23 CONGRESO NACIONAL DE SEGURIDAD

INCUMPLIMIENTOS Y HALLAZGOS COMUNES QUE SE IDENTIFICAN EN AUDITORÍAS DE CIBERSEGURIDAD

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

CNS

Wilson Andia

- Ingeniero de Sistemas con Postgrados en Seguridad y Auditoría de TI, con más de 20 años de experiencia.
- Instructor acreditado CISA® y CRISC ® por APMG.
- Inicialmente fue Analista Programador en diferentes Empresas. Posteriormente Consultor Internacional en Auditoría de TI y Seguridad en Sud, Centro América y el Caribe en Bancos de prestigio y Empresas, así como Entidades Fiscalizadoras (Contralorías, Cámara de Cuentas, Tribunal de Cuentas), Proy. BID, Banco Mundial, PNUD y Unión Europea.
- Actualmente es Director de Auditorías y Consultorías de TI de la Firma PKF Dominicana, firma con presencia en República Dominicana en el Sector Bancario, Entidades Públicas y Privadas.

CNS

OBJETIVO

Generar conciencia a las Organizaciones sobre la importancia de la Ciberseguridad y que aún nos falta por madurar en las Entidades e Instituciones.

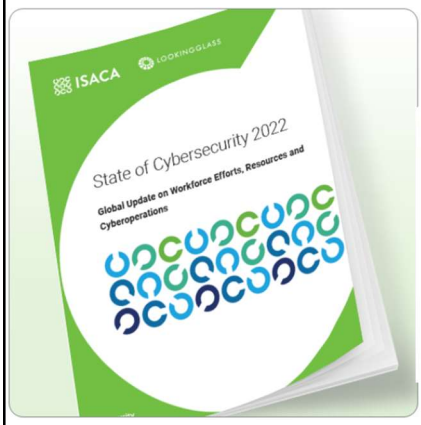
Socializar algunos incumplimientos o hallazgos más comunes comunes en diferentes tipos de Empresas.

Recomendar el fortalecimiento de las Áreas de TI, Seguridad de la Información, Riesgos y Auditoria Interna en las Organizaciones.

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

ESTADO DE LA CIBERSEGURIDAD 2022

Actualización global sobre los esfuerzos, recursos y Ciberoperaciones



¿Su empresa está experimentando un aumento o una disminución de los ataques cibernéticos en comparación con hace un año?

FIGURE 31—CHANGE IN NUMBER OF CYBERSECURITY ATTACKS

Is your enterprise experiencing an increase or decrease in cyberattacks as compared to a year ago?

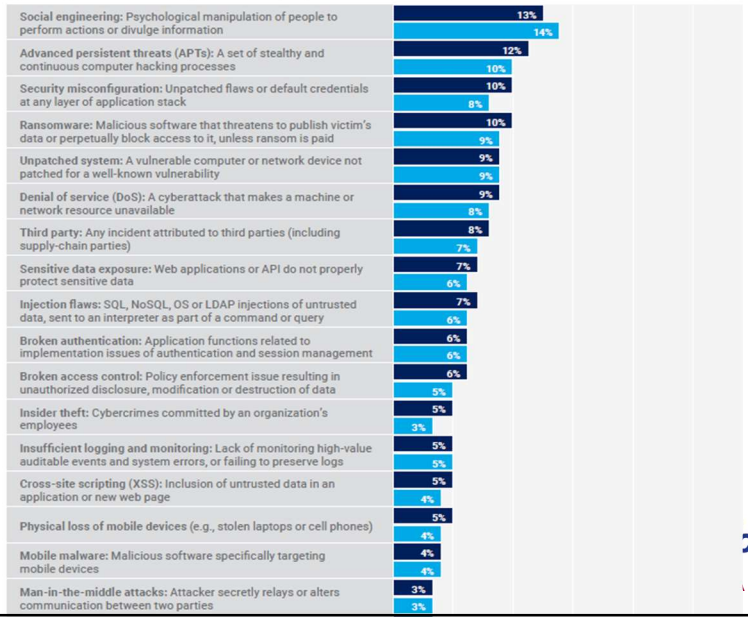
https://www.isaca.org/go/state-of-cybersecurity-2022?tfa_next=%2Fresponses%2Flast_success%3Fjsid%3DeyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ImI5NjBiNWY5NjMzNTA0NjM0MTgwYTU3NWEyOTU2MDVllg.mecFOYb0IsWIGe1WXdib50-QxzFHJxvu0hs-XXH6zOk

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

ESTADO DE LA CIBERSEGURIDAD 2022

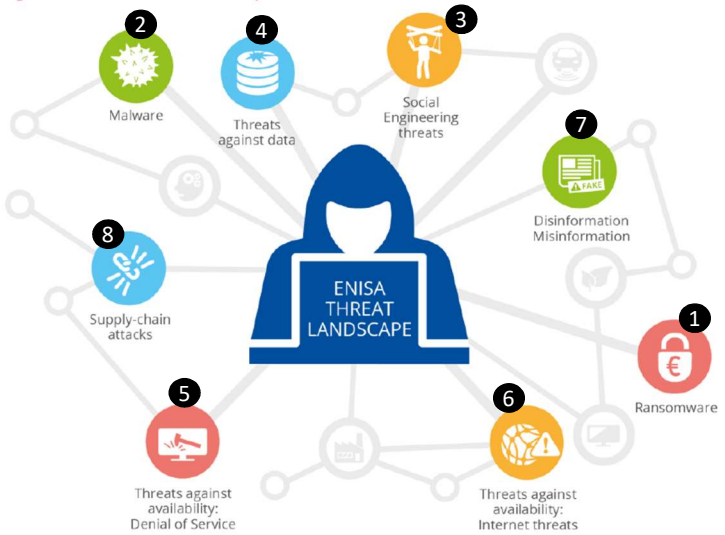
FIGURE 36—ATTACK TYPES

If your organization was compromised this year, which of the following attack types were used? Select all that apply.



AMENAZAS Y RIESGOS DE TI

Figure 1: ENISA Threat Landscape 2022 - Prime threats



https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

TENDENCIA DE ACTORES DE AMENAZAS

1. ACTORES PATROCINADOS POR ESTADOS
2. CIBERCRIMINALES externos e INSIDER (internos)
3. CIBERDELINCUENTES A CONTRATO
4. HACKTIVISTAS

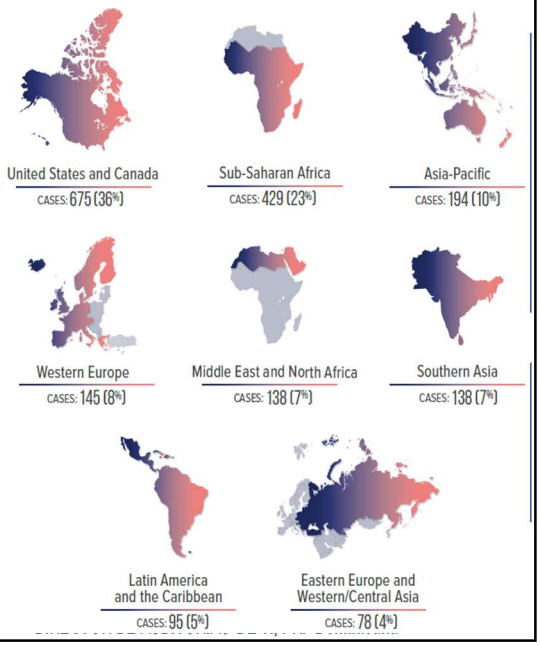
CNS

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA

Concientizando sobre el fraude ocupacional

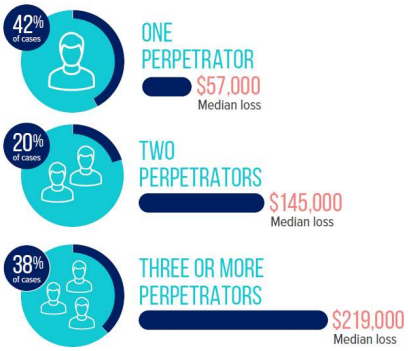
https://acfepublic.s3.us-west-2.amazor

FIG. 1 REPORTED CASES BY REGION



Fraude ocupacional
Factor Humano, el eslabón más débil

Usuarios Deshonestos



UN CASO TÍPICO DE FRAUDE
Dura 12 meses
antes de ser detectado

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

Esquemas de fraude y Departamentos

Departa-mentos	Casos	Facturación	Robo de Efectivo registrado	Robo de efectivo disponible	Manipulación de cheques	Corrupción	Reembolso de gastos	Fraude en EEFF	Bienes que no son efectivo	Nómina	Desembolsos	Robo de Efectivo no registrado
	Esquemas de fraude											
Operaciones	273	16%	7%	8%	11%	48%	9%	6%	16%	8%	1%	6%
Contabilidad	230	24%	15%	13%	29%	33%	10%	10%	7%	16%	3%	19%
Alta Dirección	206	31%	9%	10%	12%	65%	18%	22%	21%	13%	2%	12%
Ventas	203	11%	6%	7%	2%	51%	8%	6%	18%	4%	2%	11%
Servicio al cliente	140	8%	10%	16%	11%	44%	6%	7%	17%	6%	3%	10%
Soporte administrativo	131	23%	8%	15%	15%	37%	16%	5%	12%	12%	5%	10%
Adquisiciones	131	27%	1%	4%	2%	82%	5%	2%	14%	3%	0%	2%
Finanzas	95	26%	7%	11%	12%	48%	20%	14%	12%	7%	3%	12%

Menos riesgo — Más riesgo

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

Estadísticas

MINISTERIO DEL INTERIOR

SECRETARÍA DE ESTADO DE SEGURIDAD

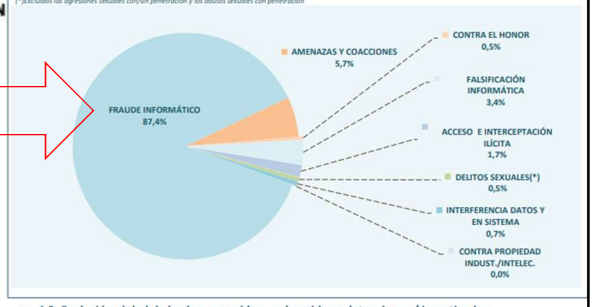
GABINETE DE COORDINACIÓN Y ESTUDIOS

DATOS ESTADÍSTICOS DE CIBERCRIMINALIDAD (Fuente de datos: Sistema Estadístico de Criminalid

>> 4.1. Evolución de hechos conocidos por categorías delictivas

HECHOS CONOCIDOS	2017	2018	2019	2020	2021
ACCESO E INTERCEPTACIÓN ILÍCITA	3.150	3.384	4.004	4.653	5.342
AMENAZAS Y COACCIONES	11.812	12.800	12.782	14.066	17.319
CONTRA EL HONOR	1.561	1.448	1.422	1.550	1.426
CONTRA PROPIEDAD INDUST./INTELEC.	121	232	197	125	137
DELITOS SEXUALES(*)	1.392	1.581	1.774	1.783	1.628
FALSIFICACIÓN INFORMÁTICA	3.280	3.436	4.275	6.289	10.47
FRAUDE INFORMÁTICO	94.792	136.656	192.375	257.907	267.01
INTERFERENCIA DATOS Y EN SISTEMA	1.291	1.192	1.473	1.590	2.13
Total HECHOS CONOCIDOS	**117.399**	**160.729**	**218.302**	**287.963**	**305.477**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



>> 4.2. Evolución global de hechos conocidos, esclarecidos y detenciones / investigados

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

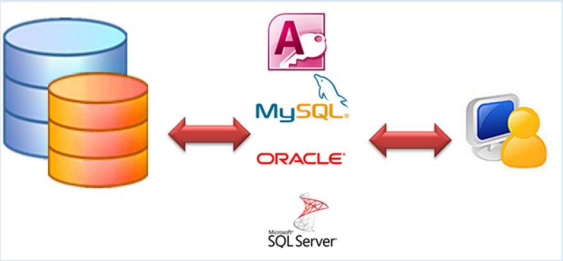
Implementación Seguridad de TI sin previo análisis de riesgos de TI. Planes y ppto. de Seguridad no tiene sustento, consecuentemente no se logra implementar seguridad donde realmente debe mitigarse (Riesgos Altos y medios). No se Gestiona el Riesgo de TI de acuerdo al REGLAMENTO. *(13 Gestión de Riesgos Tecnológicos ,15 Metod. para la Gestión de Riesgos de TI)*

Proyectos de Seguridad de TI no implementados o dejados a medias por no apoyarse en los Consultores Externos en el proceso de implementación (vinculado al contrato).

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

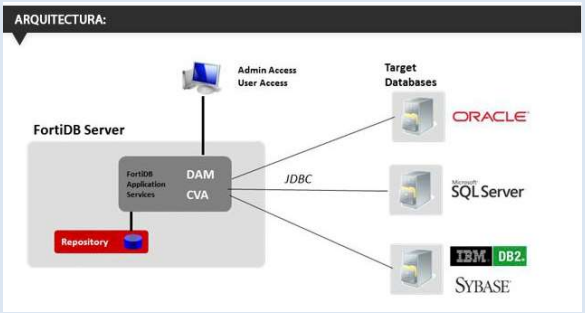
- El Área de Seguridad de TI no se entera cuando Personal de TI (DB) cambia algún control, usuarios o se modifica data directamente en la DB vía SQL.
- En BD (ORACLE, SQL Server), existen usuarios con ROL DBA ó SYSADMIN a parte del (DBA), máximo "privilegio" que no les corresponde, que podrían afectar la integridad y disponibilidad del Sistema. *(24 Gestión de Accesos de los Colaboradores, 26e retención de las pistas de auditoría será de por lo menos 180 días)*

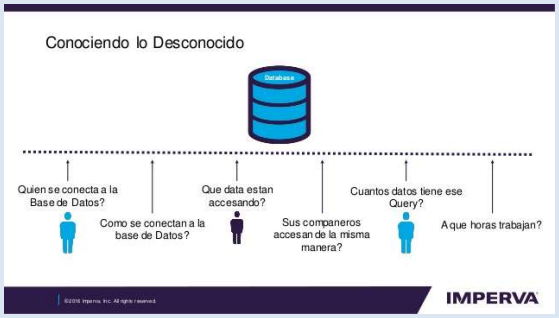


Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

- Organizaciones no implementaron de forma eficiente SW/HW de **Monitoreo de Base de Datos** y de Monitoreo de Redes, que notifique y alerte OPORTUNAMENTE cualquier cambio no autorizado o incidente de seguridad. *(30 Gestión de Vulnerabilidades y Amenazas Tecnológicas, e) Monitoreo de los Sistemas y la Infraestructura Tecnológica).*

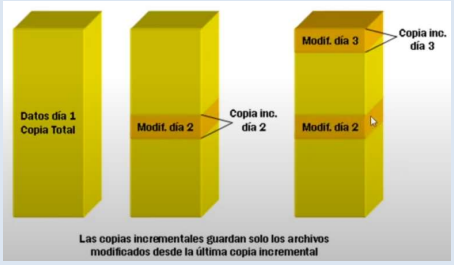


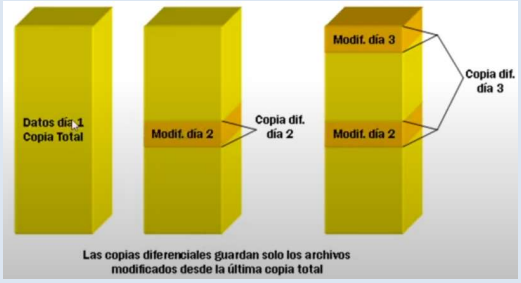


Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

- No se colectan LOGs de Infraestructura Tecnológica importante y no se cumplen tiempos de retención (3 años). (*30. Gestión de Vulnerabilidades y Amenazas Tecnológicas d) Registro de Eventos de Seguridad Cibernética*)
- Los BACKUPS en servidores están conectados a la red interna y en línea y no se guarda el tiempo que se establece en el Reglamento (1 año) (Riesgo ransomware) y además no están cifrados. (*30 "e) Copias de Resguardo y su Retención*).

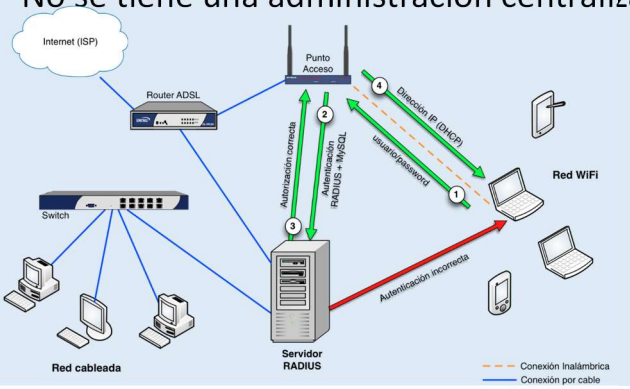


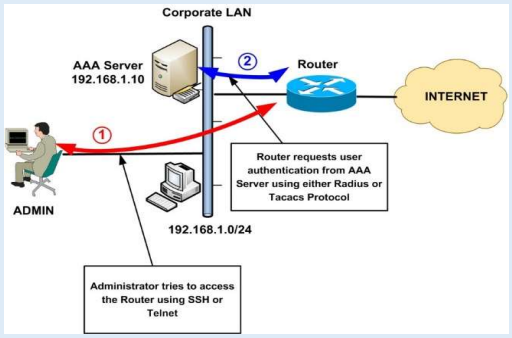


Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

- Dispositivos de redes y comunicaciones (Ej. switch, routers) configurados con debilidades de seguridad importantes y con diferentes políticas. (*28 Gestión de la Red inciso a) Configuración de Dispositivos de Red, evitar cambios no autorizados.*)
- No se tiene una administración centralizada de los dispositivos de red.

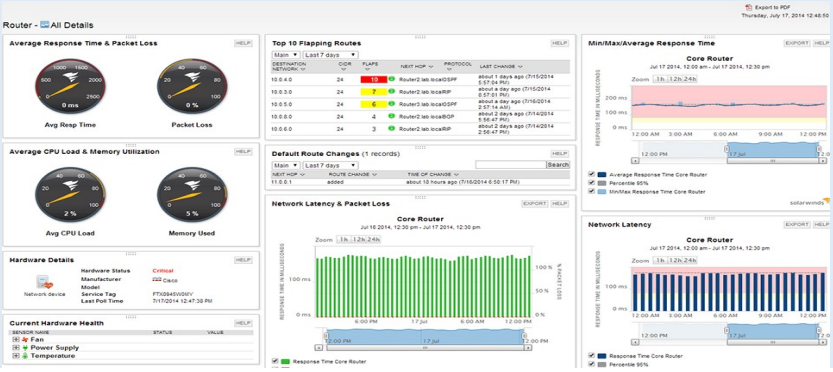




Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

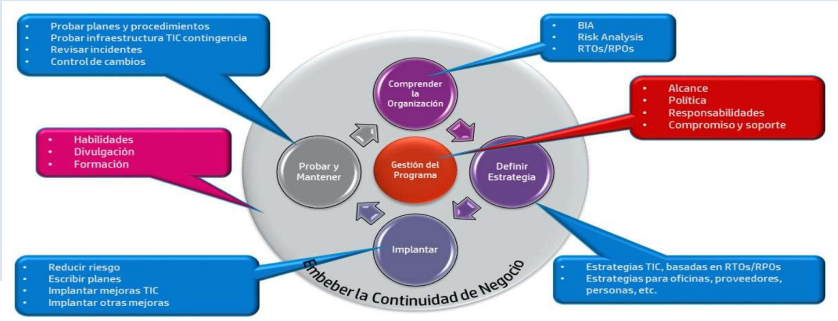
- El monitoreo de los equipos de Red y Comunicaciones no es de forma preventiva, es reactiva.
- La detección de eventos o incidentes de seguridad NO ES TEMPRANA, debido a la ausencia de software de monitoreo.



Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

INCUMPLIMIENTOS Y HALLAZGOS COMUNES

- Planes de Continuidad (BCP) y Recuperación (DRP) no acorde a estándares y no probados.(*40. Continuidad de las Operaciones Tecnológicas*)
- Análisis de Impacto del Negocio (BIA) no desarrollado que determine la IT necesaria para Site y Replicación. (*e) Planes de Recuperación ante Desastres*)
- Site Alterno/Contingencia que no realizan pruebas periódicas. (*f) Pruebas de Estrés: ..deben ser ejecutadas en intervalos de períodos no mayores a 1 (un) año*)



Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

- ✓ Fortalecer Áreas de TI, Seguridad de la Información, Riesgos y Auditoria Interna en las Organizaciones.
- ✓ Realizar Análisis de Riesgos de TI para Planificar y elaborar ppto de seguridad.
- ✓ Implementar Seguridad con expertos.
- ✓ Implementar IT de monitoreo oportuno.
- ✓ Aplicar mejores prácticas de Seguridad de TI (marcos y estándares).
- ✓ Implementar Seguridad de TI en las diferentes capas.
- ✓ Cumplir las recomendaciones de Auditoría y Consultores.

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana

23 CONGRESO NACIONAL DE SEGURIDAD

Muchas Gracias!!

Wilson Andia Cuiza, CISA, CRISC, CSXF, CDPSE, 27001LA
DIRECTOR DE AUDITORÍAS DE TI, PKF Dominicana
Accredited Trainer CISA y CRISC ISACA, APMG

Consultor Internacional en Auditoria, Riesgos y Seguridad de TI - PKF Dominicana

auditoriaTI@gmail.com

@wilson_andia

Fecha: agosto 2023