Webinar Series
Retos Ciberseguridad 2025

DFK – González y Asociados es una entidad legal autónoma e independiente que forma parte de DFK International, con una red de 24 oficinas en México y presencia en 90 países.

DFK INTERNATIONAL

Panorama de los riesgos de ciberseguridad

Las organizaciones han iniciado esfuerzos para proteger su información. ¿Por qué la ciberseguridad sigue siendo un ámbito muy importante en los negocios?

El panorama de riesgos de ciberseguridad sigue evolucionando, incluyendo el incremento en:

Complejidad y diversidad de grupos atacantes

Leyes y regulaciones

Tecnologías emergentes

Esta evolución en el panorama de amenazas de ciberseguridad obliga a las organizaciones a mantener evaluaciones continuas, auditorías y a estar alertas para gestionar de manera eficiente los riesgos de ciberseguridad, esto intensifica la necesidad de mantener un dialogo estratégico a lo largo de la organización para un mejor entendimiento y concientización de los riesgos.

Agenda

Introducción

¿Por qué los riesgos de ciberseguridad son importantes para las organizaciones?

Comunicación entorno a la ciberseguridad

Tendencias en ciberseguridad

Análisis de casos de ataques de ciberseguridad

Q&A

Riesgos de ciberseguridad y su organización

¿Que grupos de atacantes, métodos de ataque, leyes y regulaciones, tecnologías emergentes son aplicables a su organización?

- Naciones, organizaciones criminales
- SOX, GDPR, LFPDPP
- Cloud, Internet of Things, AI

¿Que pasaría a su negocio si los riesgos asociados a los puntos identificados previamente no son adecuadamente gestionados?

- Reputacionales
- Financieros
- Operacionales

¿Por qué los riesgos de ciberseguridad son importantes para las organizaciones?

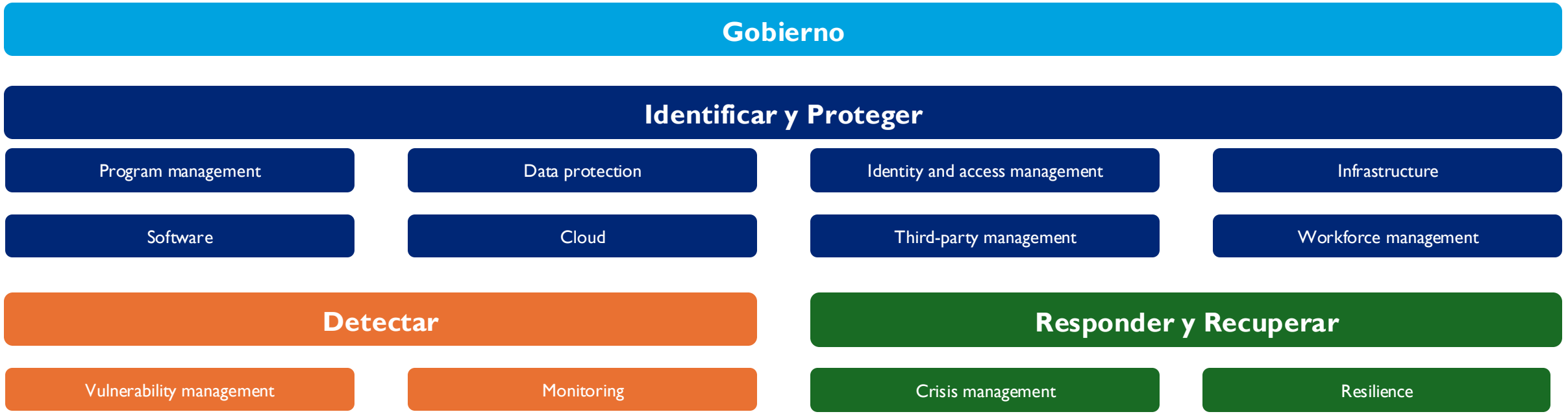
Impactos potenciales por brechas de ciberseguridad o fallas en controles de ciberseguridad

- Reputacionales
- Financieros
- Operacionales

¿Cómo habilitar la comunicación de ciberseguridad en una organización?

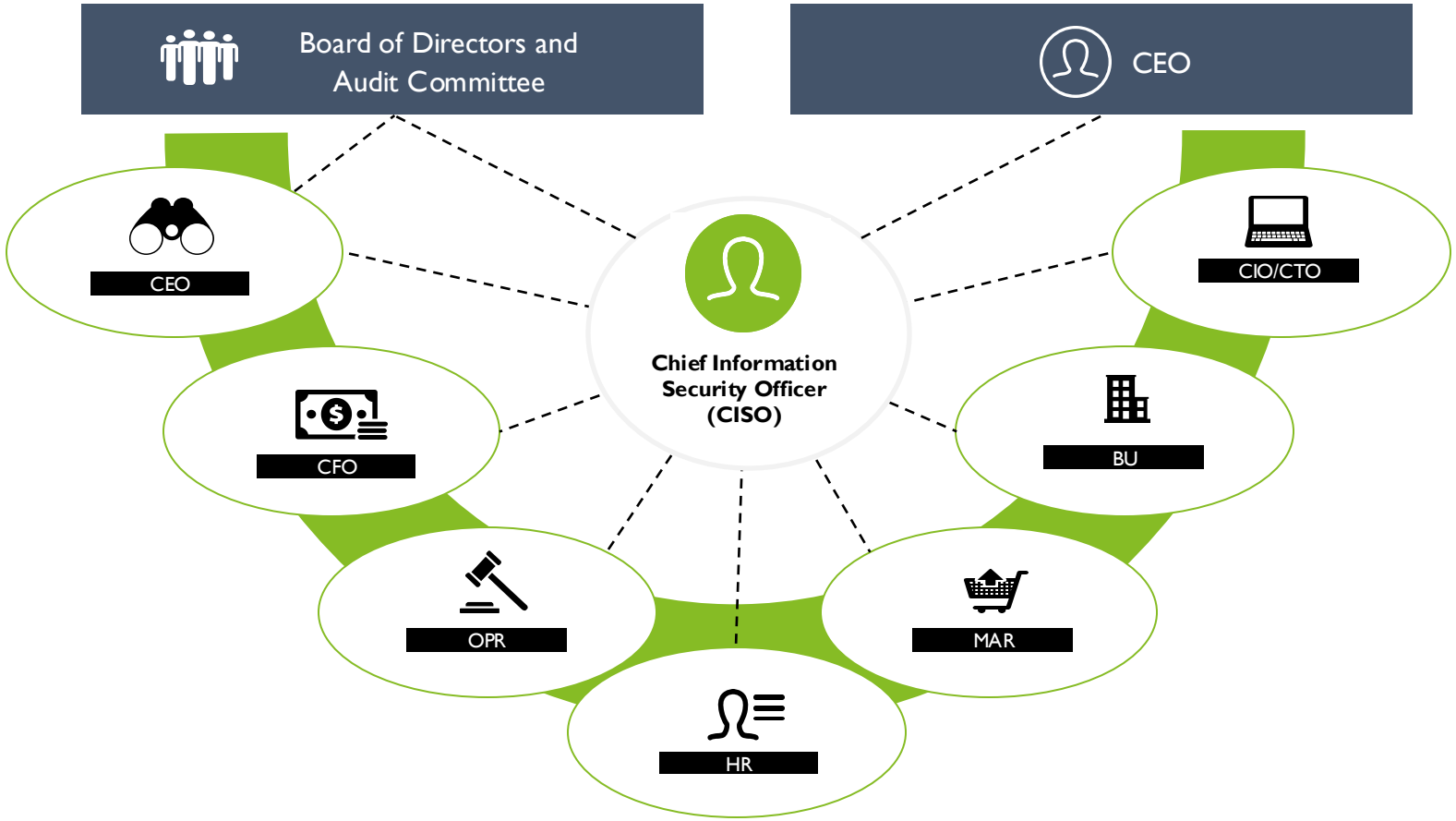
Comunicación entorno a ciberseguridad: cyber security framework

Un framework de ciberseguridad puede ayudar en esta tarea de habilitar la comunicación de ciberseguridad en la organización.



Líneas de comunicación – CISO

Las líneas en este slide no corresponden a niveles jerárquicos, en realidad representan canales de comunicación entre el responsable del programa de ciberseguridad de la organización y el senior management del negocio.



¿Cuáles son las tendencias de ciberseguridad en 2025?

Tendencias en Ciberseguridad

¿Qué dicen los expertos?

- Las amenazas digitales evolucionan constantemente. Para entender cómo protegernos, debemos conocer lo que indican algunas organizaciones independientes sobre estas tendencias.

  - Foro Económico Mundial (WEF)
  - NIST (EE.UU.)
  - Centro Canadiense de Ciberseguridad
  - OCC (EE.UU. - Regulador financiero)

WORLD ECONOMIC FORUM

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Canadian Centre for Cyber Security

Office of the Comptroller of the Currency

Tendencias en Ciberseguridad

Riesgo Cibernético como Amenaza Global (WEF)

91% de los líderes creen que un ciberataque significativo ocurrirá en 2 años.

Uso de IA por atacantes para automatizar fraudes.

Brecha entre líderes de negocio y equipos de seguridad.

→**Necesitamos traducir el riesgo cibernético al lenguaje del negocio.**

Tendencias en Ciberseguridad

Nuevo Gobierno Digital (NIST CSF 2.0)

Se refuerza la gobernanza como eje central del marco.

Énfasis en mejora continua y madurez.

Gestión de proveedores como riesgo clave.

→ **La ciberseguridad debe ser parte del gobierno corporativo, no solo de TI.**

Tendencias en Ciberseguridad

IA maliciosa y amenazas estatales (CCCS)

Canadian Centre for Cyber Security

- Actores estatales aprovechan IA para lanzar ataques avanzados.
- Deepfakes y malware personalizado al alza.
- Riesgo creciente para sectores profesionales y servicios financieros.

→ **Requiere monitoreo continuo y análisis de amenazas dirigidas.**

Tendencias en Ciberseguridad

Resiliencia y cumplimiento financiero (OCC)

Office of the Comptroller of the Currency

La ciberseguridad se evalúa como parte de la continuidad operativa.

Pruebas de recuperación ante incidentes.

Mayor escrutinio sobre terceros y servicios en la nube.

→ **La resiliencia ya no es opcional, es requisito de negocio.**

Tendencias en Ciberseguridad

Resumen de Tendencias Clave 2025

1. IA y amenazas avanzadas
2. Gobierno y control del riesgo digital
3. Actores sofisticados y geopolítica
4. Resiliencia y cumplimiento normativo

→ Las amenazas evolucionan. Nuestra defensa también debe hacerlo.

- **Las tendencias globales nos muestran que el riesgo es real, creciente y estratégico.**
- **Ahora más que nunca, debemos pasar del conocimiento a la acción**

Casos reales de brechas de ciberseguridad

Análisis de Ataques de Ciberseguridad

Perfil organización
Sector: Consumo productos de energía

Brecha
Febrero 2024
Método: Ransomware
Alcance: Encriptación de servidores, incluyendo servidores donde residía su ERP

Impactos
Operacionales y Financieros
La compañía no estuvo en posibilidad de operar por la ausencia de su sistema ERP, impidiendo entregar sus productos, afectando ingresos y los costos que implicó el análisis forense

Causa - raíz
Procesos de gestión de cuentas administradoras deficientes y falta de concientización de aseguramiento de cuentas privilegiadas

Análisis de Ataques de Ciberseguridad

Perfil organización
Sector: Health Tech

Brecha
Octubre 2023
Método: Credential stuffing
Alcance: Reúso de contraseñas para capturar 14,000 cuentas de usuarios

Impactos
Reputacionales
Exposición de datos personales y de salud de 5.5 millones de personas.

Causa - raíz
Falta de uso de contraseñas seguras, métodos de autenticación multifactor

Análisis de Ataques de Ciberseguridad

Perfil organización
Sector: Software

Brecha
Mayo 2023
Método: zero-day SQL injection vulnerability
Alcance: Extracción de datos y base de datos de aplicación

Impactos
Reputacionales
Exposición de datos afectando a 2,700 organizaciones que usaban la aplicación

Causa - raíz
Procesos de análisis de vulnerabilidades deficientes y falta de control en procesos de actualización de parches

Q&A

Servicios de Aseguramiento de Riesgos de TI y Ciberseguridad

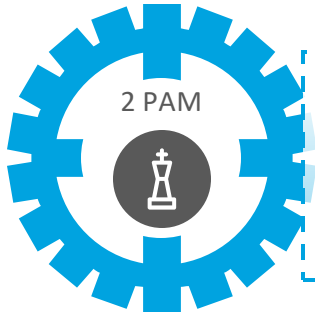
Operaciones seguras en aplicaciones empresariales que apoyen a las organizaciones a alcanzar sus objetivos de negocio, de seguridad de la información y de cumplimiento normativo

Combinamos experiencia e innovación para ayudar a las organizaciones a estar preparadas para el futuro, apoyándolas en la definición y mantenimiento de un modelo efectivo de seguridad en aplicaciones. Nuestro enfoque incorpora buenas prácticas de industria y marcos globales de trabajo para ayudar a las organizaciones a navegar en un panorama de TI complejo y en constante evolución.

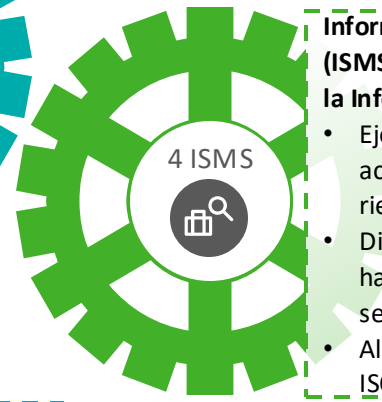
Plataformas Tecnológicas Seguras = **Seguridad** / **Cumplimiento**

User and Access Management (UAM)
- Controles en el ciclo de vida de accesos de usuarios
- Gobierno de accesos
- Diseño y gestión de procesos de certificación

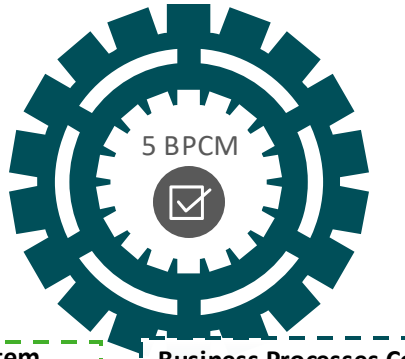
Segregation of Duties (SOD) – Segregación de Funciones
- Evaluación del modelo de gestión de conflictos de segregación de funciones.
- Evaluación de la situación de conflictos de segregación de funciones y de alternativas de remediación y mitigación
- Evaluación de las reglas de conflictos de segregación de funciones.



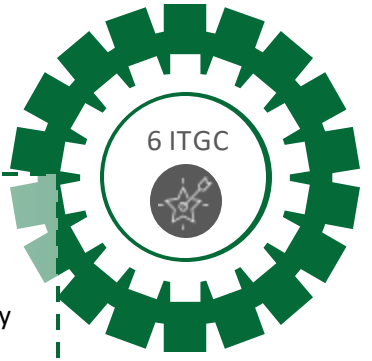
Privileged Access Management (PAM)
- Diseño de los procesos de asignación de accesos de emergencia
- Evaluación de logs y mejoras en la revisión y gestión.



Information Security Management System (ISMS) – Sistema de Gestión de Seguridad de la Información
- Ejecución de risk assessment y acompañamiento en el tratamiento de los riesgos
- Diseño de los procesos de seguridad y habilitación del Sistema de gestión de seguridad de la información
- Alineación a marcos globales como ISO27001, NIST, COBIT, CIS



Business Processes Control Management – Gestión de Controles en Procesos de Negocio
- Identificación y racionalización de controles en los procesos de negocio
- Evaluación periódica de los controles
- Controles de migración de datos en implementación de nuevos sistemas



IT General Controls – Controles Generales de TI
- Evaluación del diseño de los controles generales de tecnología
- Pruebas de implementación y efectividad de los controles
- Alineación de los controles generales de TI a buenas prácticas y requerimientos de cumplimiento

DFK INTERNATIONAL | GONZÁLEZ Y ASOCIADOS
AUDIT - TAX - CONSULTING

Salomón Rico
Socio Information Technology Risk
salomon.rico@gyg.com.mx

"Ampliamos sus oportunidades de negocio"

Síguenos en nuestras redes sociales:

www.gyg.com.mx

Association of the Year Winner 2015 International Accounting Bulletin

Rising Star Association of the Year Winner 2020 International Accounting Bulletin

Río Mississippi 303 Ote., Col. Del Valle, San Pedro Garza García, N.L. 66220 Tel. (81)1340-3500