XXIII Congreso Regional de Auditoría Interna

Control de Gestión, Riesgo y Finanzas

Del 19 al 22 de Junio 2025

Hotel Live Aqua Punta Cana

Punta Cana, República Domninicana

Una Auditoría Diferente.

Mis Experiencias de Hacker como Auditor.

Julio Ureña

Fundador & Chief Technology Officer
Plaintext Cybersecurity Solutions

CRAICG 2025 PUNTA CANA

Instituto de Auditores Internos República Dominicana

The Institute of Internal Auditors

Mi Primera Experiencia con el Hacking

¿Qué Aprendí de este Escenario?

1. La ciberseguridad **no es un juego**.
2. Debo Tomar **una Actitud Proactiva.**
3. Continuamente **Monitorear.**
4. Comprender la **Mentalidad** de un **Hacker**.

Mi introducción a la mentalidad del Hacker

Me hice a mi mismo la siguiente pregunta:

¿Y será cierto esto que digo? *¿Qué instalar estos equipos evitará que hackeen a mis clientes?*

Observaciones Comunes como Auditor/Hacker

Cumplimiento y Pruebas: Complementarios, No Excluyentes

Enfoque Documental vs. Enfoque Operativo

- El **cumplimiento** (políticas, procedimientos, certificaciones) define qué debe hacerse.
- Las **pruebas** (pentests, auditorías técnicas, simulaciones) validan cómo se aplica en la realidad.

Revisiones de Cumplimiento

Pruebas de Ciberseguridad

Cumplimiento y Pruebas: Complementarios, No Excluyentes

Enfoque Documental vs. Enfoque Operativo

- El **cumplimiento**
- Las **pruebas**

Cumplimiento

- ✓ Revisión de Políticas y Procedimientos
- ✓ Inventario y Clasificación de Activos
- ✓ Control de Accesos y Gestión de Identidades
- ✓ Monitoreo y Registro de Eventos
- ✗ Pruebas de Vulnerabilidad y Gestión de Parcheo

Pruebas

- ✓ Gestión de Autenticación y Autorización
- ✓ Validación yGestión de Sesiones y Cookies
- ✗ Saneamiento de Entradas
- ✗ Manejo de Errores y Registro (Logging)
- ✗ Configuración Segura y Dependencias

Ausencia de Ciclos de Desarrollo Seguro

92%

de las compañías tuvieron una brecha por una aplicación que ellos desarrollaron.

91%

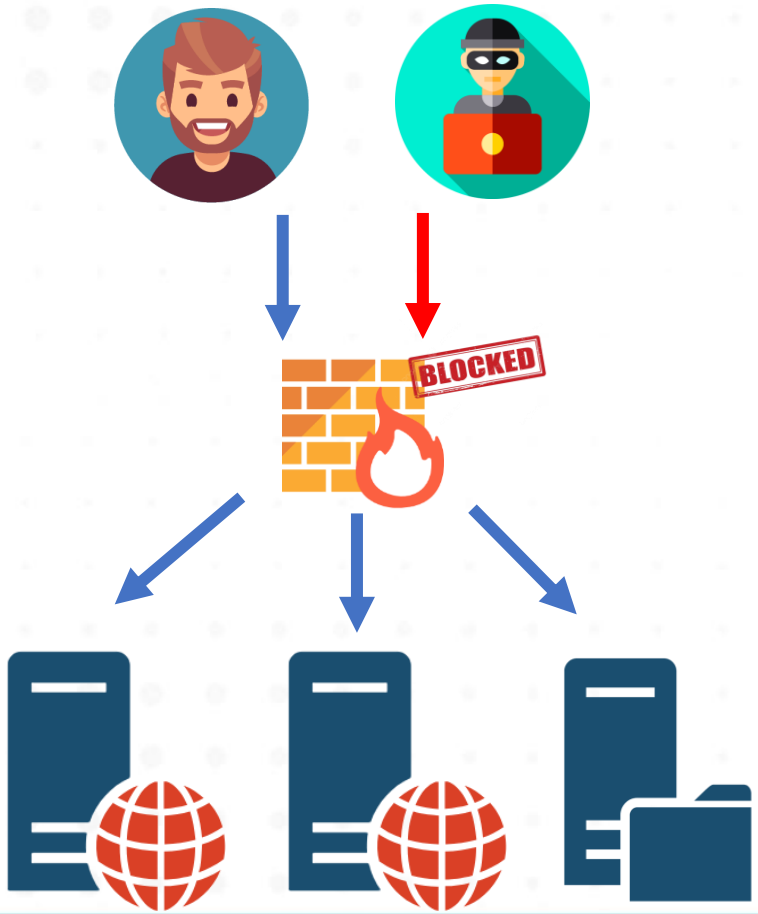
de las compañías han publicado concientemente, aplicaciones vulnerables.

67%

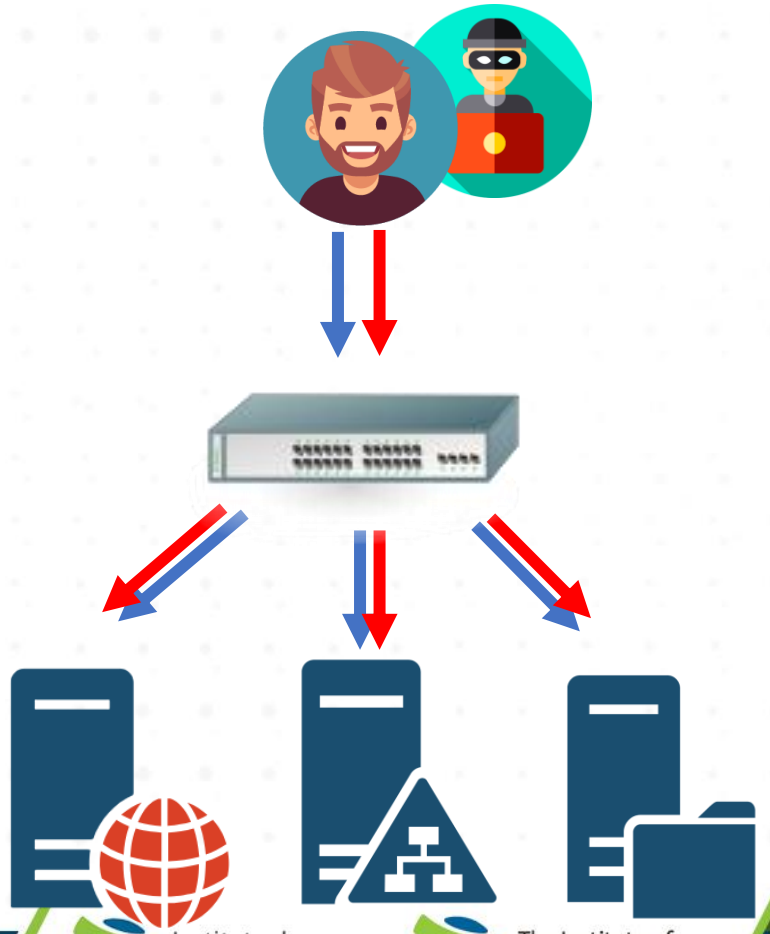
de las aplicaciones están actualmente funcionando en la nube

Muchos Controles Externo & Falta de Controles Internos

Red Externa



Red Interna



Principales riesgos que enfrentan las organizaciones

Audit area	Average of all regions	Asia Pacific	Latin America	Africa	North America	Middle East	Europe
Cybersecurity	73%	66%	75%	58%	85%	70%	84%
Human capital	51%	59%	44%	39%	65%	47%	50%
Business continuity	47%	61%	47%	52%	36%	53%	35%
Regulatory change	39%	35%	48%	32%	43%	33%	43%
Digital disruption	34%	30%	38%	33%	36%	32%	33%
Financial liquidity	32%	21%	33%	47%	28%	38%	26%
Market changes	32%	47%	26%	21%	41%	26%	30%
Geopolitical uncertainty	30%	28%	42%	25%	28%	16%	43%
Governance/corporate reporting	27%	24%	18%	36%	16%	45%	22%
Supply chain and outsourcing	26%	27%	16%	19%	36%	28%	30%
Organizational culture	26%	23%	26%	34%	21%	30%	20%
Fraud	24%	22%	30%	46%	9%	26%	13%
Communications/reputation	21%	18%	22%	27%	21%	28%	12%
Climate change	19%	22%	22%	19%	12%	10%	31%
Health and safety	11%	12%	8%	10%	17%	9%	13%
Mergers and acquisitions	6%	4%	3%	3%	8%	10%	8%

risk-in-focus-survey-results-global-summary-2024.pdf

Conclusiones

Cumplir ≠ Estar Seguro | Pruebas ≠ Estar Seguro

La mejor forma que **podemos apoyar a las organizaciones es guiándolas** para **comprender que la seguridad evoluciona constantemente**, que **deben preocuparse por estar en cumplimiento** con los estándares de sus industrias, **pero que deben probar la eficacia de los controles y soluciones** que están implementando.

Los informes de la IIA, ISACA y Deloitte coinciden en que **los mejores resultados se logran cuando el cumplimiento normativo se complementa con pruebas técnicas de eficacia.**

Contactos & Preguntas adicionales

Julio Ureña
juliourena@plaintexto.do
juliourena@redteamrd.org
Móvil: +1-829-641-8347
Fundador & CTO – Plaintext Cybersecurity Solutions
Fundador Comunidad de Hackers RedTeamRD & HackConRD

PLAINTEXT CYBERSECURITY

Certificaciones

HackConRD

REDTEAMRD