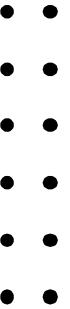
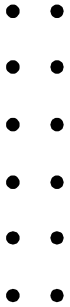


Cadena de Custodia y Entrega (“La Prueba”)





INSTRUCTOR

CPP©

Carlos Ramírez Rodríguez, CPP

Consultor internacional en seguridad convergente, ciberseguridad y gestión de riesgos, con amplia experiencia liderando proyectos de protección de infraestructuras críticas en sectores como energía, minería y telecomunicaciones.

Es miembro activo de ASIS International e IFPO, y ha sido expositor en congresos internacionales sobre protección de activos, ciberdefensa y cultura de seguridad.

Fundador de Smart Spartans, empresa dedicada al cumplimiento normativo y la integración de seguridad física y cibernética, y creador de la plataforma SECURIX, una solución tecnológica para la gestión de incidentes y riesgos convergentes.

Autor del libro “Defensa Total: Ciberseguridad y Seguridad Física en la Protección de Infraestructuras Críticas”, reconocido por su enfoque innovador en la formación de profesionales de seguridad moderna.

Su misión es elevar el nivel profesional del sector de la protección, inspirando a los futuros Oficiales Certificados CPO a comprender que la verdadera prevención se logra con conocimiento, ética y liderazgo.



INTERNATIONAL
FOUNDATION FOR
PROTECTION OFFICERS
KNOWLEDGE TO PROTECT

Cadena de Custodia: qué es y por qué importa



- ❑ Registro completo del manejo de la evidencia
- ❑ Permite saber:
 - Quién la obtuvo
 - Quién la manipuló
 - Quién la trasladó
 - Quién la recibió
- ❑ Debe ser:
 - Continua (sin interrupciones)
 - Documentada (con respaldo)
 - Trazable (verificable)

“Si no puedes reconstruir el recorrido de la evidencia... no puedes defenderla.”



Formulario de Cadena de Custodia: el respaldo del proceso



- ❑ Documento que registra todo el manejo de la evidencia
- ❑ Permite mantener la trazabilidad completa
- ❑ Información mínima:
 - Identificación de la evidencia
 - Fecha y hora de cada acción
 - Quién entrega
 - Quién recibe
 - Medio de almacenamiento (pendrive, disco, etc.)
- ❑ Debe ser:
 - Completo
 - Claro
 - Sin espacios en blanco

Trazabilidad: mantener la cadena sin interrupciones

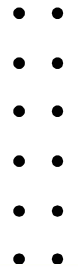


- ❑ La evidencia debe tener un recorrido claro y continuo
- ❑ Cada traspaso debe quedar registrado
- ❑ Evitar:
 - ✗ Accesos no autorizados
 - ✗ Copias sin control
 - ✗ Períodos sin registro
- ❑ Riesgo crítico:
 - Pérdida de control sobre la evidencia
 - Dudas sobre su integridad

“Un solo punto sin control... puede invalidar todo el proceso.”

Entrega a autoridad: control y formalidad

- ❑ La entrega de evidencia es un acto formal
- ❑ Debe quedar completamente registrada
- ❑ Registrar:
 - Identificación del funcionario (nombre / placa / CI)
 - Fecha y hora de entrega
 - Medio entregado (pendrive, disco, etc.)
- ❑ Solicitar:
 - Constancia de recepción
 - Firma o respaldo del traspaso
- ❑ En caso de flagrancia:
 - Actuar con rapidez, pero sin perder el registro.”



Acta de entrega: cierre formal de la evidencia



- ❑ Documento que formaliza la entrega de la evidencia
- ❑ Deja constancia del traspaso de custodia}
- ❑ Debe incluir:
 - Identificación de la evidencia
 - Detalle del contenido entregado
 - Fecha y hora
 - Identificación de las partes
 - Firmas
- ❑ Permite:
 - Cerrar la cadena correctamente
 - Evitar cuestionamientos posteriores

“La evidencia no se entrega... se formaliza.”

Cierre del ciclo: control posterior a la entrega

- ❑ Confirmar recepción de la evidencia
- ❑ Verificar que el traspaso quedó documentado
- ❑ Gestión interna posterior:
 - Eliminación de copias no autorizadas
 - Resguardo del archivo original
 - Control de accesos
- ❑ Evitar:
 - ✗ Evidencia circulando sin control
 - ✗ Duplicaciones innecesarias
 - ✗ Pérdida de trazabilidad interna

“Cada copia sin control... es un riesgo para la evidencia.”



CASE NOTES

- Case wiring
- Case Firewall
- Case host
- Case building
- Server logs

Case Notes

EVIDENCE

NETWORK TRAFFIC MONITORING

NETWORK TRAFFIC MONITORING

INCIDENT TIMELINE - LIVE ANALYSIS

CORRELATION ENGINE

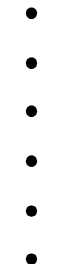
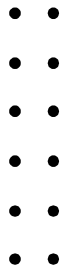
SECURITY
POTES

**OFFICER
M. RIVERA**

CASE MATCH
FACE MATCH
BUCKET MATCH

MUCHAS
GRACIAS!!

CARLOS RAMIREZ, CPP
+56950923135



INTERNATIONAL
FOUNDATION FOR
PROTECTION OFFICERS
KNOWLEDGE TO PROTECT