

A photograph of a person from behind, sitting at a desk in a server room. They are using a laptop. In the background, there are server racks filled with equipment. The lighting is soft, and the overall tone is professional and technical. There are two red vertical bars on the page: one on the left side and one at the bottom left corner.

ENCUESTA GOBIT 2022

# ESTADO DEL ARTE DE LA **CIBERSEGURIDAD**, GOBIERNO DE TI Y LOS NEGOCIOS

DICIEMBRE 2021 - ENERO 2022

# CONTENIDO

---

Encuesta GOBIT	3
Objetivos y Alcance	4
Entorno, Gestión y Tecnología	5
Las partes que conforman el cubo	6
Resumen comparativa 2019-2022	7
Entorno	11
Gestión	13
Tecnología	15
Principales puntos hacia la innovación	18
Enfoque de la ciberseguridad 2022	19
Conclusiones	21
La importancia de la seguridad de la información	22
Recomendaciones para la compañía	23
Servicios gestionados para la tercerización en seguridad de la información, ciberseguridad y gobierno TI	26
Contacto	28

---



# ENCUESTA GOBIT 2022

## CIBERSEGURIDAD, GOBIERNO DE IT Y LOS NEGOCIOS

Las nuevas tecnologías y los modelos de negocio se integran sin distinguir donde empieza uno y donde termina el otro.

Así también, la seguridad de la información abraza a ambas desde la concepción que la información circulante, en proceso y almacenada le da vida a las organizaciones.

Es imposible tener una visión empresarial sin al menos tomar consciencia de la importancia de todas ellas.

El gobierno tecnológico y la seguridad de la información deben ser considerados por las Juntas Directivas, para conformar un plan de negocio en donde sus objetivos y metas se van apoyados por la innovación que propone el uso de la tecnología.

Las áreas de TI ¿están preparadas para pensar en función del negocio y responder a las necesidades de innovación y transformación digital?, en las áreas del negocio ¿se tienen en cuenta las necesidades de gobierno y cumplimiento de la empresa en función de los riesgos asociados a su entorno de negocio en el uso de la tecnología?

Desde BDO en Argentina hemos planteado una nueva visión sobre el gobierno tecnológico para alcanzar la innovación y la transformación digital en el negocio.

Bajo este enfoque, y a través de esta encuesta, hemos detectado la brecha actual para alcanzar este objetivo.

## OBJETIVO Y ALCANCE

### Pequeños actos de consciencia generan un gran efecto en la seguridad para todos

#### ► OBJETIVO

El objetivo de nuestro estudio es el de determinar el nivel de madurez e implementación de capacidades de gobierno de la tecnología en las empresas, para estimar el nivel de exposición a las brechas de seguridad en el negocio -respecto del uso de la tecnología-, y cuán distantes pueden estar de alcanzar la transformación digital y contar con herramientas tecnológicas necesarias para innovar.

#### ► ALCANCE

El estudio se desarrolló en la región LATAM, con la participación de los principales CXO Latinoamericanos (50% CISOs, 31% CIOs y 19% CXO), mediante una encuesta realizada a fines del 2021 y principio 2022 en Argentina, Colombia, Paraguay, Perú, Uruguay y Venezuela.

#### ► DIRIGIDO A

Gerentes de área de negocio, CFO (directores financieros), CIO (directores y gerentes de sistemas), CISO (directores, gerentes y jefes de seguridad informática o seguridad de la información).

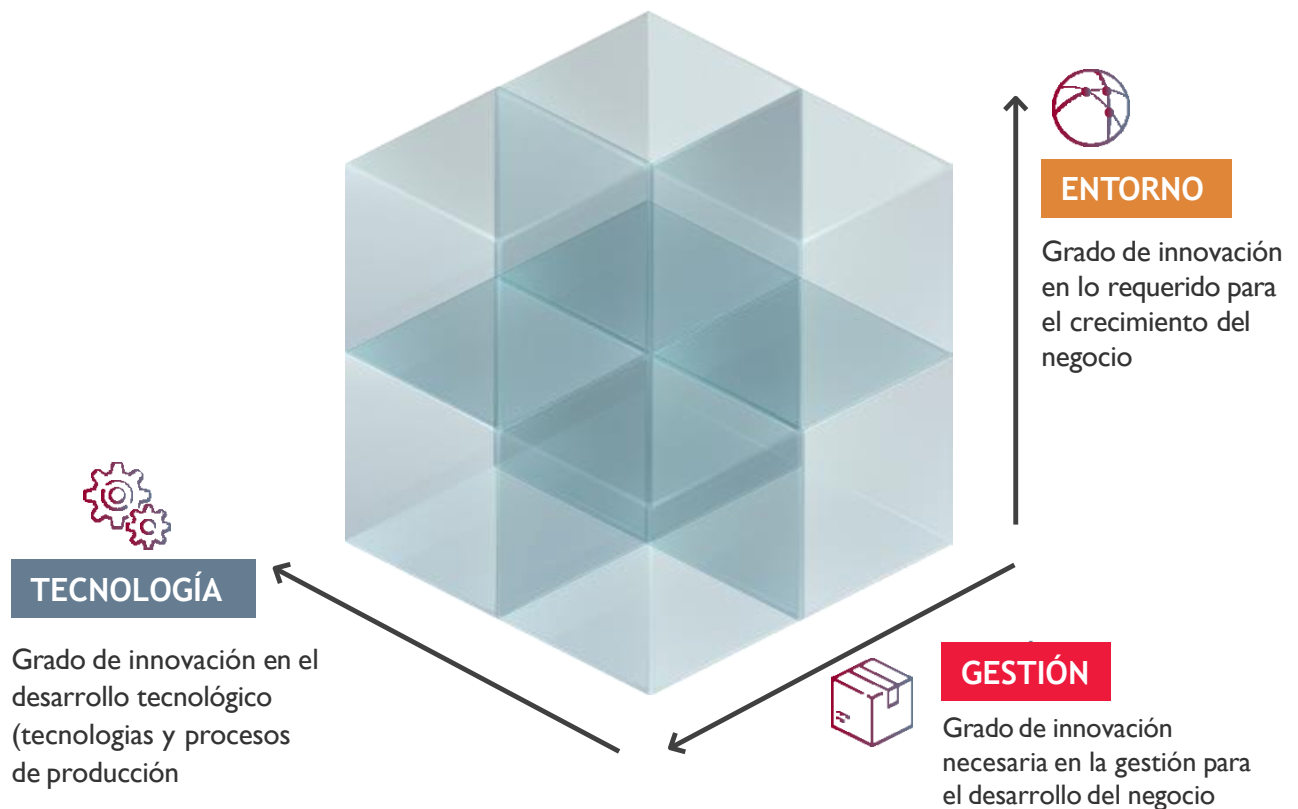
“ La digitalización de los procesos trae un sinfín de ventajas en el ecosistema de negocios: rapidez, eficiencia, menores costos, pero también nos colocan en el radar de ciberdelincuentes que evolucionan y perfeccionan sus métodos de acción.

FABIÁN DESCALZO | Socio en API en BDO Argentina

”

# ENTORNO, GESTIÓN Y TECNOLOGÍA

Hemos planteado una nueva visión sobre el gobierno tecnológico y de ciberseguridad para facilitar a nuestros clientes la innovación y transformación digital



La estrategia corporativa y sus necesidades de innovación en el negocio, requiere de cambios en su entorno de gestión y tecnológico, lo que impacta directamente a su función de acompañar al negocio con soluciones tecnológicas que le den un resultado que aporte al cumplimiento de sus objetivos.

Por ello, esta necesidad de innovación planteada desde la estrategia corporativa está condicionada por el mercado y las presiones regulatorias, a que hoy se requiere un alto rendimiento, velocidad en los cambios para la toma de decisiones de negocio y una mayor exigencia en la transparencia y el cumplimiento de nuevas regulaciones, basadas en su mayoría, en la gestión de la información y el uso de nuevas tecnologías.

Debido a ello es que entendemos que una forma de abordar la planificación estratégica para nivelar en forma balanceada el grado de innovación en cada compañía, se traduce en conformar un “CUBO DEL GOBIERNO TECNOLÓGICO”, en el cual podemos evaluar las condiciones de entorno de negocio, desarrollo de la tecnología y la madurez y capacidades de la gestión, lo que nos permite determinar el grado de innovación en:

- ▶ Lo requerido para el crecimiento del negocio (**Entorno**)
- ▶ El desarrollo tecnológico y procesos de producción (**Tecnología**)
- ▶ La gestión necesaria para el desarrollo del negocio y la tecnología asociada (**Gestión**)

# LAS PARTES QUE CONFORMAN EL CUBO

## Medir y facilitar la innovación y transformación digital

API, el área de servicios de BDO en Argentina especializada en estos temas, ofrece a las empresas de cualquier tipo de industria soluciones estratégicas para el gobierno de su tecnología y ciberseguridad, con una visión corporativa para considerar en el objetivo de lograr el resultado del negocio apoyado en la tecnología.

Estos sectores interactúan entre sí basándose en nuestro concepto de “CUBO DE GOBIERNO TECNOLÓGICO”, orientado a medir y facilitar la innovación y transformación digital en las empresas para ayudar y orientar en temas de ciberseguridad y tecnología aplicada sobre la base de conocimiento de su entorno, la tecnología actual y la gestión sobre sus procesos de negocio y tecnológicos.



### ► GOVERNANCE, RISK & COMPLIANCE

**SERVICIOS:** Análisis de riesgo tecnológico del negocio. Gestión y análisis de procesos de servicios de ciberseguridad y tecnología. Protección y privacidad de información.

### ► PROCESOS Y GESTIÓN DEL CONOCIMIENTO

**SERVICIOS:** Diagnóstico de gobierno tecnológico y ciberseguridad industrial y empresarial. BCM-Continuidad y ciber-resiliencia. Implementación de Sistemas de Gestión ISO27001, ISO20000-1, ISO22301.

### ► AUDITORÍA IT

**SERVICIOS:** Auditoría IT Bancos Físicos y Digitales, Fintech y Empresas. Auditoría a Sistemas de Gestión ISO27001, ISO20000-1, ISO22301.

### ► CIBERSEGURIDAD Y FORENSIA DIGITAL

**SERVICIOS:** Pentest y Análisis de Vulnerabilidades. Forensia digital. Seguridad en ambientes remotos, virtualizados y nube. Ciberseguridad industrial. Playbooks y análisis de ingeniería social.

### ► GOBIERNO E INFRAESTRUCTURA IT

**SERVICIOS:** Diagnóstico de gobierno tecnológico y ciberseguridad industrial y empresarial. BCM-Continuidad y ciber-resiliencia. Implementación de Sistemas de Gestión ISO27001, ISO20000-1, ISO22301.

### ► CONTROL Y REGULACIONES

**SERVICIOS:** Auditorías y certificaciones de riesgos IT. ISAE 3402 / ISAE3000. Medios ópticos (IGJ) y Auditoría de cumplimiento CNV.

## RESUMEN COMPARATIVO 2019-2022

### Antes y después de la pandemia, analizamos el impacto en los indicadores estudiados

Previo a la pandemia realizamos este estudio en el 2019, sin esperar el impacto de la pandemia durante los años 2020-2021.

La situación de la seguridad de la información sigue en crecimiento y en importancia en las organizaciones en general y en particular para Latinoamérica.

Durante el 2022, retomamos la encuesta y de manera extendida hemos agregado algunos nuevos conceptos o ampliación de los mismos para obtener mayor profundidad en las consultas realizadas.

A continuación podrán tener un resumen comparativo 2019-2022, de los principales indicadores en los tres grupos bajo análisis de ENTORNO, GESTIÓN y TECNOLOGÍA.

En algunos casos figurará n/a en la columna de 2019 debido a que es un indicador que no se consultó específicamente en dicho año.

ENTORNO - Indicadores	2019	2022
Deben cumplir con regulaciones de su mercado	52%	50%
Deben cumplir con algún estándar certificable	40%	31%
Se ha concientizado y capacitado al personal sobre riesgo y seguridad	75%	81%
No posee un programa de concientización y capacitación	31%	19%
El presupuesto en seguridad ha aumentado con respecto a años anteriores	32%	69%
El área de seguridad de la información posee su propio presupuesto	80%	77%
SEGURIDAD: Su área es independiente de la gerencia de sistemas	70%	62%
SEGURIDAD: Su área posee más de 3 colaboradores	50%	85%
SEGURIDAD: Posee un marco normativo de seguridad de la información	60%	92%
- Posee política y normas de seguridad para la gestión de terceros (Respondida desde el área de Seguridad Informática o de la Información)	60%	92%
TECNOLOGÍA: Separación de ambientes (desarrollo, pruebas y producción)	100%	75%
- Segregación de funciones por ambiente	70%	38%
- Posee un marco documental para la gestión de servicios de TI (Respondida desde el área de TI)	54%	63%



## RESUMEN COMPARATIVO 2019-2022

Antes y después de la pandemia, analizamos el impacto en los indicadores estudiados

GESTIÓN - Indicadores	2019	2022
<p>AREA DE TI sobre la gestión de proyectos:</p> <ul style="list-style-type: none"> <li>- Participa a usuarios en pruebas funcionales y previas al pasaje a producción</li> <li>- Incluye una evaluación de riesgos técnicos, funcionales, administrativos y de cumplimiento en el diseño de servicios de TI</li> <li>- Realiza actividades de revisión de alineamiento con las políticas de seguridad de la organización</li> <li>- Incluye una revisión de código</li> <li>- Incluye testeo de intrusión y vulnerabilidades previo pasaje a producción</li> </ul>	<p>54%</p> <p>54%</p> <p>77%</p> <p>40%</p> <p>40%</p>	<p>75%</p> <p>63%</p> <p>50%</p> <p>38%</p> <p>38%</p>
<p>AREA DE NEGOCIOS: Ha desarrollado proyectos de negocio que se apoyan en la tecnología</p> <ul style="list-style-type: none"> <li>- Desarrollo aplicado a mejora de aplicaciones de software existente</li> <li>- Desarrollo aplicado a nuevas aplicaciones de software</li> <li>- Desarrollo a ser utilizado en mobile (smartphone/tablet)</li> <li>- Involucró la tercerización de servicios de TI</li> </ul>	<p>65%</p> <p>89%</p> <p>56%</p> <p>56%</p> <p>30%</p>	<p>54%</p> <p>76%</p> <p>76%</p> <p>63%</p> <p>50%</p>
<p>AREA DE NEGOCIOS: Sobre la gestión adecuada de los datos y activos de información donde es propietario de los mismos:</p> <ul style="list-style-type: none"> <li>- Ha realizado una clasificación que le permita identificar su criticidad y criterios de uso</li> <li>- En proyectos tecnológicos o en el uso habitual por parte de la tecnología de los datos de su propiedad, es consultado para dar su parecer, sus recomendaciones y autorización en su uso</li> <li>- Valida y autoriza el tipo de Backups y tiempos de resguardo de los datos de su propiedad.</li> </ul>	<p>70%</p> <p>70%</p> <p>64%</p>	<p>62%</p> <p>39%</p> <p>38%</p>
<p>Desde el AREA DE TI:</p> <ul style="list-style-type: none"> <li>- La gestión de incidentes incluye las definiciones a tomar en caso de incidentes mayores, con el fin de activar el DRP (Disaster Recovery Plan)</li> <li>- Poseen un sitio de contingencia</li> <li>- Se realizan las pruebas anuales de verificación</li> <li>- Intervienen los colaboradores del negocio en las pruebas</li> </ul>	<p>77%</p> <p>85%</p> <p>69%</p> <p>27%</p>	<p>63%</p> <p>50%</p> <p>50%</p> <p>38%</p>

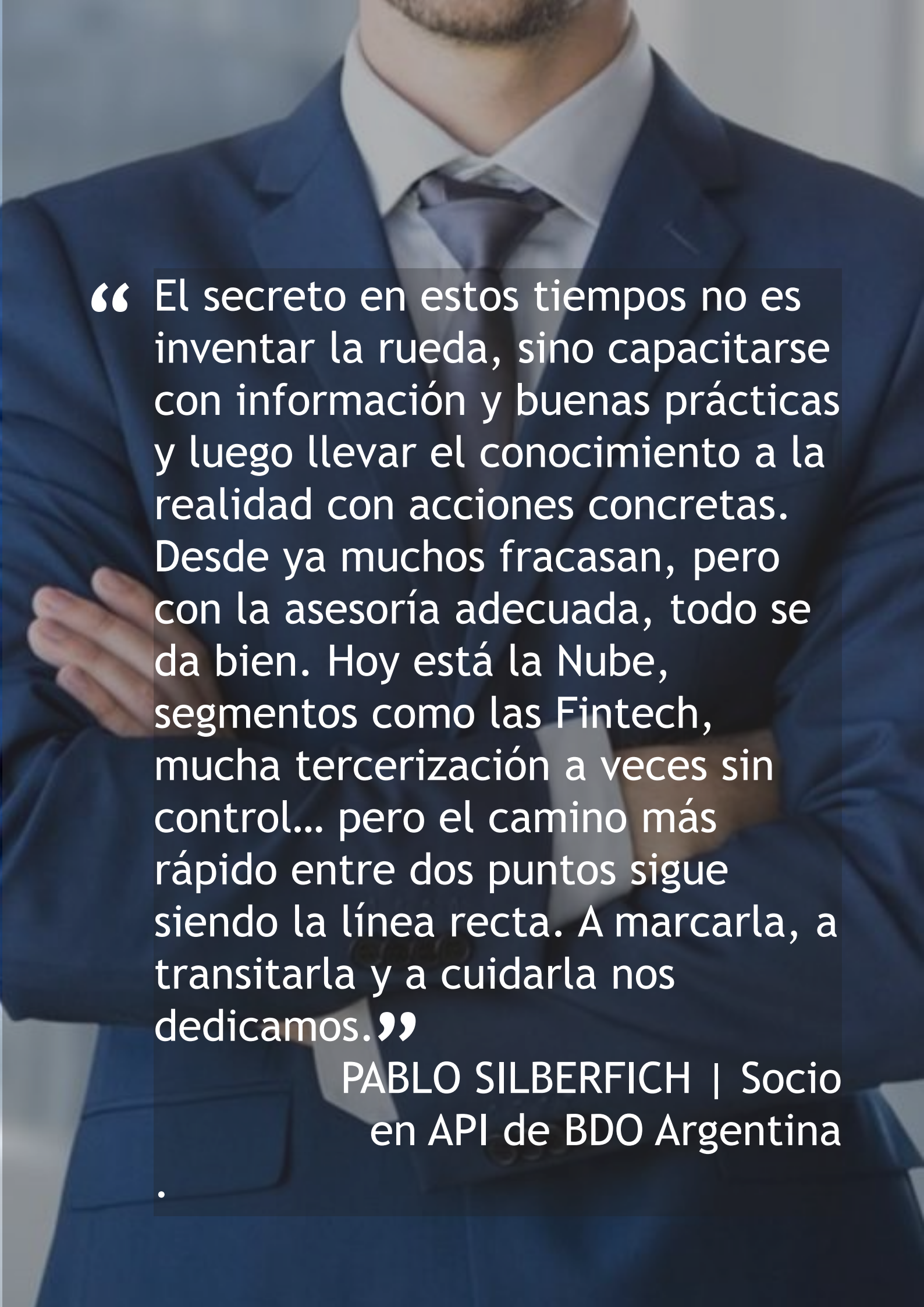


## RESUMEN COMPARATIVO 2019-2022

Antes y después de la pandemia, analizamos el impacto en los indicadores estudiados

TECNOLOGÍA - Indicadores	2019	2022
<p>ÁREAS DE TI: Sobre los controles y monitoreos implementados se mencionan (opción múltiple):</p> <ul style="list-style-type: none"> <li>- Monitorea las comunicaciones</li> <li>- Monitorea los umbrales de capacidad (procesamiento, memoria, disco)</li> <li>- Ha activado pistas de auditoria para la registración de ABM de usuarios, accesos, uso de usuarios privilegiados, etc.</li> <li>- Controla el funcionamiento de infraestructura de energía (UPSs, generador)</li> <li>- Controla el enmascaramiento / ofuscación de datos en ambiente de desarrollo</li> <li>- Controla el funcionamiento de equipos de protección ambiental.</li> </ul>	<p>85%</p> <p>85%</p> <p>54%</p> <p>85%</p> <p>8%</p> <p>15%</p>	<p>88%</p> <p>88%</p> <p>75%</p> <p>50%</p> <p>38%</p> <p>26%</p>
<p>ÁREA DE TI: Realiza un pentest interno y externo a la infraestructura y recursos de TI en forma anual.</p>	23%	50%
<p>INCIDENTES DE SEGURIDAD: Ha sufrido algún incidente de seguridad en este último año:</p> <ul style="list-style-type: none"> <li>- Por Intrusión interna</li> <li>- Por Error humano</li> <li>- Por Error intencional</li> </ul>	<p>56%</p> <p>42%</p> <p>42%</p> <p>21%</p>	<p>54%</p> <p>16%</p> <p>33%</p> <p>n/c</p>
<p>INCIDENTE DE SEGURIDAD: Motivaciones asociadas:</p> <ul style="list-style-type: none"> <li>- Robo de datos</li> <li>- Fraude interno</li> <li>- Disrupción del servicio</li> <li>- Relacionadas con virus o ransomware</li> <li>- En el caso de ransomware, pagaron rescate</li> </ul>	<p>35%</p> <p>20%</p> <p>45%</p> <p>74%</p> <p>20%</p>	<p>33%</p> <p>56%</p> <p>33%</p> <p>33%</p> <p>n/c</p>





“ El secreto en estos tiempos no es inventar la rueda, sino capacitarse con información y buenas prácticas y luego llevar el conocimiento a la realidad con acciones concretas. Desde ya muchos fracasan, pero con la asesoría adecuada, todo se da bien. Hoy está la Nube, segmentos como las Fintech, mucha tercerización a veces sin control... pero el camino más rápido entre dos puntos sigue siendo la línea recta. A marcarla, a transitarla y a cuidarla nos dedicamos.”

PABLO SILBERFICH | Socio  
en API de BDO Argentina

# ENTORNO

## Grado de innovación en lo requerido para el crecimiento del negocio.

De las empresas involucradas, el **50% deben cumplir con regulaciones de su mercado** o una ley específica de su negocio (Por ejemplo SOX, Banco Central, PCI, etc.)

El **31% debe cumplir con algún estándar certificable** adoptado de sus sistemas de gestión (como, por ejemplo, ISO27001, ISO20000, ISO9001) las cuales requieren el cumplimiento de requisitos tanto desde áreas de negocio como desde áreas tecnológicas.

Entre uno de los requisitos, tanto en regulaciones como en certificaciones, se encuentra la capacitación y concientización a todo el personal de la organización.

Hemos identificado que en estos aspectos **ha sido capacitado el 81% del personal** sobre los riesgos e implicancias en el mal uso de las tecnologías y los datos. El 19% no posee un programa de concientización y capacitación.

Otras consideraciones son importantes que definen las condiciones del entorno de una organización para la innovación y transformación digital arrojando los siguientes resultados:

### ÁREAS DE SEGURIDAD DE LA INFORMACIÓN

- ▶ El 62% de las áreas de seguridad de la información son independientes de la gerencia de sistemas. Y un 30% de ellas dependen directamente de la dirección (CEO/Directorio). El 85% están compuestas por más de 3 colaboradores.
- ▶ El 92%\* de los encuestados posee un marco normativo de seguridad de la información. Mismo porcentaje aplica a la gestión de terceros (proveedores, contratistas y consultores), así también considera que los servicios del área están organizados y documentados.

\*Respondida desde el área de Seguridad Informática o de la Información

- ▶ El 69% indicó que los servicios CORE (principales) son tercerizados. Solo el 77% ha indicado que se establecen controles en los contratos con los proveedores de los servicios tercerizados.

### ÁREAS DE TI

- ▶ El 25% de las áreas de TI dependen directamente de la dirección (CEO/Directorio).
- ▶ El 38% posee directamente un área de ciberseguridad.
- ▶ El 75% de los encuestados posee separación de ambientes (desarrollo, pruebas y producción), solo el 38% segrega las funciones por ambientes.
- ▶ El 50% indica que los servicios del área están organizados y documentados.
- ▶ El 63%\* posee un marco documental para la gestión de servicios de TI. Pero solo el 38% posee políticas o normas de seguridad para la gestión de terceros.

\*Respondida desde el área de TI

- ▶ El 38% indicó que los servicios CORE (principales) son tercerizados. Solo el 13% ha indicado que se establecen controles en los contratos con los proveedores de los servicios tercerizados.





## ENTORNO

### Grado de innovación en lo requerido para el crecimiento del negocio

#### ► PRESUPUESTO DE ÁREAS DE SEGURIDAD DE LA INFORMACIÓN

El 69% de los encuestados considera que el presupuesto ha aumentado con respecto a años anteriores.

El 77% de las áreas de seguridad de la información posee su propio presupuesto.

El 85% contempla dentro de su presupuesto aspectos económicos como no económicos. El 85% de los encuestados considera las amenazas y riesgos actuales.

#### ► PRESUPUESTO ÁREAS DE TI

- El 50% de los encuestados considera que el presupuesto ha aumentado con respecto a años anteriores.
- El 63% de las áreas de TI posee su propio presupuesto.
- El 50% contempla dentro de su presupuesto aspectos económicos como no económicos. El 50% de los encuestados considera las amenazas y riesgos actuales.

\* Los aumentos de presupuesto son en valor real independiente del ajuste o corrección inflacionaria.

# 50%

De las áreas de TI, considera que su presupuesto ha aumentado con respecto a los años anteriores





# GESTIÓN

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

Necesitamos de la gestión para el desarrollo del negocio y la tecnología asociada. Si pensamos en desarrollar nuevos negocios o nuevos modelos de negocio, soportados por la tecnología y seguridad de la información, solo será posible si sabemos gestionarla.

### ÁREAS DE TI

- ▶ La **gestión de proyectos** (opción múltiple):
  - El 75% participa a los usuarios en las pruebas funcionales y previas al pasaje a producción.
  - El 63% incluye una evaluación de riesgos técnicos, funcionales, administrativos y de cumplimiento en el diseño de servicios de TI.
  - El 50% realiza actividades de revisión de alineamiento con las políticas de seguridad de la organización.
  - El 38% incluye una revisión de código.
  - El 38% incluye un testeo de intrusión y vulnerabilidades previo al pasaje a producción.

### ÁREAS DEL NEGOCIO

- ▶ El **54% de las áreas de negocios** encuestadas, **ha desarrollado proyectos** de negocio que se apoyan en **tecnología**.
- ▶ Dentro de los **proyectos desarrollados** podemos destacar (opción múltiple):
  - El 76% involucró desarrollo aplicado a mejora de aplicaciones de software existente.
  - El 76% involucró desarrollo aplicado a nuevas aplicaciones de software.
  - El 63% involucró desarrollo a ser utilizado en mobile (smartphone/tablet).
  - El 50% involucró la tercerización de servicios de TI.
  - El 50% involucró servicios en la nube.

- ▶ La **participación activa** de las áreas de negocio (opción múltiple) lo hizo:
  - El 50% en la selección del servicio/producto.
  - El 50% en el análisis de factibilidad de adquisición/implementación del servicio/producto.
  - El 63% en la etapa de las pruebas de funcionamiento.
  - El 76% en la etapa de las pruebas previas a la puesta en producción.
- ▶ Las áreas de negocio que han participado y requieren tecnología, en relación al **análisis de los riesgos**:
  - El 85% capacita a su personal en la práctica y cuidados en el uso de la tecnología implementada en el proyecto.
  - El 77% evalúa los riesgos e impacto de cumplimiento.
  - El 77% evalúa los riesgos e impacto de integridad y confidencialidad de los datos.

- ▶ Considerando la gestión adecuada de los datos y **activos de información** donde es propietario de los mismos:
  - El 62% realizó una clasificación que le permita identificar su criticidad y criterios de uso.
  - En proyectos tecnológicos o en el uso habitual por parte de la tecnología de los datos de su propiedad, el 39% es consultado para dar su parecer, sus recomendaciones y autorización en su uso.
  - El 38% valida y autoriza el tipo de Backups y tiempos de resguardo de los datos de su propiedad.

## GESTIÓN

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

- ▶ El 66% de las empresas encuestadas han realizado un **análisis de riesgo tecnológico** orientado al negocio, que concuerda con la cantidad de empresas que ha realizado un **análisis de impacto al negocio**.
- ▶ El 92% de los encuestados indican que cuenta con un **plan de continuidad de servicios de TI**. A nuestro criterio al no tener un análisis de riesgo tecnológico y de impacto en el negocio, entendemos que existirán puntos no considerados en alguno de estos planes de continuidad.
- ▶ El 63% de las áreas de TI indican que la gestión de incidentes incluye las definiciones a tomar en caso de incidentes mayores, con el fin de **activar el DRP** (Disaster Recovery Plan).
- ▶ El 50% de las áreas de TI indican que poseen un **sitio de contingencia**. En la misma proporción se realizan las pruebas anuales de verificación. Pero solo el 38% indica que en las **pruebas intervienen colaboradores del negocio**. Solo el 25% rota a los colaboradores para maximizar la capacitación.
- ▶ Calificando entre 0 (mínimo) y 10 (máximo), las empresas encuestadas consideran en **6.38** que es de importancia y está desarrollada la **estrategia de ciberseguridad** en la organización.

# 6.38

Considera que es importante y está desarrollada la estrategia de ciberseguridad en la organización



# TECNOLOGÍA

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

Cualquier organización necesita adoptar una visión de gobierno de tecnología e implementarla ordenada y metodológicamente, para administrarla en forma segura y bajo una estrategia corporativa que le permita asignar responsabilidades y recursos orientados a la concreción de sus objetivos de negocio y las necesidades de cumplimiento de su industria.

### ÁREAS DE SEGURIDAD DE LA INFORMACIÓN

- ▶ El 69% posee un **programa** de administración, operación y práctica técnica de seguridad de la información.
- ▶ Sobre los controles y monitoreos implementados se mencionan (opción múltiple):
  - El 100% ha instalado antivirus / antimalware.
  - El 100% ha instalado firewall / cortafuegos.
  - El 85% ha implementado el doble factor de autenticación.
  - El 85% ha implementado control de contenidos.
  - El 85% instaló un antispam.
  - El 77% ha implementado IDS/IPS.
  - El 77% ha implementado la encriptación de datos.
  - El 62% ha implementado la seguridad en dispositivos móviles.

### ÁREAS DE TI

- ▶ El 38% posee un **programa** de administración, operación y práctica técnica de seguridad de la información.
- ▶ Sobre los controles y monitoreos implementados se mencionan (opción múltiple):
  - El 88% monitorea las comunicaciones.
  - El 88% monitorea los umbrales de capacidad (procesamiento, memoria, disco).
  - El 75% ha activado pistas de auditoría para la registración de ABM de usuarios, accesos, uso de usuarios privilegiados, etc.
  - El 50% controla el funcionamiento de infraestructura de energía (UPSs, generador).
  - El 38% controla el enmascaramiento / ofuscación de datos en ambiente de desarrollo.
  - El 26% controla el funcionamiento de equipos de protección ambiental.
- ▶ El 50% realiza un **pentest interno y externo** a la infraestructura y recursos de TI en forma anual. El 38% no lo realiza. El 12% restante no sabe/no contesta.

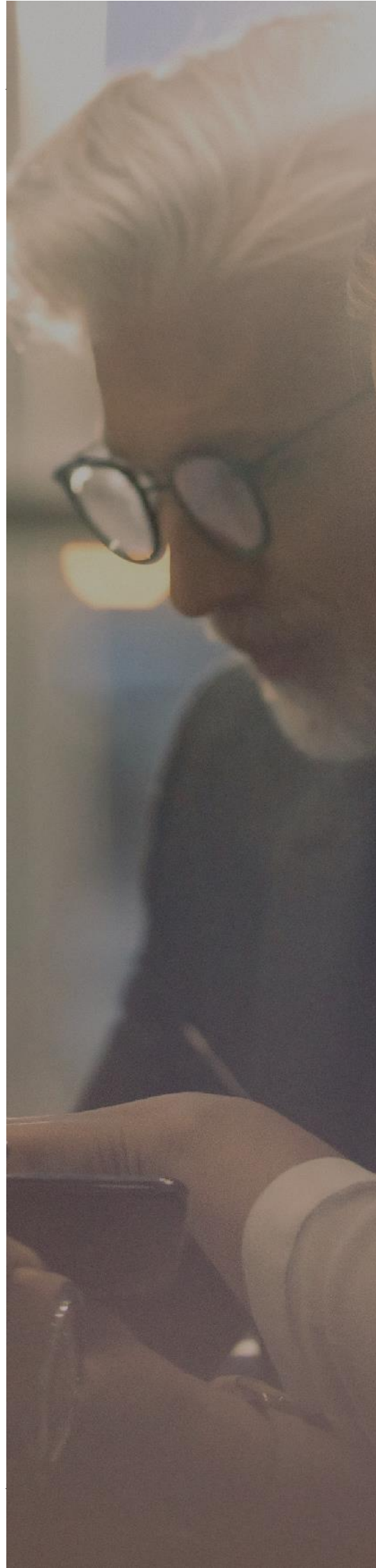
## TECNOLOGÍA

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


- ▶ El 54% de las áreas de seguridad de la información han sufrido algún incidente de ciberseguridad o de seguridad de la información.
- ▶ En los casos que han sufrido un incidente de ciberseguridad (opción múltiple):
  - El 33% indicó que el incidente estuvo relacionado con ataques por ransomware y/o virus. El 67% indica que no se ha pedido un pago o un rescate, mientras que el 33% lo desconoce.
  - El 16% de los casos estuvo relacionado con una intrusión externa (robo de datos, cambio en configuraciones). El 68% dijo que no.
  - El 33% indicó que el incidente estuvo relacionado con una actividad interna por error. El 83% indica que la acción no fue provocada, mientras que el 17% lo desconoce.
  - El 56% tuvo como motivación el fraude. El 33% indica que la motivación ha sido la interrupción de servicio. El 33% el robo de datos.

# 54%

Las áreas de seguridad de la información indicaron que han sufrido algún tipo de incidente de ciberseguridad.





A close-up photograph of a man and a woman looking at a smartphone together. The man, on the left, has short blonde hair and is wearing glasses. The woman, on the right, has long blonde hair and is wearing a white shirt. They are both looking down at the phone held by the woman. The background is blurred with warm, bokeh lights.

“ No bajas la guardia, la falta de concientización en materia de ciberseguridad es una ventaja para los cibercriminales. ”



# PRINCIPALES PUNTOS HACIA LA INNOVACIÓN

Nuestro “Cubo de Gobierno Tecnológico”, para medir y facilitar la innovación y transformación digital en las empresas orientando en temas de ciberseguridad y tecnología aplicada en la gestión sobre sus procesos de negocios y tecnológicos

## ENTORNO

Incluir en los programas concientización a los directivos y personal técnico.

Facilitar los recursos profesionales adecuados, que permitan una buena gestión y una segregación adecuada.

Crear programas de concientización en relación al entorno de negocio y responsabilidades de la organización.

Establecer un marco documental que facilite y delimite la gestión tecnológica alineada al negocio.

## GESTIÓN

Mejorar los controles previos al pasaje a producción e involucrar a los usuarios, dándoles participación en los proyectos y capacitándolos en el uso de las nuevas tecnologías.

El negocio debe involucrarse en las definiciones y actividades de continuidad operacional y tecnológica.

## TECNOLOGÍA

Mejorar los controles a proveedores críticos de servicios tercerizados.

Mejorar los controles periódicos de seguridad en infraestructura de IT y acceso a la información.

Implementar procesos de control y herramientas para prevenir incidentes internos.

Implementar herramientas para la Seguridad Mobile, tecnología de virtualización y cloud.

# ENFOQUE DE LA CIBERSEGURIDAD 2022

## 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.

► **CAMBIO EN EL ENTORNO REGULATORIO:** Los desafíos a los que se enfrentan las organizaciones en un entorno regulatorio dinámico y ambiguo.

► **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.

► **INNOVACIÓN DISRUPTIVA:** Si las organizaciones están preparadas para adaptarse y / o capitalizar la disrupción.

► **CULTURA:** Si las organizaciones entienden, monitorean y administran el nivel, los incentivos y las acciones que impulsan el comportamiento deseado frente a la ciberseguridad y seguridad de la información.

► **PRIVACIDAD DE DATOS:** Cómo las organizaciones protegen los datos confidenciales bajo su cuidado y garantizan el cumplimiento de todas leyes y regulaciones aplicables.

► **GESTIÓN DE PROVEEDORES:** La capacidad de las organizaciones para seleccionar y monitorear las relaciones con terceros.



An aerial photograph of a paved path with a grid pattern. A large, semi-transparent map of South America is overlaid on the path. Several cyclists are riding along the path, their shadows cast on the pavement. The cyclists are wearing various colored jerseys and helmets. The map of South America is positioned in the upper left and center of the frame, with the text block in the lower right.

“En BDO hacemos lo que hacemos de manera excepcional y lideramos en cada lugar donde estamos presentes: hemos sido la organización global con mayor crecimiento en nuestro rubro durante los últimos 10 años, y atendemos a más de 775.000 clientes a nivel global”.



# CONCLUSIONES

## Principales puntos del estudio ENCUESTA GOBIT

La seguridad de la información desde los aspectos del cubo de gobierno tecnológico, está tomando cada año mayor importancia en el proceso y estrategia de innovación a nivel empresarial.

### ENTORNO

Observamos que se ha mantenido e incrementado el proceso de **concientización** a las personas de las organizaciones, como una fuente de prevención de los posibles riesgos de ciberseguridad. Así mismo, los programas de **concientización y capacitación** forman parte del ciclo de entrenamiento periódico en las empresas, muy pocas de ellas no lo poseen llegando este año a solo un 19%.

El **área de ciberseguridad se mantiene mayormente independiente** de la gerencia de sistemas, con el fin primero de evitar sesgos y ser contralor tanto del negocio como de los procesos tecnológicos e informáticos por sí mismos. Además se consolida poco a poco a conformar un área con funciones y cantidad de colaboradores en crecimiento.

**Alinearse a estándares y a un marco normativo** ha sido un punto de notorio crecimiento este año, llegando al 92% en caso afirmativo, situación que valoramos desde el punto de vista de entendimiento, análisis y planificación de mejorar en torno al ciclo de calidad de la seguridad de la información.

### GESTION

La toma de **responsabilidad y participación de las áreas de negocio** y TI, en los temas de seguridad de la información mantiene y denota un crecimiento cada año.

Más del 60% de los encuestados este año han desarrollado un **análisis de riesgo tecnológico orientado al negocio** junto con el análisis de impacto que estos riesgos pudieran producir.

La toma de **responsabilidad y participación de las áreas de negocio** y TI, en los temas de la seguridad de la información mantiene y denota un crecimiento cada año.

En este sentido casi la totalidad de los encuestados, en un 92% cuenta, con un **plan de continuidad del negocio**, visto como un instrumento necesario o exigido de importancia. Igualmente no se corresponde con el bajo compromiso en las actividades que ello implica.

Los entrevistados califican en **promedio en 6.38 la importancia de la seguridad de la información**, creemos que la calificación debería ser mucho mayor entendiendo la proposición de valor que efectiviza la prevención y cuidado de la misma para las empresas.

### TECNOLOGÍA

Junto con el cumplimiento de estándares y marcos normativos, se ha generado un impacto en el desarrollo de la documentación y el cumplimiento con programas de **administración, operación y práctica** de la seguridad de la información. No tanto en las áreas tecnológicas por fuera de la ciberseguridad.

La implementación de controles y monitoreos a nivel tecnológico muestra un incremento de alto impacto, por las tecnologías instaladas (antimalware, firewalls, doble autenticación, antispam, ids/ips, etc.)

Apenas de la mitad de los encuestados, realizan un pentest interno y externo a la infraestructura y recursos de TI en forma anual. Creemos que es una actividad muy importante que debería ser parte de las actividades habituales de control de las organizaciones.

El 54%, un porcentaje que se mantiene, ha sufrido un incidente de seguridad, lo que nos refleja que todavía existe un gran camino por mejorar en los aspectos de innovar en la seguridad de la información.

# LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN

La información es el activo que nos permite tomar decisiones tanto en lo personal y lo laboral, por eso debemos protegerla.

La información es un recurso esencial y vital para nuestra organización.

- ▶ Los datos que generamos y/o utilizamos en nuestro trabajo diario.
- ▶ Los sistemas en los cuales operamos.
- ▶ Los informes que leemos.
- ▶ El conocimiento que poseemos de la empresa.

Toda forma parte de la INFORMACIÓN de la organización y debe ser protegida.

## ¿QUÉ INFORMACIÓN DEBE SER CONSIDERADA CONFIDENCIAL?

- ▶ Datos personales de clientes y colaboradores en general.
- ▶ Información financiera.
- ▶ Proyectos de desarrollo de productos o servicios.
- ▶ Información comprometida con un tercero a mantener confidencial. Cliente, socio, proveedor, etc.

Diariamente manejamos todo tipo de información en nuestra vida laboral y personal. Si miramos con atención, podremos ver que es muy valiosa. No solo para nosotros, sino también para personas malintencionadas que cometen ciberdelitos a través del uso de tecnología e Internet.

Para mantener a salvo nuestros datos privados de estas amenazas que cada vez son más comunes, el ámbito de la Seguridad de la Información nos enseña buenos hábitos a tener en cuenta en nuestra vida personal, familiar y laboral. Sin un comportamiento seguro, los ciberdelincuentes se aprovecharán de nosotros, y además de pérdidas económicas, expondremos la imagen de nuestra organización y la de sus clientes.

## ¿PARA QUÉ PUEDEN UTILIZAR LOS CIBERDELINCUENTES ESTE TIPO DE INFORMACIÓN?

- ▶ Obtener grandes sumas de dinero al venderla en el mercado negro.
- ▶ Suplantar la identidad de algún directivo.
- ▶ Dañar la imagen o credibilidad de nuestra organización.
- ▶ Extorsionar a miembros de nuestra organización.

**No necesitamos ser expertos en seguridad, pero sí ser conscientes de las amenazas a las cuales estamos expuestos y evitar caer en los engaños de los ciberdelincuentes aprendiendo unos pocos hábitos seguros.**



# RECOMENDACIONES PARA LA COMPAÑÍA

La seguridad de la información se construye todos los días, con pequeñas medidas aplicadas por todos.

## ► GESTIÓN DE ROLES

Mantener y controlar que la información solo sea accesible para los perfiles de usuario que realmente necesitan visualizarla y modificarla. Para el resto, debería estar restringida.

## ► CONTROL DE DISPOSITIVOS

Teniendo en cuenta la amplia variedad de dispositivos en el mercado, restringir el acceso solamente a aquellos en los cuales se aplican las herramientas de seguridad adecuadas

## ► PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Para garantizar que los datos no sean afectados por códigos maliciosos, todos los dispositivos deben contar con soluciones de seguridad que detecten proactivamente este tipo de amenazas.

## ► MONITOREO DEL TRÁFICO DE RED

Dado que hay dispositivos que están ingresando a la red por fuera del perímetro físico de la oficina, es necesario hacer un seguimiento de qué tipo de tráfico generan.

## ► CONEXIONES SEGURAS

Para teletrabajo, la implementación de conexiones VPN basadas en el cliente es lo más conveniente, donde el usuario ejecuta la aplicación autenticándose con un nombre de usuario y contraseña, e incluso agregar un segundo factor de autenticación, creando el canal cifrado entre el equipo y la red remota, para un intercambio seguro de datos.

## ► REDACCIÓN DE UNA POLÍTICA DE SEGURIDAD

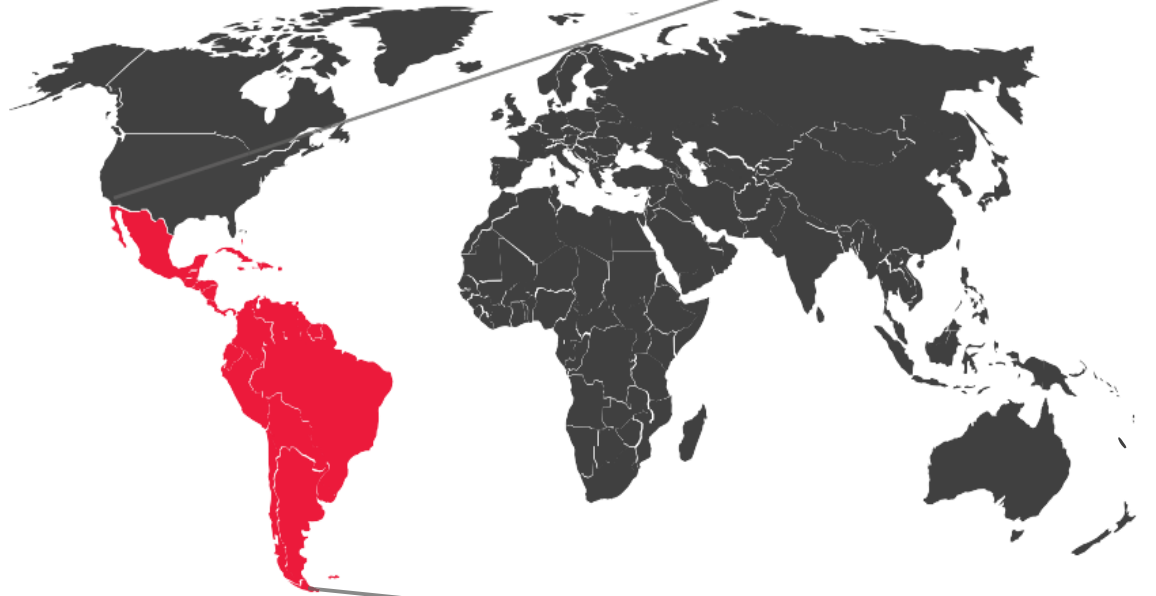
Determinar las obligaciones y responsabilidades de los usuarios respecto al uso de las tecnologías que tienen a su disposición. Definir el tipo de acciones que se pueden hacer y quién está habilitado a ejecutarlas

## ► CONCIENTIZACIÓN DE LOS EMPLEADOS

La educación debe ser un pilar importante para que todos los usuarios sean conscientes de los riesgos a los cuales pueden verse expuestos y cuáles son los cuidados que deben tener al ingresar dispositivos ajenos a la compañía.







## Global

---

**10.8 %**

Incremento  
(A tipo de cambio constante)

---

**1728**

Oficinas

---

**167**

Países

**97.292**

Colaboradores

---



## LATAM

---

**66** Desde Mexico hasta Argentina  
Oficinas

---

**+5.200**  
Colaboradores

## Argentina

---

**4** Buenos Aires  
-Retiro  
-Distrito Tecnológico  
Oficinas **Córdoba**  
**Santa Fé**  
-Rosario

**+800**  
Colaboradores

# SERVICIOS GESTIONADOS PARA LA TERCERIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y GOBIERNO IT

Contamos con una mesa de innovación, donde realizamos un análisis sobre las tecnologías disponibles para aplicarlas en servicios eficaces para la actualidad de nuestros clientes.



## DIGITAL CISO

Externalización de la gestión de seguridad de la información



## SMAAS (SIEM)

Externalización de la gestión de monitoreo y análisis de eventos



## @LIBRARY

Externalización en la gestión del marco documental



## CIBERSEGURIDAD PARA C-LEVEL

Apoyo estratégico en tecnología y ciberseguridad a Directores y C-Level



## GOVERNOR

Automatización de gestión de gobierno tecnológico y de ciberseguridad




## CIBERKNOW

Externalización de la gestión del programa de concientización





A photograph of three business professionals in an office setting. In the center is a woman with long, straight brown hair, wearing a dark blazer over a white collared shirt. To her left is a man with short, wavy brown hair and blue eyes, wearing a white shirt and a blue patterned tie. To her right is a man with dark hair and a beard, wearing a dark suit jacket, white shirt, and dark tie. All three are smiling warmly at the camera. The background is a bright, out-of-focus office environment.

“ La digitalización de los procesos trae un sinfín de ventajas en el ecosistema de negocios: rapidez, eficiencia, menores costos, pero también nos colocan en el radar de ciberdelincuentes que evolucionan y perfeccionan sus métodos de acción. ”

FABIÁN DESCALZO | Socio  
en API de BDO Argentina



FOR MORE INFORMATION:

**PABLO SILBERFICH**

**Socio**

[psilberfich@bdoargentina.com](mailto:psilberfich@bdoargentina.com)

**FABIAN DESCALZO**

**Socio**

[fdescalzo@bdoargentina.com](mailto:fdescalzo@bdoargentina.com)

[www.bdoargentina.com](http://www.bdoargentina.com)

Service provision within the international BDO network of independent member firms ('the BDO network') is coordinated by Brussels Worldwide Services BVBA, a limited liability company incorporated in Belgium.

Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BVBA and the member firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BVBA and/or the member firms of the BDO network.

BDO is the brand name for the BDO network and for each of the BDO member firms.

The fee income of the member firms in the BDO network, including the members of their exclusive alliances, was US\$ 9.6 billion in 2019. These public accounting, tax and advisory firms provide professional services in 167 countries, with 88,120 people working out of 1,809 offices worldwide.

