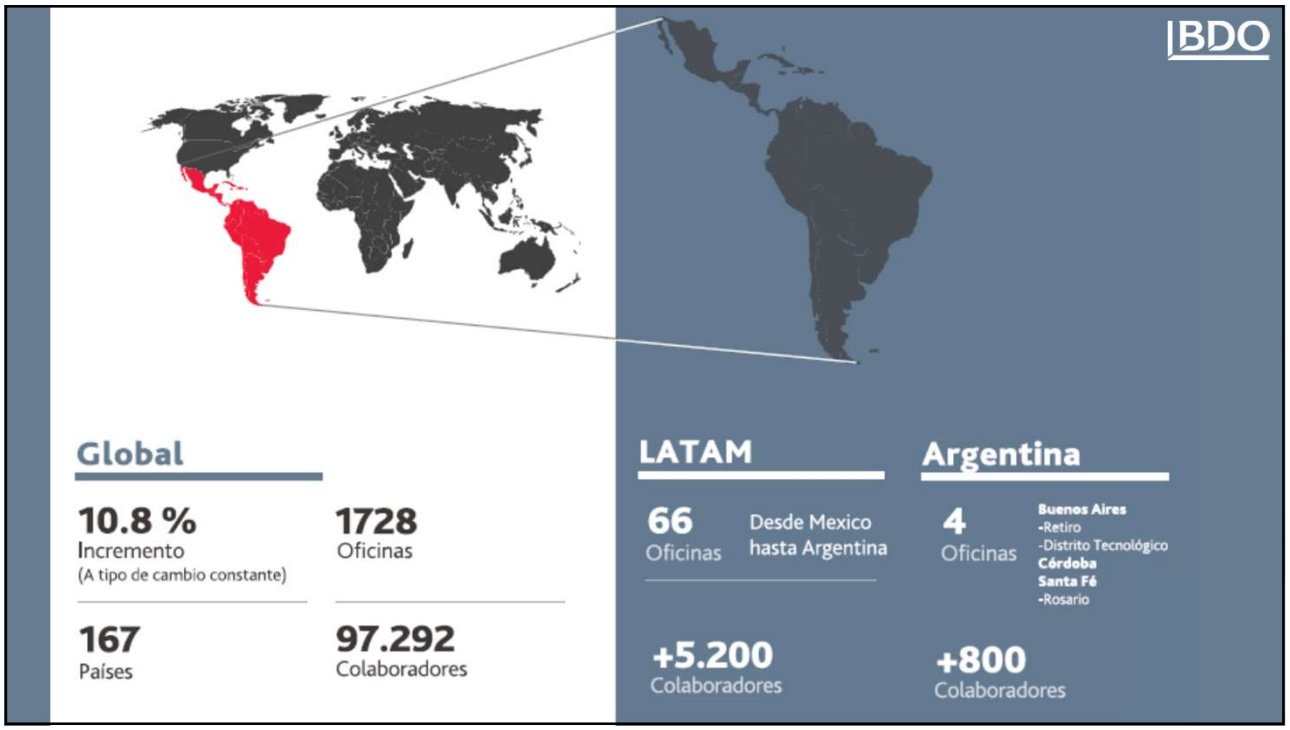

BDO
CFOs
MEETING
2023
Cross
Industria
ENTENDIENDO LA SEGURIDAD
PARA LA TOMA DE DECISIONES
API | Aseguramiento de Procesos Informáticos
RAS | Risk Advisory Services | IT Assurance, Audit and Compliance

1


BDO
Global
10.8 %
Incremento
(A tipo de cambio constante)
1728
Oficinas
167
Países
97.292
Colaboradores
LATAM
66
Oficinas
Desde Mexico
hasta Argentina
+5.200
Colaboradores
Argentina
4
Oficinas
Buenos Aires
-Retiro
-Distrito Tecnológico
Córdoba
Santa Fé
-Rosario
+800
Colaboradores

2

API | Aseguramiento de Procesos Informáticos

RAS | Risk Advisory Services | IT Assurance, Audit and Compliance

Fabián Descalzo (fdescalzo@bdoargentina.com)

Socio y DPO de BDO en Argentina del Departamento de Aseguramiento de Procesos Informáticos (API). Posee 30 años de experiencia en el área de gestión e implementación de Gobierno de Seguridad de la Información, Gobierno de TI, Compliance y Auditoría de TI en Argentina y Latinoamérica, y asesoramiento para el cumplimiento de Leyes y Normativas Nacionales e Internacionales en compañías de primer nivel de diferentes áreas de negocio. Docente del Diplomado Universitario en Accounting Tech en la Universidad Argentina de la Empresa - UADE del módulo BIG DATA Y SERVICIOS EN LA NUBE, Docente del módulo 27001 de las Diplomaturas de "IT Governance, Uso eficiente de Frameworks" y "Gobierno y Gestión de Servicios de TI" del Instituto Tecnológico Buenos Aires (ITBA), Docente del Módulo de Auditoría de IT de la Diplomatura en Delitos Informáticos para EDI en la Universidad Nacional de Río Negro y Docente en Sistemas de Gestión IT, Seguridad de la Información y Auditoría IT para TÜV Rheinland. Miembro del Comité Directivo de ISACA Buenos Aires Chapter, Miembro del Comité Directivo del "Cyber Security for Critical Assets LATAM" para Qatalys Global sección Infraestructura Crítica, Miembro del Comité Científico del IEEE (Institute of Electrical and Electronics Engineers)

Laura Dangelo (ldangelo@bdoargentina.com)

Directora de BDO en Argentina del Departamento de Aseguramiento de Procesos Informáticos (API). Posee más de 20 años de experiencia en el área de gobierno tecnológico y ciberseguridad, con especialización en el gerenciamiento de proyectos para el Gobierno de IT, Ciberseguridad, Riesgos y Cumplimiento en la prestación de servicios tecnológicos y de seguridad de la información. Con experiencia en liderazgo y coordinación de proyectos tecnológicos, infraestructura tecnológica y reingeniería de procesos. Especialista en Tecnologías de Bases de Datos. Es Auditor Interno de Sistema de Gestión de Continuidad del Negocio según ISO 22301:2019 y Auditor Interno de Sistemas de Gestión de Seguridad de la Información ISO 27001:2013

BDO

3

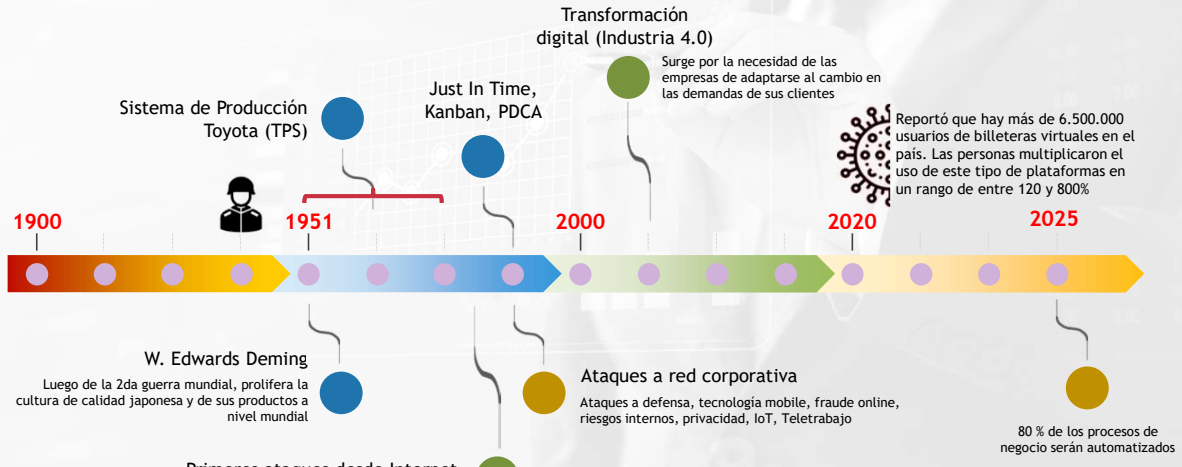
"LOS DIRECTORES DEBEN COMPRENDER Y ABORDAR LA CIBERSEGURIDAD COMO UN RIESGO ESTRATÉGICO Y EMPRESARIAL, NO SOLO COMO UN RIESGO DE TI"

BDO

4

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones



PREVIO A LA PANDEMIA, GARTNER ESTIMABA QUE EN 2020 EL 60% DE LOS NEGOCIOS DIGITALES SUFRIRÁN GRANDES FALLOS DE SEGURIDAD

BDO

5

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

EL 60% DEL CRECIMIENTO ECONÓMICO ESTÁ SIENDO IMPULSADO POR LAS TECNOLOGÍAS DIGITALES (FORO ECONÓMICO MUNDIAL)

IMPACTO DEL USO DE LA TECNOLOGÍA EN EL NEGOCIO Y SU REGULACIÓN (LA CAUSA MÁS COMÚN DE FILTRACIÓN DE DATOS ES EL ROBO DE CREDENCIALES DE USUARIO)

LA OBSOLECIANCIA TECNOLÓGICA Y LA NECESIDAD DE INNOVACIÓN ESTÁ AMPLIANDO LA BRECHA DE SEGURIDAD SUMANDO EL CUMPLIMIENTO COMO UNO DE SUS FACTORES DE RIESGO

BDO

6

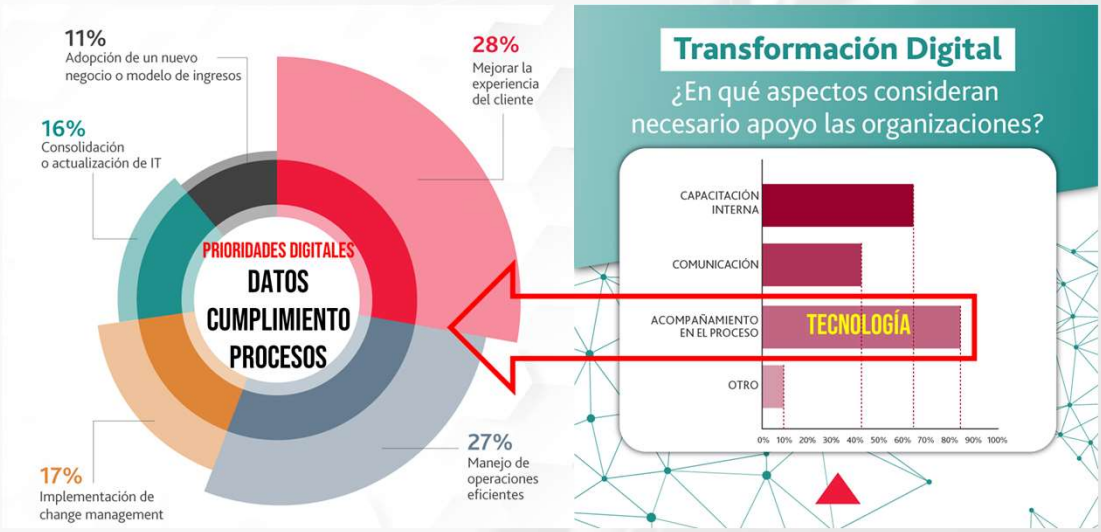
CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

7

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones



8

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

9

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

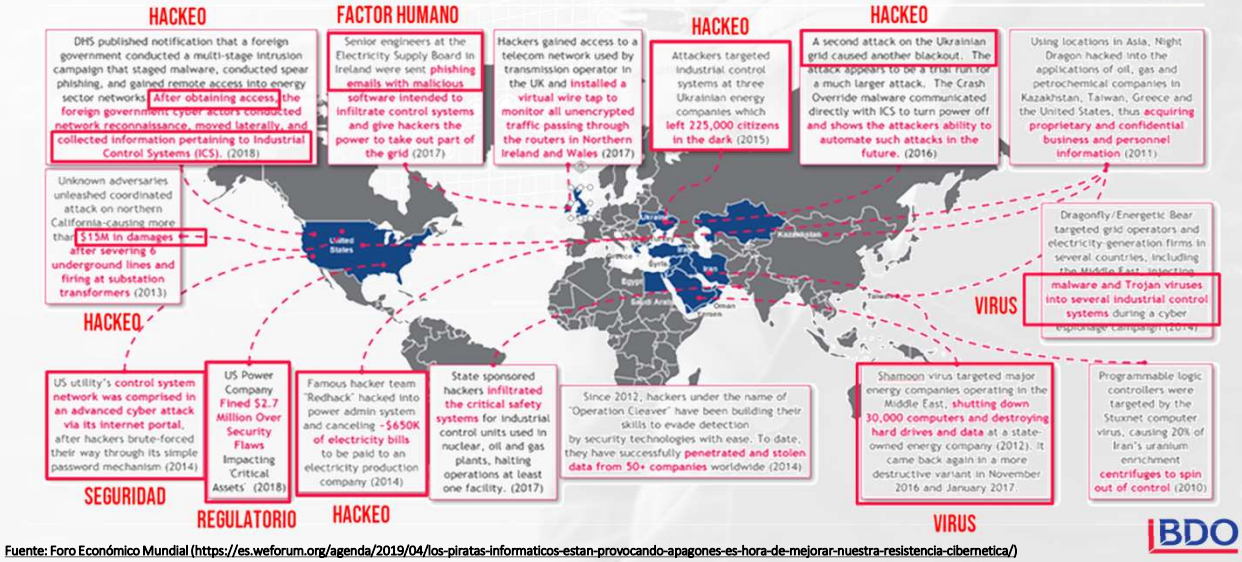
10

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

Many attacks on energy industry, various methods, serious consequences

(Selection)



Fuente: Foro Económico Mundial (https://es.weforum.org/agenda/2019/04/los-piratas-informaticos-estan-provocando-apagones-es-hora-de-mejorar-nuestra-resistencia-cibernetica/)

11

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

ZERO TRUST - ÉXITO A TRAVÉS DE LA TRANSPARENCIA Y LA CONFIANZA

Fuente: WORLD ECONOMIC FORUM

12

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

OTRAS MEDIDAS: IMPORTANCIA DE LOS TERCEROS

Acuerdos de niveles de servicio

- Interrupción del servicio
- Violación de contrato
- Tiempos establecidos de respuesta a incidentes
- Reporting
- Resolución de disputas
- Intervención de terceros
- Renovación de contrato

Gestión

- Implementaciones de software
- Backups y restauraciones
- Infraestructura tecnológica de contingencia
- Normativa regulatoria de los procesos
- Capacitación continua
- Escalabilidad y actualización de la infraestructura

Cláusulas de protección

- Protección de la propiedad
  - Intelectual
  - Industrial
  - Soluciones computadorizadas que integran procesos propietarios
  - Bancos de datos de clientes
- Cláusulas de confidencialidad y no revelación
- Acuerdos de no competencia
- Cláusulas de auditabilidad
- Alteración de información

Acceso a la información

- Alteración de la información
- Violación de la confidencialidad

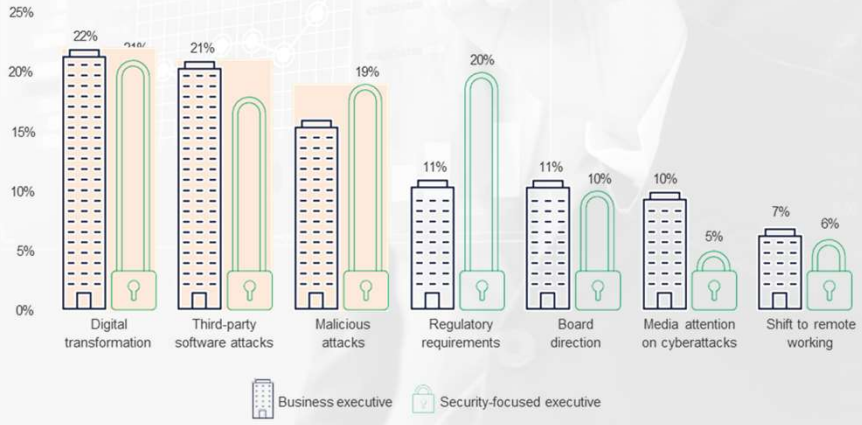
BDO

13

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

Los ejecutivos centrados en el negocio y la seguridad están alineados en lo que creen que tendrá la mayor influencia en el enfoque de ciberseguridad de su organización el próximo año.



Fuente: Global Cybersecurity Outlook 2022 WORLD ECONOMIC FORUM

BDO

14

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

PREGUNTAS DE REFERENCIA QUE LA DIRECCIÓN PUEDE HACERSE SOBRE RIESGOS DE CIBERSEGURIDAD

- ¿Estamos considerando los aspectos de ciberseguridad de nuestras principales decisiones comerciales, como fusiones y adquisiciones, asociaciones, lanzamientos de nuevos productos, etc., de manera oportuna?
- ¿Controlamos adecuadamente en aspectos de ciberseguridad a proveedores críticos del negocio?
- ¿Cuáles nuestros activos más valiosos?
- ¿Cómo interactúa nuestro sistema de TI contra esos activos?
- ¿Qué se necesitaría para sentirse seguro de que esos activos están protegidos?

BDO

15

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

PLANIFICACIÓN ESTRATÉGICA Y GRADO DE INNOVACIÓN

TECNOLOGÍA

Grado de innovación en el desarrollo tecnológico (tecnologías y procesos de producción)

ENTORNO

Grado de innovación en lo requerido para el crecimiento del negocio

GESTIÓN

Grado de innovación necesaria en la gestión para el desarrollo del negocio

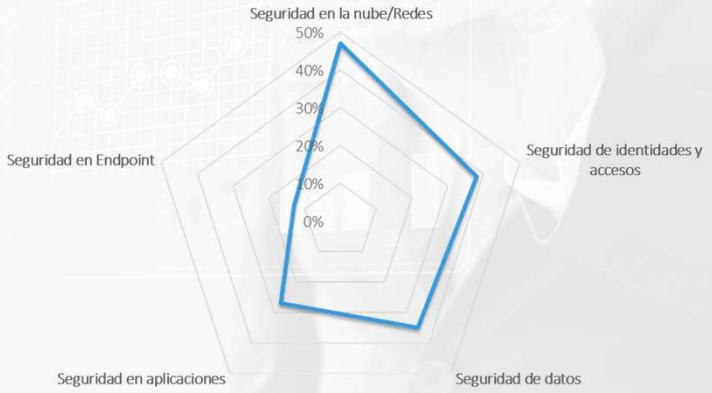
BDO

16

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

FOCOS DE ATENCIÓN EN EL PROGRAMA DE CONTROL DE CIBERSEGURIDAD



Source: Heidrick & Struggles' global chief information security officer (CISO) survey, 2021, n = 354 information security professionals
Note: Respondents may have chosen more than one focus area.

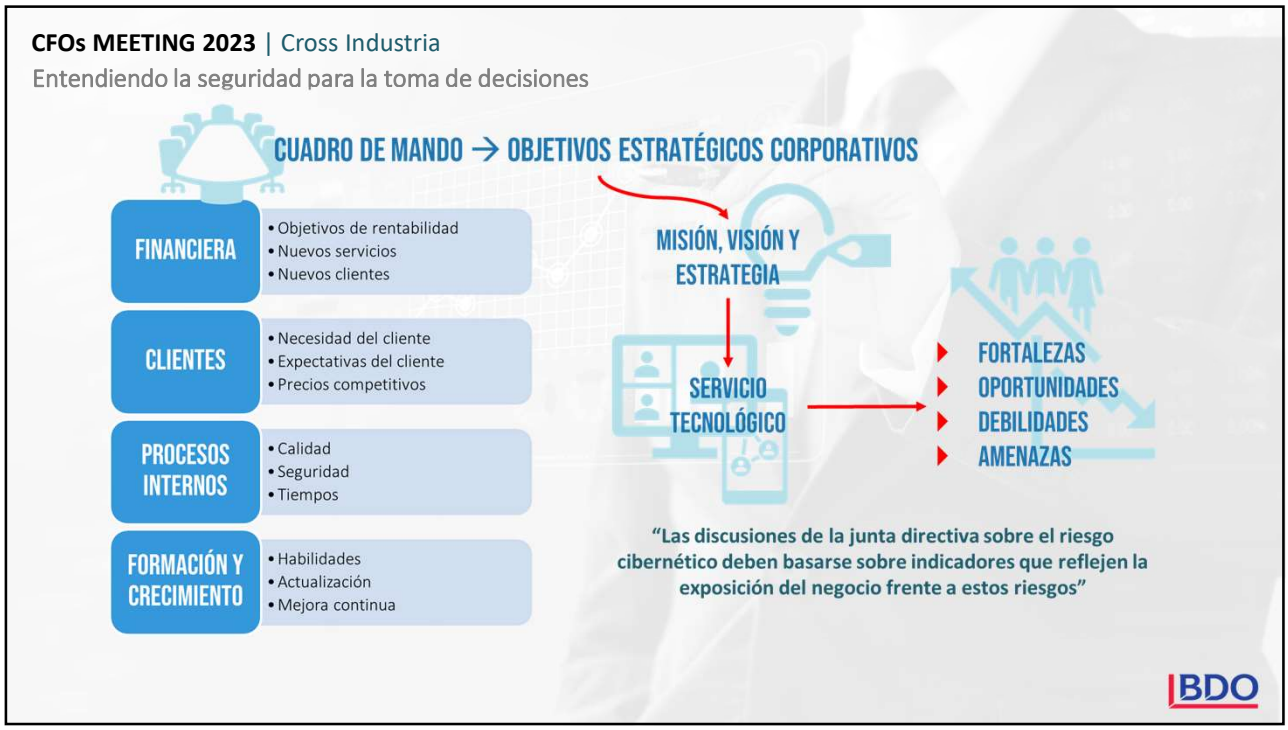
17

CFOs MEETING 2023 | Cross Industria

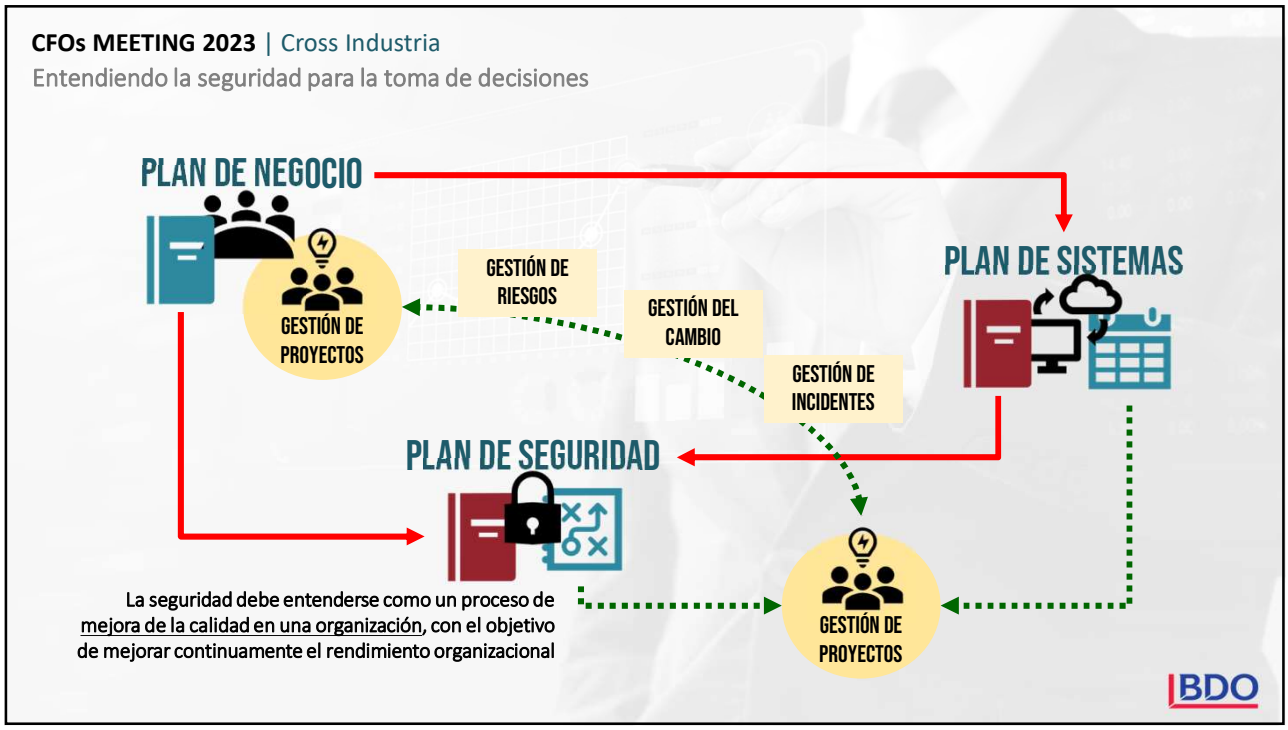
Entendiendo la seguridad para la toma de decisiones

ISO 27032 Gestión de ciberseguridad; ISO 27701 Privacidad; ISO 27031 Continuidad de negocios de las TICs; Estándares del NIST (800-53); OWASP; SOC 2; ENS y guías del CCN-CERT

18


CFOs MEETING 2023 | Cross Industria
Entendiendo la seguridad para la toma de decisiones
CUADRO DE MANDO → OBJETIVOS ESTRATÉGICOS CORPORATIVOS
FINANCIERA
• Objetivos de rentabilidad
• Nuevos servicios
• Nuevos clientes
CLIENTES
• Necesidad del cliente
• Expectativas del cliente
• Precios competitivos
PROCESOS INTERNOS
• Calidad
• Seguridad
• Tiempos
FORMACIÓN Y CRECIMIENTO
• Habilidades
• Actualización
• Mejora continua
MISIÓN, VISIÓN Y ESTRATEGIA
SERVICIO TECNOLÓGICO
FORTALEZAS
OPORTUNIDADES
DEBILIDADES
AMENAZAS
"Las discusiones de la junta directiva sobre el riesgo cibernético deben basarse sobre indicadores que reflejen la exposición del negocio frente a estos riesgos"
BDO

19


CFOs MEETING 2023 | Cross Industria
Entendiendo la seguridad para la toma de decisiones
PLAN DE NEGOCIO
GESTIÓN DE PROYECTOS
GESTIÓN DE RIESGOS
GESTIÓN DEL CAMBIO
GESTIÓN DE INCIDENTES
PLAN DE SISTEMAS
PLAN DE SEGURIDAD
GESTIÓN DE PROYECTOS
La seguridad debe entenderse como un proceso de mejora de la calidad en una organización, con el objetivo de mejorar continuamente el rendimiento organizacional
BDO

20

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

EL ESTABLECIMIENTO DE UN SISTEMA DE GESTIÓN DE LA CALIDAD ES ESENCIAL PARA QUE UNA EMPRESA PUEDA DESARROLLAR SU ACTIVIDAD CON ÉXITO, PERO LA CIBERSEGURIDAD ES LA PRIORIDAD Y DEBE SER TRATADA ANTES

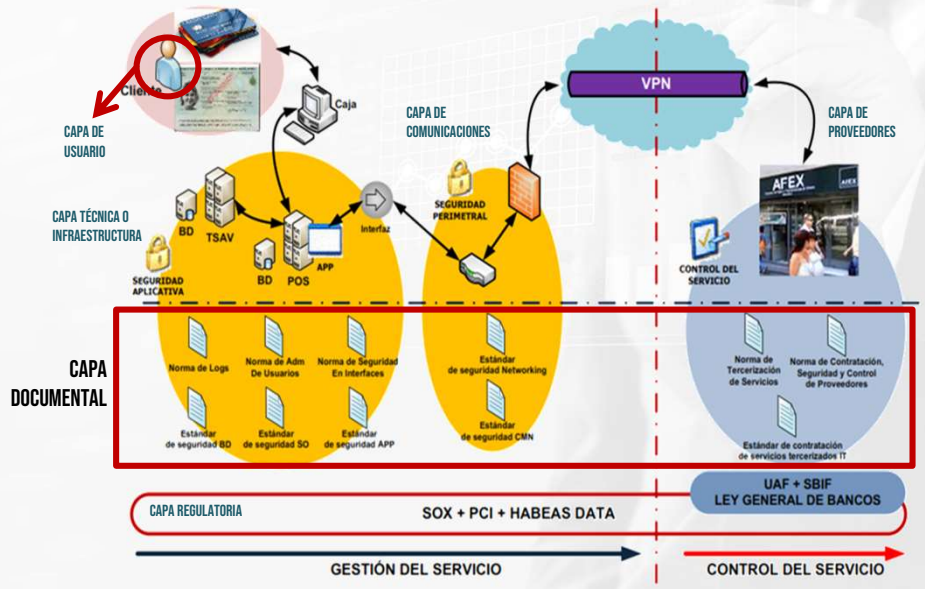
- Definiciones y ámbito de aplicación
- Proporcionalidad
- Gobernanza y mantenimiento de registros
- Fase previa a la externalización
- Acuerdos de subcontratación
- Seguridad de los datos
- Derechos de acceso, auditoría e información
- Subcontratación
- Respuesta a incidentes y planes de continuidad del negocio

BDO

21

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

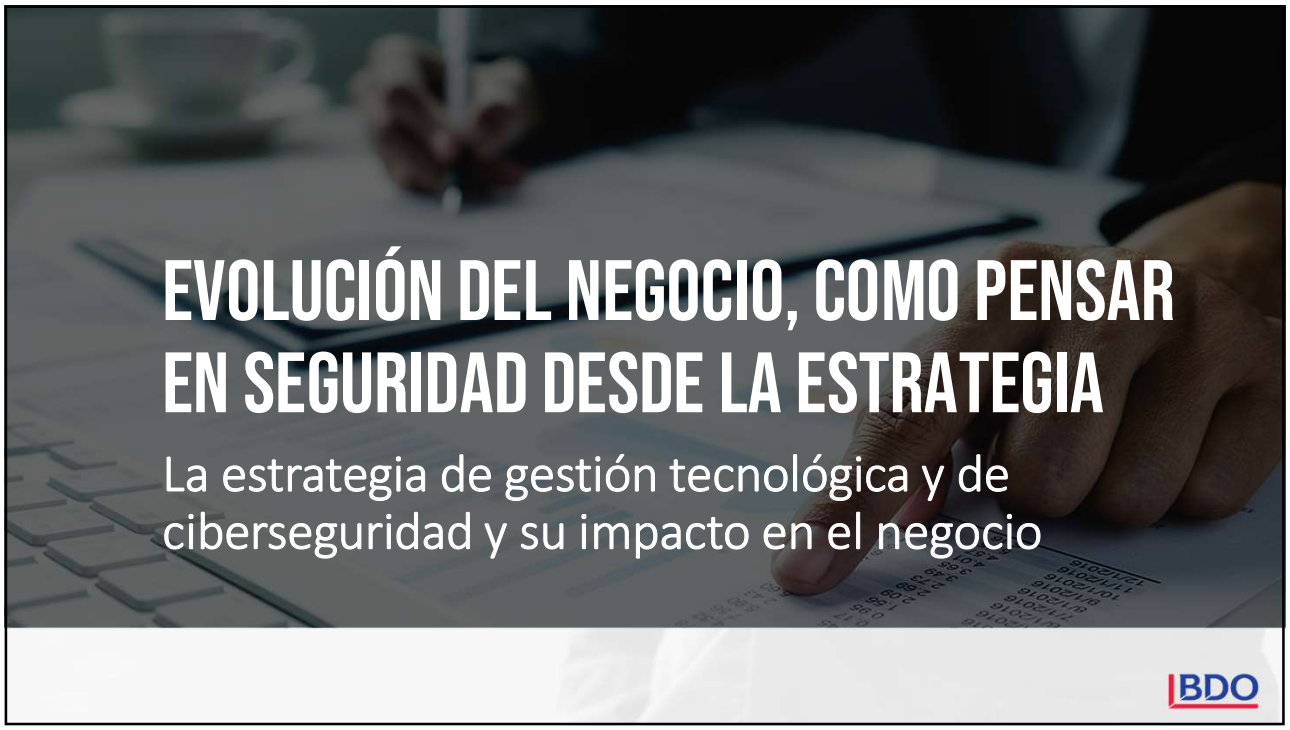


LA CIBERSEGURIDAD ¿POR QUÉ SE NECESITA MÁS QUE NUNCA?

PORQUE NECESITAMOS ENFOCARNOS EN UNA SEGURIDAD INTEGRAL

BDO

22


EVOLUCIÓN DEL NEGOCIO, COMO PENSAR EN SEGURIDAD DESDE LA ESTRATEGIA
La estrategia de gestión tecnológica y de ciberseguridad y su impacto en el negocio
BDO

23


"LOS DIRECTORES DEBEN COMPRENDER LAS IMPLICANCIAS DE LOS RIESGOS CIBERNÉTICOS EN RELACIÓN CON LAS CIRCUNSTANCIAS ESPECÍFICAS DE SU EMPRESA."
BDO

24

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

EL APETITO POR EL RIESGO ES UNA CUESTIÓN DE JUICIO BASADA EN LAS CIRCUNSTANCIAS ESPECÍFICAS DE CADA EMPRESA

Una discusión sobre el apetito por el riesgo debe abordar las siguientes preguntas:

- **Valores corporativos** ¿Qué riesgos no aceptaremos?
- **Estrategia** ¿Que riesgos que debemos asumir?
- **Partes interesadas** ¿Qué riesgos están dispuestos a asumir las partes interesadas y a qué nivel?
- **Capacidad** ¿Tengo los recursos que se requieren para gestionar esos riesgos?
- **Financiero** ¿Somos capaces de cuantificar adecuadamente la eficacia de nuestra gestión de riesgos y armonizar nuestro gasto en controles de riesgos?
- **Medición** ¿Estoy desarrollando informes sobre la base de mediciones que garanticen un monitoreo, tendencias y comunicación adecuados?

BDO

25

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

PRINCIPALES RIESGOS QUE AFECTARÁN A LAS ORGANIZACIONES (SIN IMPORTAR SU TAMAÑO) EN 2022

- **CIBERSEGURIDAD**: Organizaciones suficientemente preparadas para gestionar ciberamenazas que podrían causar interrupciones, daños a la reputación y daños económicos.
- **GOBIERNO ORGANIZACIONAL**: Si la gobernanza de las organizaciones ayuda o dificulta el logro de los objetivos.
- **PRIVACIDAD DE DATOS**: Cómo las organizaciones protegen los datos confidenciales bajo su cuidado y garantizan el cumplimiento de todas leyes y regulaciones aplicables.
- **CULTURA**: Si las organizaciones entienden, monitorear y administrar el tono, los incentivos y las acciones que impulsan el comportamiento deseado frente a la ciberseguridad y seguridad de la información.
- **CAMBIO EN EL ENTORNO REGULATORIO**: Los desafíos a los que se enfrentan las organizaciones en un entorno regulatorio dinámico y ambiguo.
- **GESTIÓN DE PROVEEDORES**: La capacidad de las organizaciones para seleccionar y monitorear las relaciones con terceros.
- **INNOVACIÓN DISRUPTIVA**: Si las organizaciones están preparadas para adaptarse y / o capitalizar la disrupción.
- **INTERRUPCIÓN DE LA CADENA DE SUMINISTRO**: Si las organizaciones han incorporado resiliencia para adaptarse a las interrupciones actuales y futuras de la cadena de suministro.

Fuente: The Institute of Internal Auditors (IIA) - The OnRisk 2022

BDO

26

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

LOS PRINCIPALES DESAFÍOS DE CIBERSEGURIDAD PARA LAS EMPRESAS Y COMO ENFRENTARLOS

- **Principio 1**: Los directores deben comprender y abordar la ciberseguridad como un problema de gestión de riesgos en toda la empresa, no solo como un problema de TI.
- **Principio 2**: Los directores deben entender las implicaciones legales de los riesgos cibernéticos según se relacionan con las circunstancias específicas de su empresa.
- **Principio 3**: Las juntas deben tener un acceso adecuado a la experiencia en ciberseguridad y se le debe proporcionar un tiempo regular y adecuado a las discusiones sobre la gestión de riesgos cibernéticos en las agendas de las reuniones de la junta.
- **Principio 4**: Los directores de la junta deben establecer la expectativa de que la gerencia establecerá un marco de gestión de riesgo cibernético para toda la empresa con personal y presupuesto adecuados.
- **Principio 5**: La discusión de la junta directiva sobre el riesgo cibernético debe incluir la gestión integral de riesgos, así como planes específicos asociados con cada abordaje para su mitigación.

Fuente: OEA - MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS 2022

BDO

27

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

CUADRO DE MANDOS

MEDICIÓN DE LA SEGURIDAD

METAS DE LA DIRECCIÓN

Objetivos estratégicos
- Cumplimiento de las metas

RIESGOS

Objetivos de reducción de riesgos
- Nivel de cumplimiento
- Valoración de resultado

TIEMPO

Evaluación del plan de tratamiento
- Grado de implementación
- Madurez de las medidas

BDO

28

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

ISO 27016
Gestión de la seguridad de información - Economía organizacional

ECONOMÍA DE LA SEGURIDAD PARA LA INNOVACIÓN
RENTABILIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

ISO 31000/31010
Directrices de implantación y técnicas de evaluación de riesgos

ISO 27002
Implementación de controles

ISO 27004
Gestión de la seguridad de la información - Medición

SGSI – ISO 27001
ISO/IEC 27005 | ISO/IEC 27035
Reducción y eliminación de incidentes de seguridad

BCP
Plan de Continuidad de Negocio (BIA)

Este tipo de estudios no es posible realizarlo **sin conocer de forma exhaustiva las amenazas** que afectan a una organización. Para realizarlo de la forma más precisa posible (siempre son estimaciones probabilísticas) debemos remontarnos a la historia reciente de la organización y ver **qué incidentes se han sufrido**, para así poder prever los posibles incidentes futuros y después calcular el **costo asociado a ellos**.

BDO

29

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

EVALUACIÓN CUANTITATIVA DEL RIESGO

EXPECTATIVA DE PÉRDIDA SIMPLE (SLE)

Cantidad esperada de dinero que se pierde cuando se produce un riesgo (costo total de un incidente)

→ Se trata de pérdidas directas (tiempo de inactividad del sitio web, reemplazo de hardware, reemplazo de la pérdida de datos, etc.) y el costo de los daños indirectos (tiempo de investigación, la pérdida de reputación, el impacto en la imagen, etc.)

FRECUENCIA ANUAL DEL RIESGO (ARO)

Medida de la probabilidad de que un riesgo se produce en un año

→
- La ARO de una inundación dependerá de factores geográficos
- La ARO de un fallo en el disco está influenciada por la temperatura de funcionamiento
- La ARO de un robo dependerá de la ubicación de la de activos, etc

EXPECTATIVA DE PERDIDA ANUAL (ALE)

Pérdida monetaria anual que se puede esperar de un riesgo específico sobre un activo específico

→ **ALE = ARO X SLE**

BDO

30

EL MODELO GORDON-LOEB

The Economics of Information Security Investment (2002)

El modelo Gordon-Loeb es un modelo económico matemático que analiza el nivel óptimo de inversión en seguridad de la información. Para redactar este modelo, la empresa debe poseer conocimiento de tres parámetros:

- Cuánto valen los datos (VA – Valor del activo);
- Cuánto están en riesgo los datos (FE – Factor de exposición);
- La probabilidad de que un ataque a los datos tenga éxito, o vulnerabilidad (ARO – Tasa de ocurrencia anualiazda)

Estos tres parámetros se multiplican para proporcionar la pérdida de dinero media sin inversión en seguridad. La cantidad de dinero que una empresa gasta en proteger la información debería ser solo una pequeña fracción de la pérdida prevista que según el modelo de Gordon y Loeb no supera el 37%.

- **Ejemplo:** Suponga un valor de datos estimado de **1.000.000 USD**, con una **probabilidad de ataque del 15%** y una **probabilidad del 80% de que un ataque tenga éxito**. En este caso, la pérdida potencial viene dada por el producto **1.000.000 USD × 0,15 × 0,8 = 120.000 USD**. Según Gordon y Loeb, la inversión de la empresa en seguridad no debería superar los **120.000 USD × 0,37 = 44.000 USD**.

31

CFOs MEETING 2023 | Cross Industria
Entendiendo la seguridad para la toma de decisiones

DEFINICIÓN DEL ALCANCE Y LOS ACTIVOS INVOLUCRADOS EN LA OPERACIÓN DEL PROCESO

INLCUIR EL COSTO DEL FACTOR HUMANO FRENTE A LA PÉRDIDA QUE PUEDE OCASIONARSE EN LA PÉRDIDA DE CONOCIMIENTO

Alcance	Activos	Valor	Porcentaje del valor total
Servicio de *hosting*	Servidor de aplicaciones	$ 17,000.00	3%
	Servidor de base de datos	$ 10,000.00	1%
	Conexión a Internet	$ 12,000.00	2%
	Intangibles	$ 15,000.00	2%
	Salarios	$ 25,000.00	4%
	Licencias	$ 100,000.00	15%
	Propiedad intelectual	$ 500,000.00	74%
	Costo total	**$ 679,000.00**	**100%**

SELECCIÓN DEL ACTIVO CRÍTICO

Activo		x 1h	x 24h	X Año
Servidor de aplicaciones	Ventas promedio	$100	$2,400	$876,000

IDENTIFICACIÓN DE AMENAZAS Y PROBABILIDAD DE OCURRENCIA

Amenazas	ARO
Infección por virus (1 vez cada 2 años)	50%
Falla eléctrica (1 veces cada 3 años)	33%
Factor humano intencional (1 vez cada 4 años)	25%
Factor humano no intencional (nunca)	0%

IDENTIFICACIÓN DEL FACTOR DE EXPOSICIÓN

Factor de exposición	Porcentaje
El sistema tiene redundancia o respaldos	30%
El sistema está detrás de un firewall de red	10%
El sistema cuenta con software antivirus instalado	10%
El sistema cuenta con las últimas actualizaciones instaladas	40%
El sistema cuenta con un firewall de host instalado	30%

32

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

Activo	Amenaza	VA	FE	ARO	ALE
Servidor de aplicaciones	Infección por virus (1 vez cada 2 años)	$ 17,000.00	20%	50%	$ 1,700.00

- VALOR DEL ACTIVO (VA): $17,000.00
- FACTOR DE EXPOSICIÓN (FE): 20% (PORCENTAJE DE PÉRDIDA DE ACTIVO CAUSADA POR LA AMENAZA)
- TASA ANUALIZADA DE OCURRENCIA (ARO): 50% (1 VEZ CADA DOS AÑOS)

BDO

33

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

MÉTRICA DE GESTIÓN DE RIESGOS CONOCIDA COMO ALE

Pérdida monetaria anual que se puede esperar de un riesgo específico sobre un activo específico

BDO

34

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

VALORES PARA ANÁLISIS DE ROSI		
Pérdidas anuales por incidentes sin tratar	$ 200.000,00	→ GESTIÓN DE INCIDENTES
Pérdidas anuales por incidentes mitigados	$ 50.000,00	→ GESTIÓN DE RIESGOS + PLAN
Ahorro bruto anual por controles	**$ 150.000,00**	
Costo inicial de implementación de controles	$ 120.000,00	→ GESTIÓN DE CONTROLES
Costos anuales operacionales de controles	$ 10.000,00	

CALCULO DE ROSI					
ROSI estimado a tres años		0	1	2	3
Ahorro bruto anual por controles			$ 150.000,00	$ 150.000,00	$ 150.000,00
Ahorro bruto anual por controles a valor actual (valor disminuye por acción de las medidas tomadas)			**$ 125.000,00**	**$ 104.166,67**	**$ 86.805,56**
Valor de controles (suma de ahorro anual a valor actual)	**$ 315.972,23**		$ 125.000,00	$ 229.166,67	**$ 315.972,23**
Costo inicial de controles		$ 120.000,00			
Costos anuales operacionales de controles			$ 10.000,00	$ 10.000,00	$ 10.000,00
Costo de controles a valor actual (valor disminuye por acción de las medidas tomadas)		**$ 120.000,00**	**$ 8.333,33**	**$ 6.944,44**	**$ 5.787,04**
Costo de controles (suma de controles a valor actual)	**$ 141.064,81**				
ROSI (%) = (VALOR - COSTO) / COSTO	**124%**	**-$ 120.000,00**	**$ 116.666,67**	**$ 97.222,23**	**$ 81.018,52**
Valor actual neto (VALOR - COSTO)	**$ 174.907,42**				
Tasa interna de rentabilidad de los controles (COSTO INICIAL DE CONTROLES / VALOR ACTUAL NETO)	**69%**	**El valor objetivo debe superar el 20% de rentabilidad de los controles**			
Plazo de recuperación (valor actual neto > costo de controles)	**Al 1er año**				
Descontando	**Al 2do Año**				

BDO

35

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

	OBJETIVOS ESTRATÉGICOS			RESPUESTA SI	
Ítem	NEGOCIO	TECNOLOGÍA INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN	Proyectos/Actividades de Seguridad de la Información asociados a los objetivos de Negocio y TI	Impacto negativo en la falta de gestión
1	Aumentar la Rentabilidad	Optimización de la gestión de licenciamiento	Cumplimiento legal Integridad de datos Disponibilidad operativa	1. Implementación de herramienta de gestión de software (p.e. Altiris, Fix IQ) 2. Desarrollo de estándares técnicos de configuración de seguridad en plataformas 3. Configuración de GPO y políticas locales en WS para no permitir la instalación de SFW desautorizado 4. Revisión anual de licenciamiento	Multas por no-cumplimiento Riesgo de virus, malware, etc. por instalación de software no autorizado Deficiencia en [illegible] funcionamiento
2	Cuidado de Imagen Aumento de Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (tercerizados)	Gestión de la entrega de servicio de terceras partes	Revisión periódica de proveedores críticos de IT para: 1. Verificar cumplimiento de requisitos normativos relacionados con la seguridad y la operación de los sistemas (SLAs acordados) 2. Verificar condiciones de seguridad asociadas a la disponibilidad de los servicios de IT	Incumplimiento los servicios co Organización (a legales), ya que solidario" en: -> Tratamiento -> Continuidad -> Cumplimient
3	Acelerar la atención de los reclamos, Gestión del cliente, Atención al cliente, Post-Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (interno)	Gestión de las vulnerabilidades técnicas y gestión de incidentes de seguridad	1. Implementación de solución de antivirus 2. Mantenimiento anual y actualización de BD de antivirus 3. Implementación de celula de respuesta ante incidentes de seguridad	Fuga de inform Indisponibilida Riesgo de integ información en
4	Mejorar los costos a partir de la selección de proveedores de productos de tecnología de punta	Implementación de herramientas tecnológicas en nuevos proyectos para el Negocio	Aceptación de sistemas de acuerdo al marco regulatorio del Negocio	Participación en reuniones de proyecto desde diseño para: 1. Resguardo del cumplimiento normativo y legal en todos los componentes del proyecto 2. Recomendación sobre herramientas o configuraciones para el resguardo de la seguridad 3. Recomendaciones sobre implementación sin perjudicar la operación	Costos adiciona adicionales Falta de cumpli elección de las Multas por no-c Problemas de pe ante implementaciones técnicas no contempladas

FRECUENCIAS				
Período de medición	Frecuencia de la recolección de datos	Frecuencia del análisis de datos	Frecuencia del reporte del resultado de las mediciones	Revisión de la medición
		Mensual	Mensual	Semestral
		Mensual	Mensual	Semestral

VARIABLES DE MEDICIÓN		
Función de medición SI	Inversión en SI	Valoración de impacto negativo en el Negocio
Licencias registradas e instaladas vs Licencias autorizadas no-autorizadas	U$S 21.000 (solución de appliance FixIQ + H/H mensuales x 1 año en controles)	U$S 68.132 (multa de 3.000 días en sueldo mínimo de U$S 500 - 22 días laborales)
Cantidad de observaciones no-conformes por proveedor en auditorías periódicas	U$S 1.000 (H/H mensuales x 1 año en controles)	U$S 100.000 (base incumplimiento de Ley de Habeas Data) riesgo anual

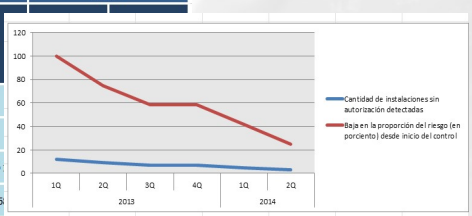
BDO

36

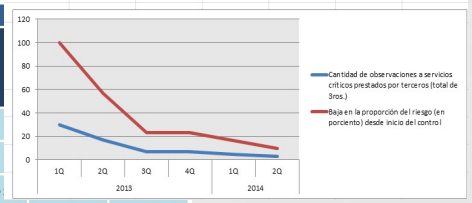
CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

1				2013				2014	
NEGOCIO	TECNOLOGÍA INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN		1Q	2Q	3Q	4Q		
Aumentar la Rentabilidad	Optimización de la gestión de licenciamiento	Cumplimiento legal Integridad de datos Disponibilidad operativa	Cantidad de instalaciones sin autorización detectadas	12	9	7			
			Baja en la proporción del riesgo (en porciento) desde inicio del control	100	75	58			
			Distribución de la inversión/costo en el período	USD 1.750	USD 1.750	USD 1.750	USD		
			Pérdida por multas en caso de materialización del impacto	USD 68.182	USD 68.182	USD 68.182	USD 6		



2				2013					
NEGOCIO	TECNOLOGÍA INFORMÁTICA	SEGURIDAD DE LA INFORMACIÓN		1Q	2Q	3Q	4Q		
Cuidado de imagen Aumento de Venta	Gestión de Nivel de Servicio en los procesos de IT que dan soporte a Áreas de Negocio (tercerizados)	Gestión de la entrega de servicio de terceras partes	Cantidad de observaciones a servicios críticos prestados por terceros (total de 3ros.)	30	17	7			
			Baja en la proporción del riesgo (en porciento) desde inicio del control	100	57	23			
			Distribución de la inversión/costo en el período	USD 1.000	USD 1.000	USD 1.000	USD		
			Pérdida por multas en caso de materialización del impacto	USD 33.000	USD 33.000	USD 33.000	USD 33.000	USD 33.000	USD 33.000



BDO

37

CFOs MEETING 2023 | Cross Industria

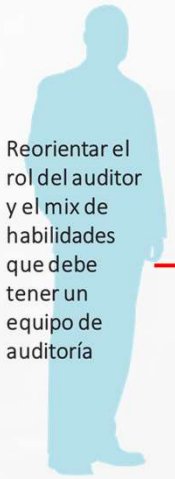
Entendiendo la seguridad para la toma de decisiones

BDO

38

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones



Reorientar el rol del auditor y el mix de habilidades que debe tener un equipo de auditoría

PARTICIPACIÓN DE AUDITORIA EN PROYECTOS

Automatización de procesos, Big Data, Machine Learning, BI

- Entender el negocio
- Definir de universo de TI
- Realizar la evaluación de riesgos
- Formalizar el Plan de Auditoría

DIRECTRICES DEL MODELO DE DIGITALIZACIÓN DE LA AUDITORÍA

- Estandarización de sistemas
- Movilidad y la interconectividad de los equipos de auditoría
- Colaboración entre los equipos y con los clientes
- Automatización y eficiencia de los procesos
- Análisis y visualización de la información disponible
- Disponibilidad y seguridad de la información
- Cumplimiento regulatorio

BDO

39

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

NIVEL 1 Madurez tecnológica

- Uso de plataformas y servicios estandarizados en la nube
- Invertir en tecnología o externalizar servicios
- Mecanismos sencillos de colaboración para intercambio de información y reporting
- Soluciones de colaboración para equipo de trabajo y con clientes.
- Explorar el uso de herramientas de análisis de datos

NIVEL 2 Madurez tecnológica

- Gestión de la organización interna basado en un sistema de gestión integrado (CRM+ERP).
- Uso de herramientas de análisis de datos para la extracción de información y pruebas de controles y sustantivas.
- Plantear el uso de soluciones automatizadas para procesos concretos

NIVEL 3 Madurez tecnológica

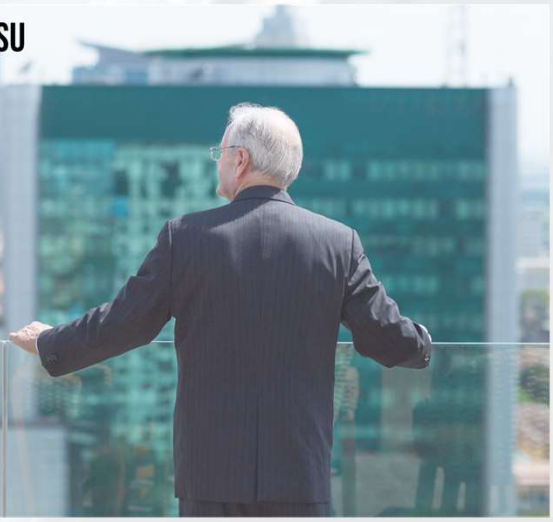
- Conexión a diferentes herramientas útiles para la identificación de riesgos preliminares y aseguramiento de la independencia.
- Uso intensivo de herramientas de análisis de datos que sean capaces de realizar también análisis predictivo.
- Automatización de los procesos de auditoría con uso combinado de robótica, inteligencia artificial y machine learning

BDO

40

LO PRIMORDIAL PARA EL NEGOCIO ES CONOCER SU ENTORNO

- PARA APLICAR TECNOLOGÍA EN FORMA ADECUADA
- ESTABLECER LOS CONTROLES NECESARIOS QUE ASEGUREN SUS PROCESOS E INFORMACIÓN
- Y LE PERMITA CREAR UN ENTORNO AUDITABLE ACORDE AL ASEGURAMIENTO DE SUS OBJETIVOS



41

42

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

¿QUÉ DEBE DOMINAR EL C-LEVEL ACERCA DE CIBERSEGURIDAD?

EL GOBIERNO ASEGURA QUE LA ESTRATEGIA DEL NEGOCIO SE MANTIENE CONSISTENTE CON LAS METAS DEL NEGOCIO

BASAR LAS DECISIONES DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y TECNOLOGÍA SOBRE LAS CONSECUENCIAS POTENCIALES AL NEGOCIO

MARCO INTERNO DE CUMPLIMIENTO Y COMUNICACIONES PARA PROTEGER EL NEGOCIO

DOMINAR UNA ESTRATEGIA PARA QUE TUS EMPLEADOS SEAN VIGÍAS Y AGENTES PARA PREVENIR CUALQUIER RIESGO EN TU COMPAÑÍA

SABER LOS RIESGOS QUE IMPLICA NO CUMPLIR CON MANDATOS LEGALES Y REGULATORIOS SOBRE LOS DATOS

CONOCER EL NIVEL DE MADUREZ RESPETO DE CIBERSEGURIDAD CON LA QUE CUENTA TU EMPRESA

BDO

43

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

¿QUÉ DEBE DOMINAR EL CISO Y EL CIO ACERCA DEL NEGOCIO?

- Entender el gobierno de seguridad de la información, en qué consiste y cómo se logra.
- Entender Estrategia de seguridad de la información
- Entender el significado, el contenido, la creación y el uso de políticas
- Desarrollar casos de negocio y obtener el compromiso de la Dirección.
- Definir requisitos de métricas de gobierno

CRITERIO ESTRATÉGICO APLICABLE AL ENTORNO

PENSAMIENTO EN PROCESOS Y LÍDERES

CONOCIMIENTO DEL NEGOCIO

CONOCIMIENTO DE LOS PROCESOS DE NEGOCIO Y SUS OBJETIVOS

CONOCIMIENTO DE LA TECNOLOGÍA APLICABLE

CONOCIMIENTO DE LAS METODOLOGÍAS APLICABLES

BDO

44

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

GESTIONAR EL TALENTO

Modificar y entrenar los equipos para que se ajusten a las nuevas tecnologías y creen valor real para el negocio

CREAR UNA ARQUITECTURA ORGANIZACIONAL

Discutir asuntos relacionados con la ciberseguridad en toda la organización. Alinear diferentes procesos de la organización orientados a los roles, datos y privilegios de acceso y procesamiento de datos con una visión de riesgos. Hacer seguimiento a las mejores prácticas de manejo de las crisis

INVERTIR EN CONTROLES

Know Your Customer (KYK) controles y procesos de supervisión para conocer a nuevos y antiguos clientes. Análisis de comportamiento, geolocalización, autenticación basada en riesgos (SOC, CIAM, IAM, OSINT, OFD, etc)

Fortalecer el monitoreo de los contratos y la gestión con terceros

DISEÑAR UN MODELO OPERATIVO CIBERSEGURO

Mejorar los diferentes procesos de la organización con una visión de riesgo. Diseñar componentes de gobierno, procesos, estructura y fuerza de trabajo, tecnología y cultura

MEJORAR LA IDENTIDAD Y AUTENTICACIÓN

Las tecnologías de **autenticación** están evolucionando **más rápido** (certificados móviles, digitales, identificación federada, biometría, etc.) convirtiéndose en la norma.

APRENDER

Divulgar con frecuencia sus políticas de ciberseguridad y capacitar en procesos seguros. Desarrollar **nuevas alianzas y formas de trabajar** en todo el ecosistema tecnológico. Mantener registros de problemas de ciberseguridad

BDO

45

CFOs MEETING 2023 | Cross Industria

Entendiendo la seguridad para la toma de decisiones

PENSAR EN SEGURIDAD Y GOBIERNO TECNOLÓGICO DESDE LAS NECESIDADES DEL NEGOCIO ASEGURA LA CONFIANZA DIGITAL EN ACCIONISTAS Y CLIENTES Y PROMUEVE LA INNOVACIÓN MINIMIZANDO RIESGOS

BDO

46


NIST
CLOUD
BIA
ISO20000
BCRA
EVALUACIÓN Y AUDITORÍAS
SANS
BYOD
COBIT5
SWIFT Security Framework
GOBIERNO
RIESGOS Y CUMPLIMIENTO
IOT
CIBERSEGURIDAD
PRIVACIDAD DE DATOS
CONSULTORÍA TI
GESTIÓN DE LA CONTINUIDAD
COMPLIANCE
PCI-DSS
ISO27001
GESTIÓN DE INCIDENTES
COSO
ISAE3402
ERP
ITIL
BCP
ISO38500
SERVICIOS GESTIONADOS
API | Aseguramiento de Procesos Informáticos
RAS | Risk Advisory Services | IT Assurance, Audit and Compliance
BDO

47