cloud security, gestión de identidades digitales y seguridad de arquitecturas Zero Trust.

Tendencias clave del mercado profesional

El mercado profesional de la ciberseguridad evoluciona rápidamente, impulsado por la tecnología, la globalización y las nuevas amenazas digitales. A continuación, se destacan algunas de las tendencias clave que marcan su desarrollo:

- **Crecimiento de las inversiones**

  Las empresas invertirán más de 212,000 millones USD en ciberseguridad en 2025, representando un crecimiento del 11 % interanual.

- **Mercado internacionalizado**

  El talento puede acceder a oportunidades laborales globales, gracias a la adopción del trabajo remoto e híbrido, lo que amplifica la competencia, pero también la oferta.

- **Automatización e inteligencia artificial**

  Si bien la IA automatiza tareas y redefine algunos perfiles, también abre nuevas áreas de especialización, como la supervisión ética y la ciberdefensa proactiva basada en modelos inteligentes.

- **Formación continua**

  La actualización constante es obligatoria; empresas y profesionales apuestan por certificaciones, másteres y programas de especialización para adaptarse a un entorno cambiante.

El crecimiento de la ciberseguridad varía según la región, con algunos países destacando por su rápida generación de oportunidades y aumento en inversiones. A continuación, se presenta un panorama internacional y el contexto específico de Colombia:

1. **Panorama internacional**

   España y América Latina muestran crecimientos sólidos: España es el segundo país del mundo en ritmo de creación de vacantes, solo superado por México y países como Colombia muestran crecimientos de inversión del 19 % anual, impulsando el desarrollo de talento local.

2. Panorama nacional

Colombia se consolida como uno de los mercados con mayor dinamismo en América Latina, impulsado por la acelerada digitalización de empresas, la expansión del comercio electrónico y el aumento tanto en la frecuencia como en la sofisticación de los ciberataques.

El sector público y privado están incrementando notoriamente su presupuesto, destinado a la protección digital. Por ejemplo, se han realizado inversiones significativas, como la inauguración del Centro de Operaciones de Seguridad Nacional (SOC) con un presupuesto de más de 15,000 millones de pesos, además de importantes iniciativas de empresas privadas. Existe un déficit significativo de profesionales en ciberseguridad. Actualmente, el país puede estar enfrentando una brecha de entre 68.000 y 112.000 vacantes sin cubrir en áreas como ciberseguridad, inteligencia artificial y desarrollo de software.

Esta alta demanda está generando una intensa competencia por el talento, lo que se traduce en oportunidades de empleo bien remuneradas y con excelentes perspectivas de desarrollo profesional. Ciudades como Bogotá, Medellín y Cali son los principales polos de innovación y adopción tecnológica, aunque la región Caribe empieza a mostrar avances llamativos.

El mercado está compuesto por actores internacionales y locales, con compañías como Fortinet, Cisco, IBM Security y firmas latinoamericanas relevantes. Sin embargo, persisten desafíos como la necesidad de mayor concienciación en pyme, una constante actualización frente a amenazas emergentes y el fortalecimiento de la capacitación y certificación profesional. Colombia dispone de una **estrategia nacional de ciberseguridad** alineada a marcos globales y con mejoras regulatorias como la Ley 1581

de 2012 sobre protección de datos, lo cual ha favorecido entornos más seguros y fomentado la adopción de buenas prácticas a nivel institucional y empresarial.

Ciberseguridad es, hoy más que nunca, una “apuesta segura” en términos profesionales: alta empleabilidad, oportunidades de rápido ascenso, salarios competitivos y la posibilidad de innovar y liderar cambios en todas las industrias. Quienes se formen y especialicen en este campo no solo aseguran su futuro profesional, sino que se convierten en piezas clave de la resiliencia y el desarrollo económico global.

3.2 Certificaciones en ciberseguridad: tipos y requisitos

Las certificaciones en ciberseguridad son credenciales reconocidas internacionalmente que validan el nivel de conocimiento, experiencia y habilidades técnicas de los profesionales en protección digital. Se han convertido en un requisito cada vez más común para acceder a mejores oportunidades laborales o para especializarse en distintos ámbitos de la seguridad informática.

A continuación, se presentan los principales tipos de certificaciones, su perfil y requisitos generales:

Tabla 3. Tipos y perfil de certificaciones

Certificación	Tipo/especialidad	Perfil/requisitos principales
CompTIA Security+.	Básica, generalista.	Recomendado: 2 años en TI, sin requisito formal, examen teórico.

Certificación	Tipo/especialidad	Perfil/requisitos principales
CISSP (ISC).	Gestión y arquitectura de seguridad.	5 años experiencia en seguridad, aprobar examen, adherirse a código ético.
CEH (Certified Ethical Hacker).	Hacking ético y pruebas ofensivas.	Experiencia en TI o curso oficial, aprobar examen práctico.
CISM (ISACA).	Gestión, dirección de seguridad.	5 años de experiencia en gestión seguridad TI, aprobar examen.
CRISC (ISACA).	Gestión de riesgos.	3 años experiencia en control y riesgo de TI, aprobar examen.
GSEC (GIAC).	Técnicas esenciales seguridad.	Sin requisito formal, recomendado experiencia en TI. Examen teórico.
OSCP (Offensive Security).	Pentesting, auditoría técnica avanzada.	Experiencia recomendada; examen práctico de hacking en entorno real.
CCSP (Certified Cloud Security Professional).	Seguridad en la nube.	Experiencia en TI/nube, aprobar examen internacional.

Certificación	Tipo/especialidad	Perfil/requisitos principales
CySA+ (CompTIA).	Detección y respuesta a amenazas.	3-4 años en seguridad, examen teórico.
CHFI (EC-Council).	Informática forense.	Experiencia en forense digital; examen y formación opcional.

De acuerdo a lo anterior, se relaciona la clasificación general de certificaciones, según sus objetivos:

- **Nivel básico y fundamental**

  CompTIA Security+, GSEC, CCT. Aptas para principiantes.
- **Defensa y análisis**

  CySA+, GCIH (gestión de incidentes), GSEC.
- **Ofensiva y pentesting**

  CEH, OSCP, PenTest+.
- **Gestión y gobierno**

  CISSP, CISM, CRISC, CCISO.
- **Cloud y tecnologías específicas**

  CCSP, AWS Security Specialty, Azure Security Engineer.
- **Forense y análisis post incidente**

  CHFI, GCFA.

Asimismo, se deben tener en cuenta los siguientes requisitos generales:

- La mayoría de certificaciones avanzadas requieren experiencia profesional (de 2 a 5 años), superar un examen extenso o práctico y en algunos casos, firmar y cumplir un código ético.
- Las certificaciones técnicas ofensivas suelen requerir aprobar pruebas prácticas en entornos reales simulados.
- Las de gestión (CISM, CRISC, CISSP) se centran en la experiencia en roles de liderazgo, dirección o gestión integral de la seguridad de la información.
- Certificaciones fundamentales o junior, exigen menos experiencia, aunque se recomienda formación básica en TI.

3.3 Educación formal y rutas de formación en ciberseguridad

La educación formal y las rutas de formación en ciberseguridad, ofrecen hoy un abanico amplio y flexible para quienes desean ingresar, especializarse o avanzar dentro de este dinámico campo profesional, sin importar su punto de partida.

Educación formal en ciberseguridad

La formación académica en ciberseguridad ofrece múltiples alternativas según el nivel de especialización y el enfoque profesional deseado. A continuación, se presentan los principales tipos de programas y su orientación:

- **Grado universitario**

  Existen programas de pregrado específicamente diseñados para formar profesionales en ciberseguridad, orientados tanto al desarrollo técnico como a la gestión estratégica. Estos estudios suelen incluir materias como redes, programación segura, criptografía, gestión de riesgos y protección de datos.

- **Ingenierías con énfasis en seguridad**

  Algunos programas de ingeniería han incorporado énfasis o módulos en ciberseguridad, abarcando el diseño y operación de infraestructuras digitales seguras, la prevención de ataques y la evaluación de vulnerabilidades.

- **Especializaciones y maestrías**

  A nivel posgrado, la formación se vuelve más específica y estratégica. Las especializaciones profundizan en áreas clave, como análisis de amenazas, investigación forense digital, diseño de políticas y gobierno de la seguridad. Las maestrías suelen incorporar tanto aspectos técnicos avanzados como gestión, cumplimiento de normativas y liderazgo para preparar a quienes aspiran a roles directivos o de consultoría.

- **Diplomados y cursos institucionales**

  Además de titulaciones tradicionales, muchas instituciones han diseñado diplomados, talleres y programas de capacitación para empresas, reforzando tanto competencias técnicas como una cultura organizacional centrada en la seguridad.

Rutas de formación profesional y continua

La formación en ciberseguridad no sigue un único camino; existen diversas rutas que permiten desarrollar competencias, según los intereses, el nivel de experiencia y las metas profesionales de cada persona. Por ello, se presentan las principales alternativas de formación y actualización continua.

- **Formaciones modulares escalables**

  Existen rutas de aprendizaje que permiten avanzar paso a paso, comenzando con fundamentos básicos y progresando hacia la defensa, el monitoreo, el desarrollo seguro de software, el análisis forense y la simulación de ataques, según el área de interés.

- **Rutas especializadas: Blue team y Red team**

  Algunas trayectorias educativas permiten optar por especializaciones prácticas en defensa (Blue team: monitoreo, respuesta a incidentes, administración de sistemas seguros) o ataque (Red team: pruebas de penetración, evaluación de seguridad ofensiva).

- **Cursos cortos, microcertificaciones y formación en línea**

  La oferta online facilita adquirir conocimientos actualizados, a través de cursos breves, certificaciones modulares, laboratorios virtuales, simulaciones realistas y retos de hacking ético. Este formato es ideal para quienes desean compatibilizar la formación con la vida laboral o actualizarse de manera continua en nuevas tecnologías y amenazas.

- **Aprendizaje autodirigido**

  Los recursos abiertos y gratuitos, como plataformas educativas y comunidades de ciberseguridad, complementan la formación formal y permiten practicar habilidades en escenarios prácticos.

4. Sensibilización de usuarios sobre ciberseguridad

Adoptar hábitos responsables que ayuden a navegar de manera segura en el mundo digital, es un compromiso de toda la organización, independientemente del software, políticas y hardware que se implemente para mitigar estos riesgos.

La sensibilización en ciberseguridad consiste en adquirir conocimientos y hábitos para reconocer, prevenir y reaccionar ante los riesgos digitales, como fraudes, malware o robo de información. La mayoría de los incidentes de seguridad suceden por errores humanos, por lo que estar bien informado es clave para evitar ser víctima de un ciberataque.

Con solo hacer clic en un enlace malicioso, es posible comprometer múltiples sistemas, lo que constituye un ejemplo común de ataque.

A continuación, se presentan algunos aspectos esenciales que todo usuario debería conocer para fortalecer sus hábitos digitales y cumplir con las normativas vigentes:

- **¿En qué consiste un programa de sensibilización en ciberseguridad?**
  Un programa de sensibilización busca cambiar comportamientos y actitudes mediante actividades constantes: seminarios, capacitaciones en línea, vídeos, juegos y simulaciones. Debe ser sencillo, práctico y repetirse de forma periódica.
  Ejemplo de actividades: reconocer intentos de phishing, aprender a crear contraseñas seguras y conocer cómo actuar si ocurre un incidente.

- **¿Qué es la información sensible y por qué protegerla?**

  La información sensible son todos aquellos datos que, si se hicieran públicos o llegaran a manos indebidas, causarían daño a una persona u organización. Incluye nombres completos, números de identificación, cuentas bancarias, contraseñas, información médica, etc.

  Consecuencias de no protegerla: robo de identidad, pérdidas económicas, daño a la reputación.

- **Cumplimiento normativo: ¿Qué es y para qué sirve?**

  El cumplimiento normativo en ciberseguridad es seguir las leyes y estándares que regulan la protección de datos y sistemas. Su objetivo es garantizar la privacidad y la seguridad digital, evitando sanciones legales, pérdida de confianza y otros riesgos.

  Ejemplo en Colombia: Ley 1273 de 2009, que sanciona los delitos informáticos.

Prácticas y tecnologías de protección básicas

Algunas tecnologías esenciales para proteger la información incluyen:

- **Firewalls**

  Barreras que bloquean accesos no autorizados.

- **Antivirus**

  Detectan y eliminan software malicioso.

- **Sistemas de destrucción de intrusos**

  Alertan sobre actividades sospechosas.

- **Cifrado**

  Protege los datos para que no puedan ser leídos si son interceptados.

Hábitos responsables para una buena ciberseguridad

Es importante tener en cuenta las siguientes recomendaciones:

1. Use contraseñas largas y únicas, cámbielas regularmente.
2. No comparta contraseñas ni información sensible.
3. Evite conectarte a redes Wi-Fi públicas sin protección.
4. Actualice siempre los dispositivos y aplicaciones.
5. Revise que los sitios web sean seguros (inicio con "https").
6. Utilice doble autenticación si está disponible.
7. Bloquee el computador o celular cuando no los use.

Las simulaciones de ataques

Sirven para poner a prueba los conocimientos y ver cómo se reacciona ante situaciones reales de riesgo, sin perjudicar los sistemas auténticos. Así, se puede identificar las áreas de mejora y reforzar la protección ante ataques reales. También las campañas de sensibilización (carteles, correos informativos, actividades de grupo) y el esfuerzo de toda la comunidad educativa o laboral, ayudan a construir una cultura de seguridad, donde todos participan activamente y comparten buenas prácticas para protegerse mutuamente.

Un ejemplo de esto, son las pruebas de phishing simuladas.

Síntesis

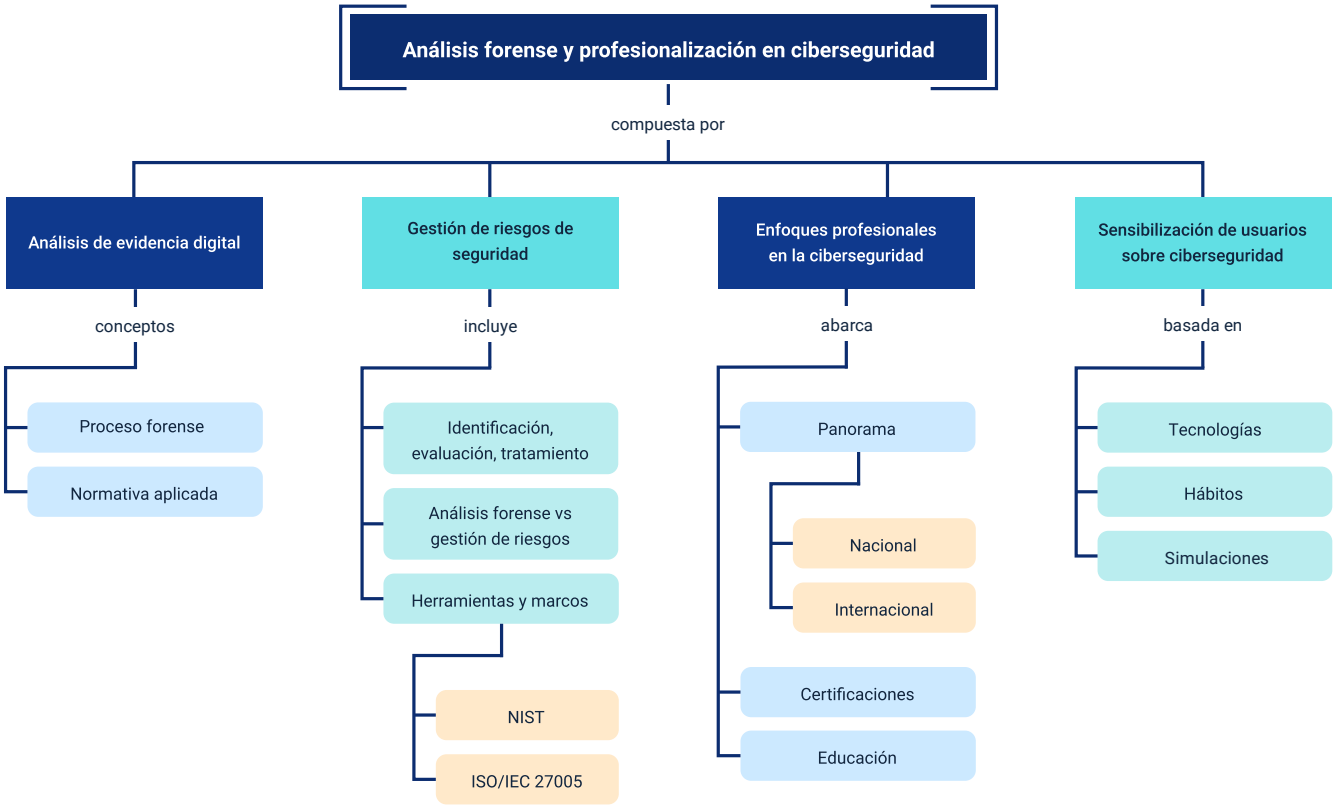
Este componente aborda principalmente el análisis forense digital, mostrando su importancia y procedimiento dentro de la ciberseguridad. El proceso forense sigue varias etapas clave enfocadas en la evidencia y manejo de la información.

Además, se ejemplifican prácticas comunes en análisis forense y paralelamente, se incluyen comparativas entre el NIST Risk Management Framework (RMF) y la norma ISO/IEC 27005, destacando sus diferencias en origen, aplicación, estructura y enfoque metodológico para la gestión de riesgos en seguridad de la información.

También se presentan certificaciones claves en ciberseguridad, detallando certificaciones básicas, avanzadas, ofensivas, de gestión y especializadas en cloud o forense.

Por último, se resalta la importancia de complementos como cursos cortos, microcertificaciones y formación en línea, que facilitan la actualización continua e igualmente, se relaciona la importancia de la sensibilización del usuario en todos los procesos de ciberseguridad.

En suma, el contenido enfatiza en la importancia del análisis forense digital como pilar en la investigación y defensa en ciberseguridad, la gestión de riesgos a través de marcos reconocidos y la necesidad de formación constante y certificaciones especializadas para abordar los retos contemporáneos de la seguridad informática.


Análisis forense y profesionalización en ciberseguridad
compuesta por
Análisis de evidencia digital
Gestión de riesgos de seguridad
Enfoques profesionales en la ciberseguridad
Sensibilización de usuarios sobre ciberseguridad
conceptos
incluye
abarca
basada en
Proceso forense
Normativa aplicada
Identificación, evaluación, tratamiento
Análisis forense vs gestión de riesgos
Herramientas y marcos
NIST
ISO/IEC 27005
Panorama
Nacional
Internacional
Certificaciones
Educación
Tecnologías
Hábitos
Simulaciones

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
2. Gestión de riesgos de seguridad de la información.	Ecosistema de Recursos Educativos Digitales SENA. (2022, 12 de junio). Tratamiento de riesgos de ciberseguridad [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=X-hUaV0nsnk&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA
2.1 Identificación, evaluación y tratamiento de riesgos.	Ecosistema de Recursos Educativos Digitales SENA. (2023, 24 de junio). Fundamentos para la gestión del riesgo de ciberseguridad [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=rIInW1zOe_I&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA
2.1 Identificación, evaluación y tratamiento de riesgos.	Grupo Fraga. (2022, 1 de agosto). Cómo realizar la evaluación de riesgos según la ISO 27001 [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=9w7O4in-Oos&ab_channel=GrupoFraga

Tema	Referencia	Tipo de material	Enlace del recurso
2.2 Relación entre análisis forense y gestión de riesgos.	Ecosistema de Recursos Educativos Digitales SENA. (2021, 1 de junio). Gestión del riesgo [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=KU4j7Cio1rk&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA
2.3 Herramientas y marcos para la gestión de riesgos (NIST, ISO/IEC 27005).	Ecosistema de Recursos Educativos Digitales SENA. (2021, 30 de septiembre). Análisis, valoración de riesgos y controles de ciberseguridad: riesgos [Video].	Video.	https://www.youtube.com/watch?v=QLWc_y6HMuA&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA

Glosario

Análisis forense digital: disciplina que se encarga de identificar, recolectar, preservar, analizar y presentar evidencia digital, con el fin de garantizar su integridad y validez legales para la investigación de incidentes o delitos informáticos.

Cadena de custodia: proceso riguroso que documenta cada manipulación y traslado de la evidencia digital, asegurando su autenticidad y admisibilidad en procedimientos legales.

Certificación CISSP: credencial reconocida internacionalmente para profesionales que demuestran experiencia y conocimientos en gestión y arquitectura de seguridad de la información.

Evidencia digital: información en formato electrónico almacenada en dispositivos digitales, que puede ser utilizada como prueba en investigaciones o procesos judiciales.

ISO/IEC 27005: norma internacional que proporciona directrices metodológicas para la gestión de riesgos en seguridad de la información, flexible y adaptable a diferentes organizaciones.

Microcertificaciones: cursos o certificaciones cortas y especializadas que permiten adquirir conocimientos específicos y actualización constante en determinadas áreas de ciberseguridad.

Monitoreo continuo: proceso permanente de supervisión del estado de seguridad y efectividad de controles implementados para detectar incidentes o desviaciones.

NIST Risk Management Framework (RMF): marco de gestión de riesgos desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., que consta de etapas para categorizar, seleccionar, implementar, evaluar, autorizar y monitorear controles de seguridad.

Pentesting (Pruebas de penetración): técnica ofensiva que consiste en simular ataques controlados para identificar vulnerabilidades en sistemas y redes informáticas.

Preservación de evidencia: conjunto de acciones que garantizan que la información digital sea mantenida intacta y sin alteraciones desde su obtención hasta su presentación.

Referencias bibliográficas

Asociación Española de Normalización. (2021, 3 de diciembre). UNE-EN ISO/IEC 27701 Gestión de la Privacidad de la Información. UNE.

https://www.une.org/la-asociacion/sala-de-informacion-une/notas-de-prensa/publicada-la-norma-une-en-isoiec-27701-para-la-gestion-de-la-privacidad-de-la-informacion/

Caballero Velasco, M. Á. (2015). El libro del hacker. Anaya Multimedia.

Cano, J. E. (2018). Ciberseguridad y protección de datos personales en Colombia. Ediciones Jurídicas Gustavo Ibáñez.

Ferrer, E. A. (2023). Estudios de cibercrimen. Ediciones Olejnik.

Gómez, L. A. & Rodríguez, M. P. (2020). Gestión de riesgos en seguridad informática: Enfoque práctico para organizaciones colombianas. Editorial Universidad del Rosario.

National Institute of Standards and Technology (NIST). (2024, 26 de febrero). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Paredes, A. R. Z., Quevedo, I. M. S., & Chalacán, L. J. M. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. Journal of Business and Entrepreneurial Studies: JBES, 4(2), 232-241.

Pérez, C. A., & González, F. J. (2021). Seguridad en redes y criptografía aplicada. Ediciones de la U.

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocio Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Javier Eduardo Díaz Machuca	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Andrés Felipe Velandia Espitia	Evaluador instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Iván Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
José Jaime Luisa Tang Pinzón	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Diego Fernando Velasco Güiza	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Veimar Celis Meléndez	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Gilberto Junior Rodríguez Rodríguez	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima
Norma Constanza Morales Cruz	Evaluadora de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Javier Mauricio Oviedo	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima