

GESTIÓN DEL CONOCIMIENTO Y CULTURA ORGANIZACIONAL

Concientización en Ciberseguridad y Change Management

Julio 2022



Fabián Descalzo



Mónica López



Carlos Rozen



Fabián Descalzo

(fdescalzo@bdoargentina.com)



Socio y DPO de BDO en Argentina del Departamento de Aseguramiento de Procesos Informáticos (API).

Posee más de 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)

Mónica López

(mlopez@bdoargentina.com)



Líder de proyectos de concientización de BDO en Argentina del Departamento de Aseguramiento de Procesos Informáticos (API).

Posee experiencia en temas relacionados con: Implementación y Gestión de Programas de Concientización, Formación y Capacitación en Seguridad de la Información, Programas de Protección de Activos de Información, Análisis de Riesgos de IT, Continuidad del Negocio (BCP), Gestión de áreas de Seguridad de la Información, Marco Normativo y documentación de procesos de ciberseguridad, Auditorías de cumplimiento BCRA, entre otras.

Durante estos años acompañó a clientes provenientes de diferentes industrias, tales como; agronegocios, alimentos y bebidas, bancos y aseguradoras, comercialización y retail, energía y recursos naturales, hotelería y entretenimiento, indumentaria y textil, laboratorios, manufactura, petróleo y gas, real estate y construcción, salud, tecnología, medios y telecomunicaciones, transporte y logística, tanto empresas multinacionales, como nacionales y pequeñas empresas.

Es responsable de la gestión de programas de concientización de seguridad de la información y ciberseguridad en clientes, así como de la coordinación para la gestión de automatización del programa, lo que incluye comunicación, evaluación y pruebas del programa de concientización.

Carlos Rozen

(crozen@bdoargentina.com)

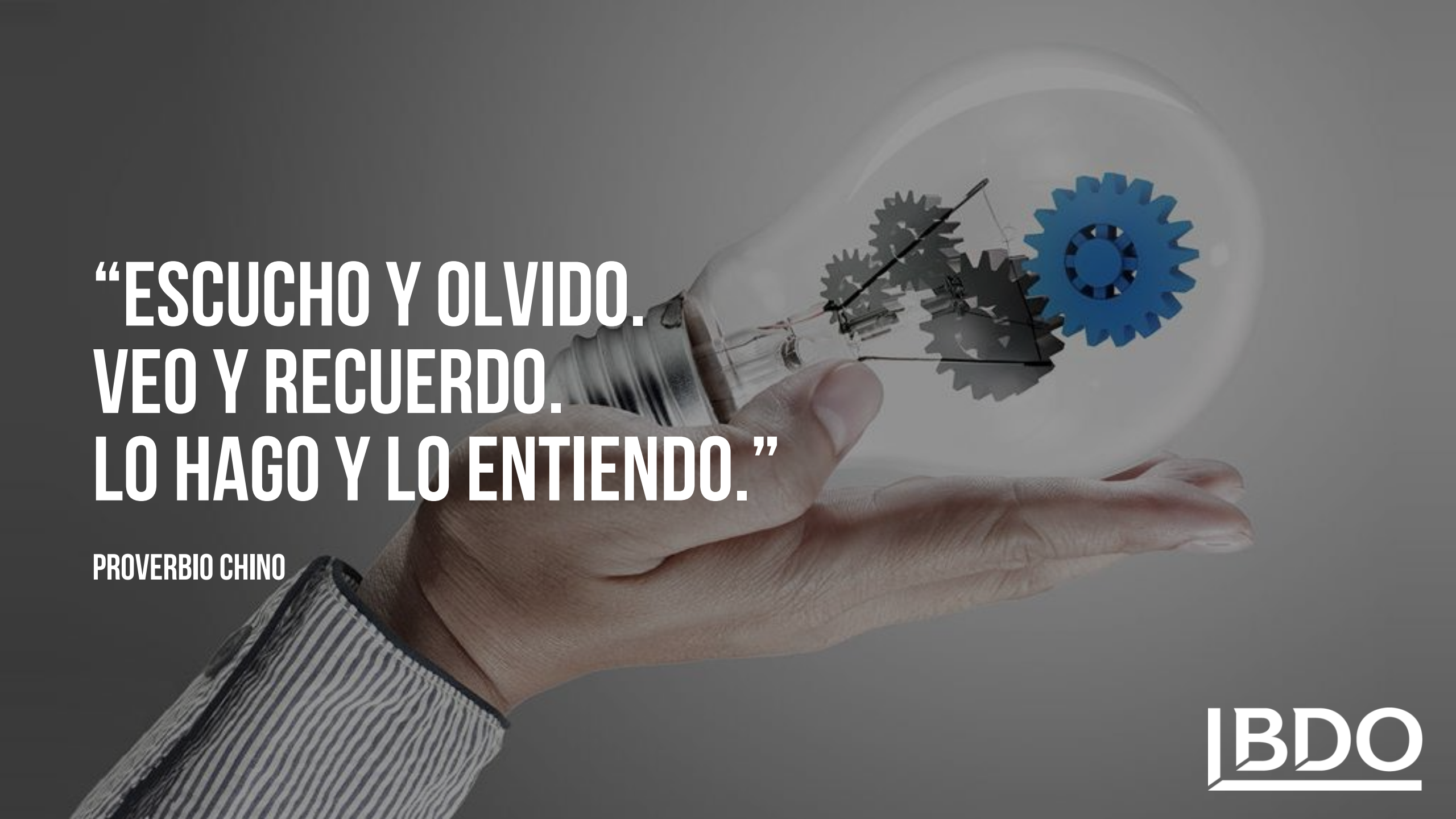


Socio de BDO en Argentina, a cargo de las prácticas de Consultoría.

Integrante del Hub Internacional de Innovación de BDO. Director de la Certificación Internacional en Ética y Compliance, dictada por la Asociación Argentina de Ética y Compliance y la Universidad del CEMA. Fue además Presidente de la Asociación Argentina de Ética y Compliance. Profesor en temas de su especialidad en distintas universidades del país (UBA, UCEMA, San Andrés, y Austral) y profesor invitado en distintas universidades del exterior. Contador Público (UBA) y Auditor Líder en Sistemas de Gestión de Calidad (Georgia Tech). Auditor y consultor certificado en Sistemas de Gestión Antisoborno bajo la ISO 37001 y Risk Manager Profesional Certificado bajo la ISO 31000. Entrenador certificado internacionalmente en los mencionados estándares.

Especialista en nuevas tecnologías y su aplicación en Auditoría y Compliance.

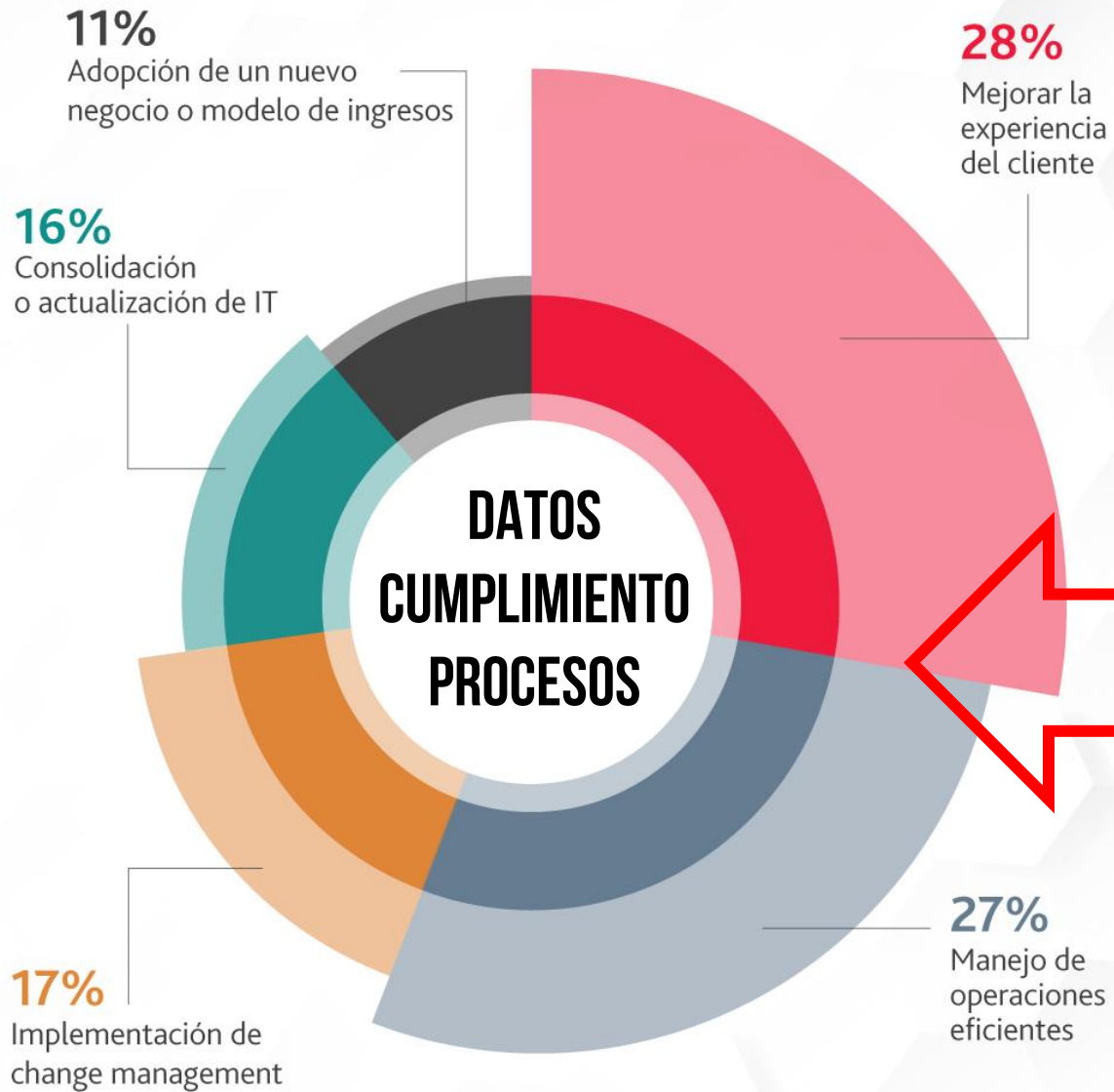
Ha dirigido más de 100 proyectos de consultoría en 10 países. Emprendedor y creador de herramientas informáticas que son usadas en diferentes partes del mundo, tales como T&E Express, ganadora del concurso Visa como la mejor Startup Fintech 2017 de Argentina y Uruguay, y SpeedFlows.com, tecnología “no code”. Conferencista internacional en 20 países

A hand holding a lightbulb with gears inside, symbolizing understanding through action. The background is a dark grey gradient. The text is in white, bold, sans-serif font.

**“ESCUCHO Y OLVIDO.
VEO Y RECUERDO.
LO HAGO Y LO ENTIENDO.”**

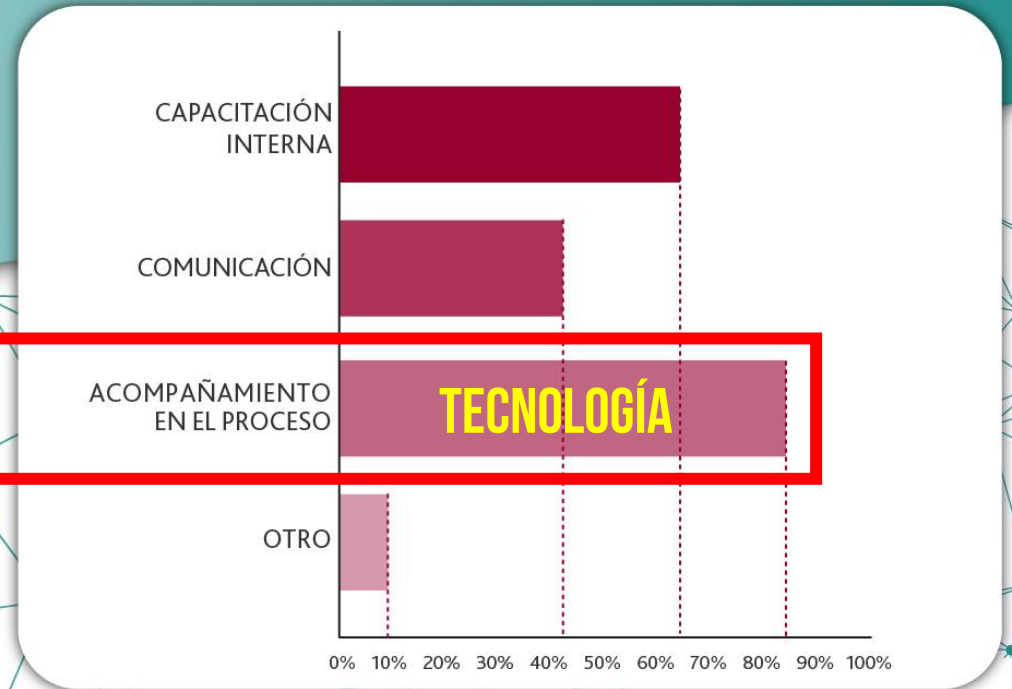
PROVERBIO CHINO

BDO



Transformación Digital

¿En qué aspectos consideran necesario apoyo las organizaciones?



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



- ▶ Las pérdidas anuales por delitos cibernéticos oscilan entre los **\$ 500 mil millones y US\$ 1 billón** y se proyecta que suba a **5 billones de dólares para 2024**.
- ▶ Un ISP reporta **80 mil millones de escaneos maliciosos al día**.
- ▶ Hay **300 millones de nuevos virus** maliciosos o malware creados cada día.
- ▶ Hay **4.000 ataques de ransomware** cada día.
- ▶ En promedio, **los ataques no se detectan hasta 146 días después** de que se haya producido la infracción.



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

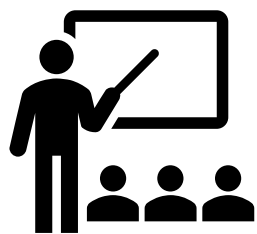
- ▶ **CIBERSEGURIDAD:** Organizaciones suficientemente preparadas para gestionar ciberamenazas que podrían causar interrupciones, daños a la reputación y daños económicos.
- ▶ **CULTURA:** Si las organizaciones entienden, monitorear y administrar el tono, los incentivos y las acciones que impulsan el comportamiento deseado frente a la ciberseguridad y seguridad de la información.
- ▶ **INNOVACIÓN DISRUPTIVA:** Si las organizaciones están preparadas para adaptarse y/o capitalizar la disrupción.



MANUAL DE SUPERVISIÓN DE RIESGOS CIBERNÉTICOS PARA JUNTAS CORPORATIVAS

Principios sobre riesgos al negocio relacionados con ciberseguridad, y como enfrentarlos (actualización y gestión del riesgo de ciberseguridad en toda la empresa, implicancias legales, discutir en las juntas estos riesgos, así como el presupuesto y recursos para mitigarlos)





SEGURIDAD ORGANIZACIONAL

Establece el marco formal de seguridad que debe sustentar la Organización, incluyendo la concientización Integrando el recurso humano con la tecnología

SEGURIDAD DE LA INFORMACIÓN

Se basa en técnicas, metodologías, normas, herramientas y estructuras dentro de la organización

SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Comprende las medidas de protección de activos e información digital que se procesa, transporta y almacena en sistemas interconectados

- ▶ **Parcialidad:** Los temas de seguridad y ciberseguridad son temas de tecnología; ellos deben proteger el negocio
- ▶ **Falsa sensación de protección:** Las más avanzadas herramientas aumentan nuestra ciberseguridad, seguridad y prevención de fraude
- ▶ **Actuar como rebaño:** Otras compañías se recuperaron a incidentes de seguridad con menos inversión

TECNOLOGÍA

GESTIÓN

ENTORNO

DIRECCIÓN Y MANDOS MEDIOS

TÉCNICOS

USUARIO FINAL

35%

DIRECCIÓN

- ▶ Estrategia de negocios
- ▶ Cumplimiento de regulaciones
- ▶ Adopción de certificaciones

MANDOS MEDIOS

- ▶ Cumplimiento de los objetivos
- ▶ Promover proyectos de negocio
- ▶ Garantizar la comunicación interna

36%

- ▶ Proveer los medios para cumplimiento de los objetivos
- ▶ Investigar para la innovación
- ▶ Apoyar tecnológicamente los proyectos de negocio

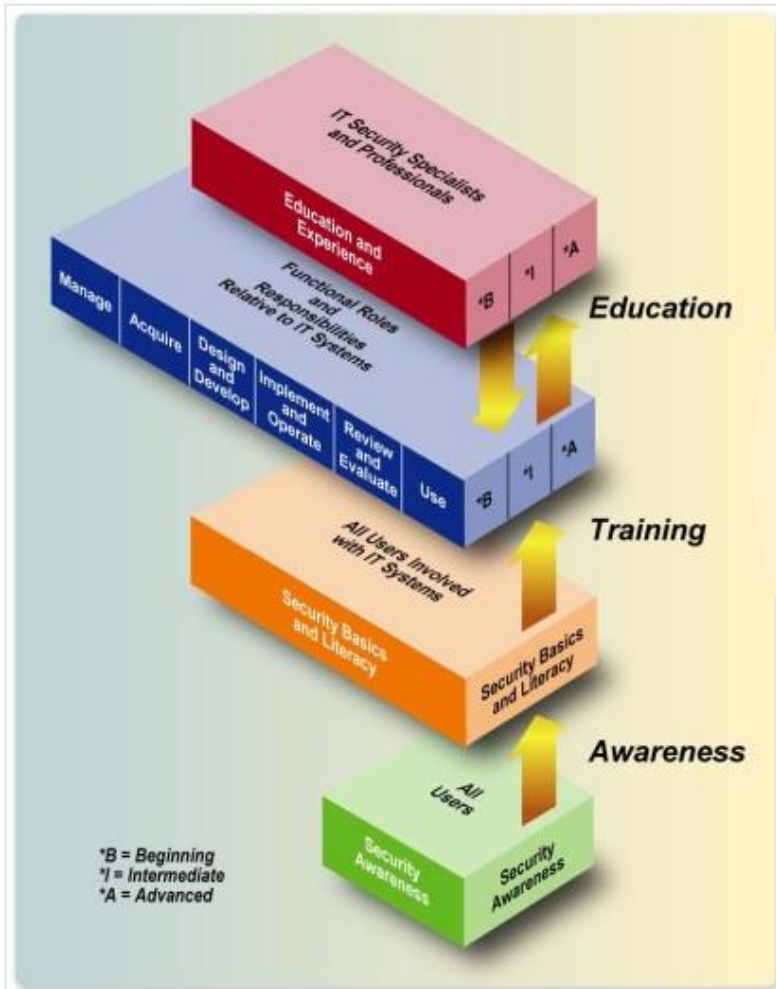
58%

- ▶ Conciencia sobre los datos
- ▶ Conocimiento del empleo de la tecnología
- ▶ Cumplimiento de las normas internas y externas

CAPACITACIÓN EN EL USO DE LA TECNOLOGÍA APLICADA (67%)

NIST SP 800-50

TRABAJA A UN NIVEL ESTRATÉGICO SUPERIOR CÓMO CONSTRUIR UN PROGRAMA DE CONCIENTIZACIÓN Y CAPACITACIÓN



NIST SP 800-16

NIVEL TÁCTICO MÁS BAJO, DESCRIBIENDO UN ENFOQUE PARA LA CAPACITACIÓN EN SEGURIDAD BASADA EN ROLES



PROGRAMA DE SENSIBILIZACIÓN

Concientizar no es capacitar

El propósito de la concientización es simplemente centrar la atención en la seguridad.

OBJETIVOS DE LA CONCIENTIZACIÓN

- ▶ Sensibilizar al personal sobre sus responsabilidades en materia de seguridad de la información
- ▶ Planificarse teniendo en cuenta las funciones del personal de la organización, incluido el personal interno y externo
- ▶ Programarse a lo largo del tiempo y regularmente
- ▶ Basarse en las lecciones aprendidas de los incidentes de seguridad de la información.
- ▶ Identificar, preparar e implementar un plan de capacitación apropiado para los equipos técnicos
- ▶ Es importante no solo centrarse en el "qué" y el "cómo", sino también en el "por qué"

PRIORIZACIÓN

- ▶ **Disponibilidad de material/recursos:** las iniciativas clave en el plan se pueden programar con anticipación.
- ▶ **Rol e impacto organizacional:** abordar como prioridad en términos de rol organizacional y riesgos.
- ▶ **Estado de cumplimiento actual:** observar las principales brechas en el programa de concientización y capacitación y enfocarse en áreas deficientes para una implementación temprana.
- ▶ **Dependencias críticas por proyecto:** si hay proyectos que dependen de un segmento de capacitación en seguridad para preparar los requisitos necesarios para el sistema en cuestión (p. ej., nuevo sistema operativo, multifactor de autenticación, proyectos de IT)

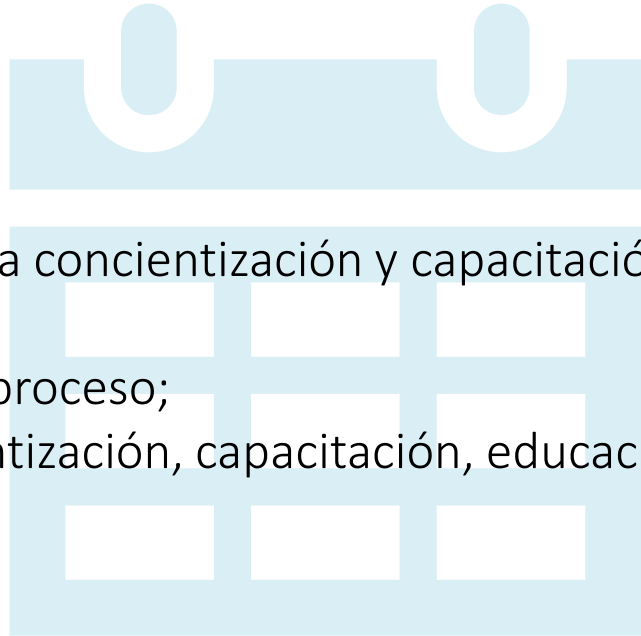
FUENTES DE TEMAS A ABORDAR

- ▶ Avisos por correo electrónico
- ▶ Sitios web de noticias diarias sobre ciberseguridad
- ▶ Publicaciones periódicas especializadas
- ▶ La política de seguridad de la información
- ▶ La gestión de proyectos, riesgos, incidentes y cambios
- ▶ Las revisiones de programas, auditorías internas, las revisiones de programas de controles internos, las autoevaluaciones y las verificaciones o auditorías externas.

PROGRAMA DE SENSIBILIZACIÓN

Elementos que componen la estrategia:

- ▶ Marco regulatorio existente que requiere que se lleve a cabo la concientización y capacitación;
- ▶ Alcance del programa de sensibilización y formación;
- ▶ Roles y responsabilidades del personal que debe gestionar el proceso;
- ▶ Metas a lograr para cada aspecto del programa (p. ej., concientización, capacitación, educación, desarrollo profesional [certificación]);
- ▶ Audiencias objetivo para cada aspecto del programa;
- ▶ Cursos o materiales obligatorios;
- ▶ Objetivos de aprendizaje para cada aspecto del programa;
- ▶ Temas a tratar en cada sesión o curso;
- ▶ Métodos de implementación que se utilizarán para cada aspecto del programa;
- ▶ Documentación, retroalimentación y evidencia de aprendizaje para cada aspecto del programa;
- ▶ Evaluación y actualización de material para cada aspecto del programa; y
- ▶ Frecuencia con la que cada audiencia objetivo debe estar expuesta al material



CONTROL 6.3 ISO/IEC 27002:2022 | SENSIBILIZACIÓN, EDUCACIÓN Y FORMACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Tipo de control	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operativas	Dominios de seguridad
Preventivo	Confidencialidad, Integridad, Disponibilidad	Proteger	Seguridad de los recursos humanos	Gobernanza y entorno

ELEMENTOS DE EVALUACIÓN

Finalidad — medir	Datos necesarios para la medición	Requerido para planificar evaluaciones	Niveles de evaluación / Tipo de herramienta de evaluación
Satisfacción del alumno	<ul style="list-style-type: none"> Datos para evaluar las condiciones de aprendizaje y la evaluación subjetiva del aprendizaje de los estudiantes 	Objetivos de comportamiento escritos: <ul style="list-style-type: none"> Condiciones de actividad Actividad a realizar Nivel de éxito 	Nivel 1 - Evaluaciones de fin de curso <ul style="list-style-type: none"> Formularios con respuestas a escala “de acuerdo” o en “desacuerdo” (escala Likert)
Eficacia del aprendizaje/enseñanza (Lo que un estudiante ha aprendido)	<ul style="list-style-type: none"> Datos para medir objetivamente cuánto conocimiento / habilidad se transmitió al alumno 	Objetivos de comportamiento escritos: <ul style="list-style-type: none"> Condiciones de actividad Actividad a realizar Nivel de éxito 	Nivel 2 - Pruebas objetivas de comportamiento Pre-prueba/post-prueba <ul style="list-style-type: none"> Prueba de rendimiento (por ejemplo, estudio de caso) Preguntas de ensayo
Efectividad en el desempeño laboral (Patrón de resultados de comportamiento de los estudiantes)	<ul style="list-style-type: none"> Datos de tendencias para la mejora de los formadores 	Pasos identificados para la recopilación, evaluación y extrapolación de datos de tendencias	Nivel 3 - Habilidades de transferencia de trabajo <ul style="list-style-type: none"> Evaluación del supervisor : cuestionario estructurado para el supervisor para la comparación de habilidades "antes y después"
Efectividad del programa (Valor del evento de capacitación en comparación con otras opciones)	<ul style="list-style-type: none"> Datos de retorno de la inversión para una asignación óptima de recursos 	Metas relacionadas con la misión vinculadas a objetivos de aprendizaje explícitos	Nivel 4 - Beneficio organizacional <ul style="list-style-type: none"> Entrevistas de seguimiento estructuradas con estudiantes, supervisores y colegas Comparación de los resultados de los estudiantes (antes y después de la formación) Evaluación comparativa



GESTIÓN DEL CAMBIO Y CIBERSEGURIDAD

A hand in a striped shirt sleeve holds a glowing lightbulb. Inside the lightbulb, several interlocking gears are visible, with one gear being a vibrant blue. The background is a soft, out-of-focus grey.

Incremento de ciber-riesgos



Incremento de requerimientos hacia la gente



“A mi no me va a pasar eso”

“Esto no es mi responsabilidad”

“No tengo tiempo para participar de la capacitación”

“¿Cómo no se dio cuenta que se trataba de una estafa?”

ROL DE GDC

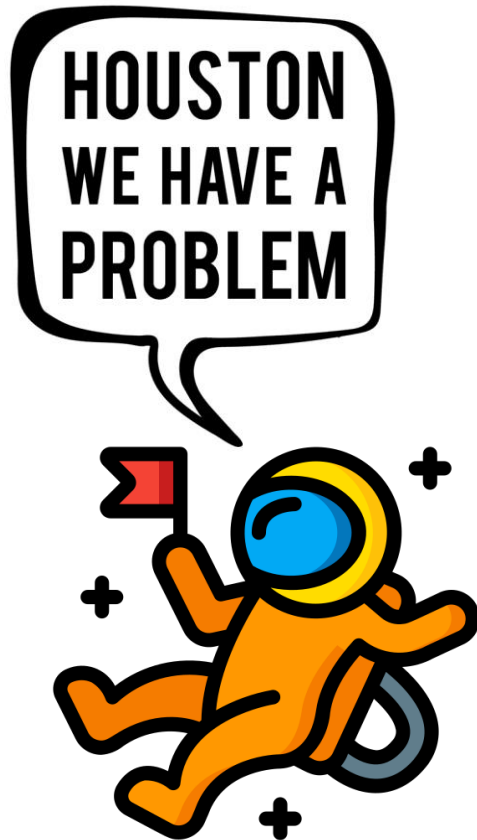
Generar conciencia / cambio de mindset

Le puede pasar a cualquiera tanto a nivel laboral como personal

Todos somos corresponsables de la Seguridad de la organización

Entendimiento de la necesidad para otorgarle tiempo a las acciones propuestas

Necesitamos que la gente haga algo diferente...
pero ...



El problema con el cambio es que la gente que lleva tiempo haciendo las cosas de una manera. No les gusta que de repente les digan que deben hacer las cosas de otra forma, en un momento en que en general no se lo esperan. Hoy, una persona promedio diría: *“tengo todos estos problemas, y ahora esto!”*



“A la mayoría de los cerebros no les gusta cambiar. Les gusta lo constante, los hábitos, la rutina. porque este órgano se dedica a una sola cosa: a sobrevivir”

- LOS PROCESOS DE CAMBIO VIENEN ACOMPAÑADOS DE ...



Incertidumbre

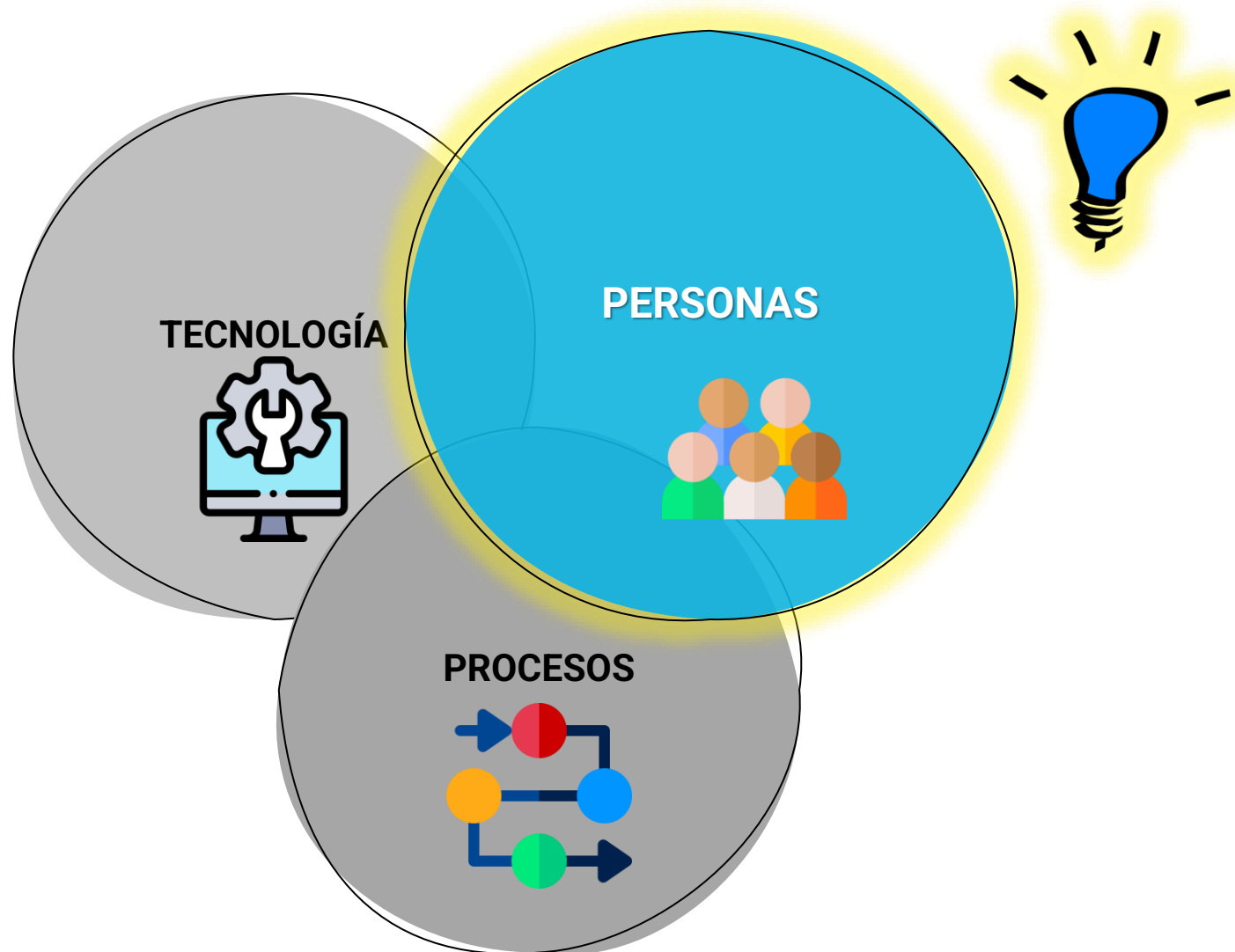


Juegos de poder



Comunicación deficiente

- VARIABLES ORGANIZACIONALES



■ OBJETIVOS DE LA GESTIÓN DEL CAMBIO



CONCIENTIZACIÓN

Razones para el cambio.
Cambio de mirada.
Sensibilización.



INVOLUCRAMIENTO

Ser parte de la solución.
Responsables de las
vulnerabilidades que
acceden en sus sistemas.



**ADOPCIÓN NUEVO
MINDSET**

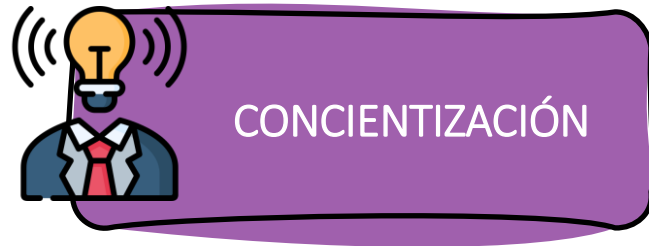
Nuevas creencias
respecto a la
ciberseguridad



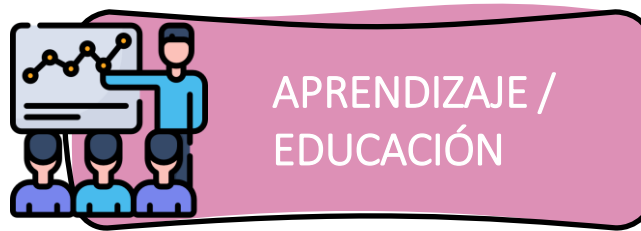
**NUEVOS HÁBITOS
SEGUROS**

Incorporar hábitos
seguros para prevención
de ciberataques

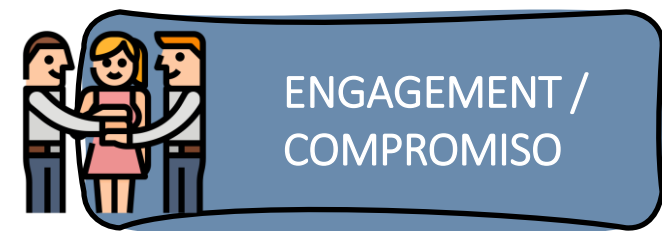
■ PROCESO DE CAMBIO



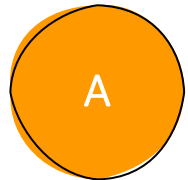
Acerca de la importancia de la Ciberseguridad. Riesgos. Cambio de creencias



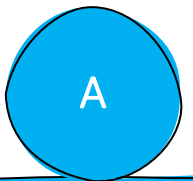
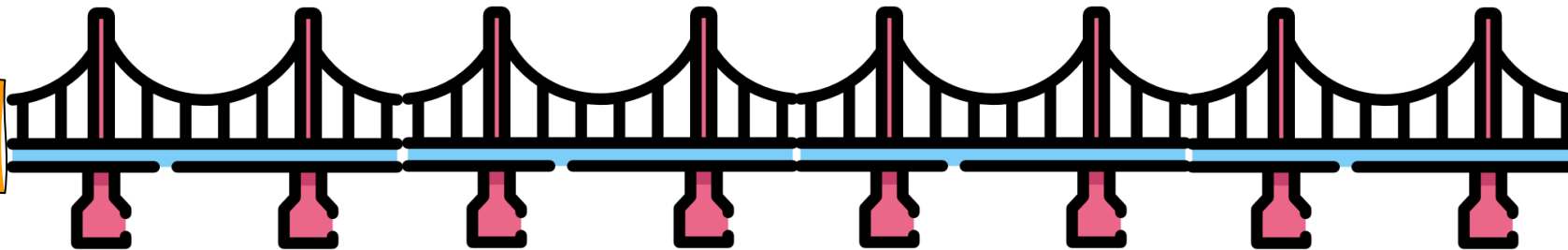
Conocimiento y habilidades para saber como actuar. Cambio de hábitos.



Adopción y compromiso con el cambio. Apropiación de hábitos.



CULTURA ACTUAL

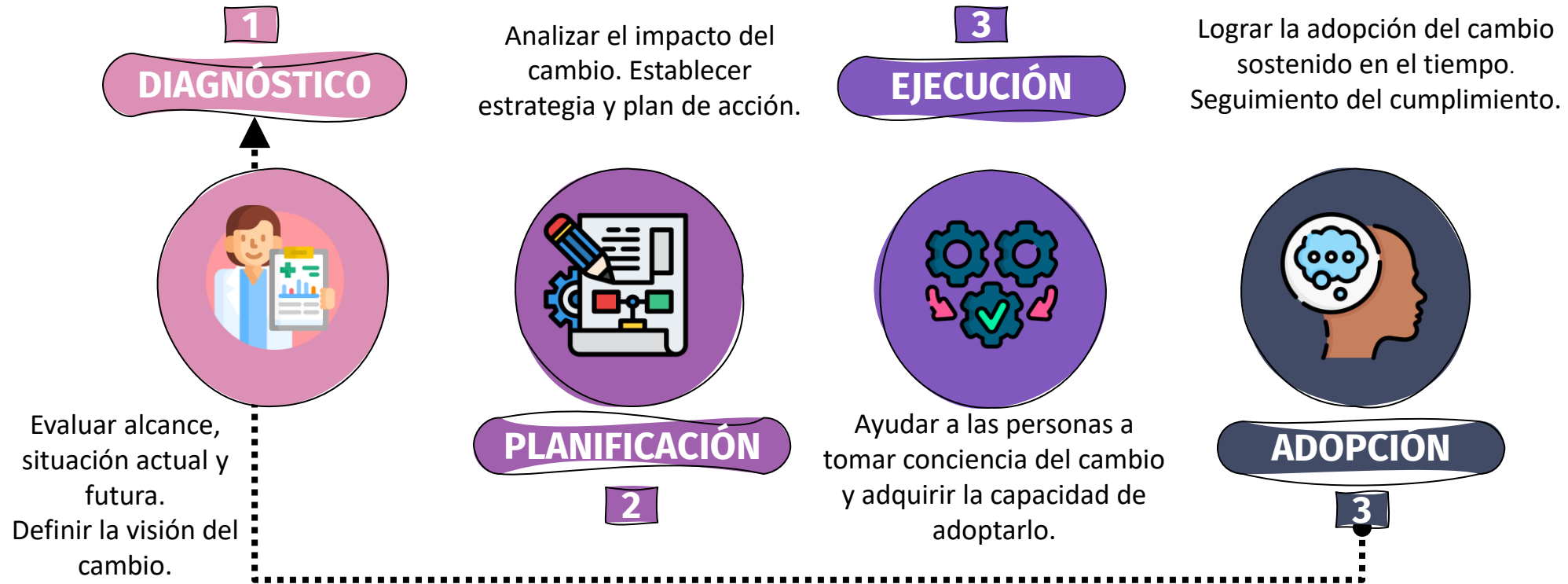


CULTURA DESEADA

■ COMO LO HACEMOS



■ FASES EL PROCESO DE CAMBIO



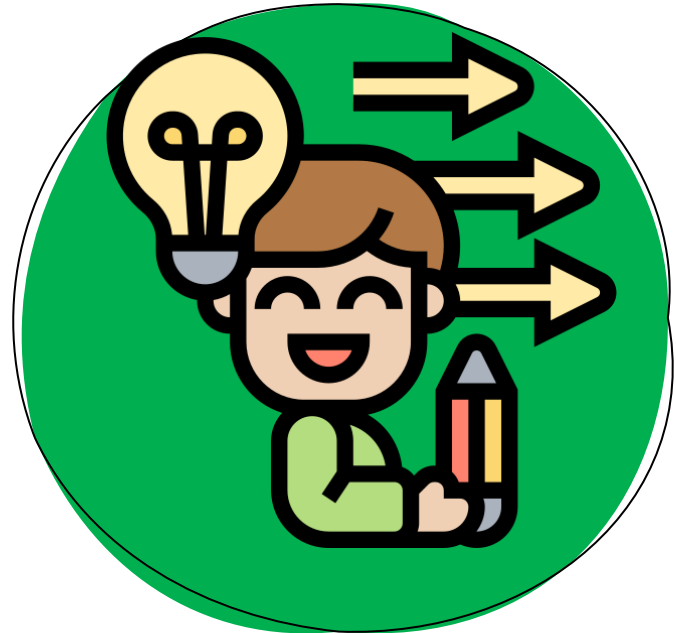
“Debemos hacer ver a la ciberseguridad no como destino final sino como viaje”

▪ LO QUE LOGRAMOS TRABAJANDO CON LAS PERSONAS



- Que se sientan responsables de la ciberseguridad de la Organización
- Que conozcan las formas de estar prevenidos frente a un ciberataque
- Que adopten hábitos que los mantengan alertas frente a posibles ataques
- Que se encuentran permanentemente comunicados
- Que adopten un rol de líderes comprometidos con una cultura Cibersegura

- UN MÉTODO QUE UTILIZAMOS QUE SUELE DAR MUY BUENOS RESULTADOS



1. Comunica claramente que no cambiar es muy peligroso y crea un sentido de urgencia.
2. Involucra al equipo de trabajo (quienes deben cambiar) en la toma de decisiones y en lo posible adóptalas. Identifica quién es quién.
3. Minimiza la incertidumbre. No dejes vacíos de información.
4. Celebra los éxitos durante el camino hacia las metas. Lo merecen.
5. Explica los motivos del cambio, en qué beneficiará y hazlo muy frecuentemente.
6. Lidera el cambio
7. Captura todas las reacciones
8. No olvides que quienes cambian son personas
9. Entusiasma a la gente

A professional business meeting scene. Two men in suits are shaking hands over a table. The table is covered with various business documents, including spreadsheets, charts, a calculator, a smartphone, and a tablet displaying a bar chart. The background is a blurred office setting with a window.

GESTIÓN DEL CONOCIMIENTO Y CULTURA ORGANIZACIONAL

CONCLUSIONES

Las organizaciones deben determinar una estrategia apropiada para la concientización y capacitación en ciberseguridad basadas en:

- ▶ Sus creencias y cultura interna, para delinear un programa que le asegure efectividad y eficiencia en la madurez de su organización
- ▶ Los requisitos de cumplimiento y seguridad específicos de su negocio y de los sistemas e información a los que el personal tiene acceso.
- ▶ Las funciones y responsabilidades asignadas a las personas de su organización.

SERVICIOS DE CONCIENTIZACIÓN Y PLAN DE APRENDIZAJE LATAM

CIBERKNOW

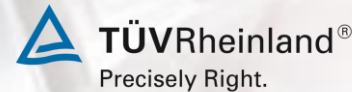
SERVICIOS PARA LA GESTIÓN DEL CONOCIMIENTO Y PROTECCIÓN BASADA EN CONCIENTIZACIÓN



- ▶ Estrategia del programa anual de concientización y capacitación
- ▶ Diseño o customización de contenido
- ▶ Administración de la herramienta y calendarización de actividades
- ▶ Estadísticas e informes de resultado de campañas educativas, phishing y ransomware
- ▶ Planes de remediación y mitigación de riesgos



Cursos de certificación internacional



CHANGE MANAGEMENT

- ▶ Análisis del impacto del cambio a implementar
- ▶ Estrategias de Gestión del Cambio y acciones
- ▶ Acompañamiento en la implementación de la estrategia, acciones y cumplimiento
- ▶ Adopción del Cambio
- ▶ Generar consciencia sobre la necesidad y urgencia del cambio
- ▶ Promover la sustentabilidad del cambio
- ▶ Entrega de Feedback
- ▶ Desarrollo del plan de mejora continua
- ▶ Indicadores de éxito

EVALUACIÓN Y AUDITORÍAS

NIST
CLOUD
BIA
ISO20000
BCRA

SANS
SWIFT Security Framework
GOBIERNO, RIESGOS Y CUMPLIMIENTO

BYOD

COBIT5

GDPR

IoT

CIBERSEGURIDAD

PRIVACIDAD DE DATOS
GESTIÓN DE LA CONTINUIDAD

DRP

CONSULTORÍA TI
COMPLIANCE

ISO27301

PCI-DSS

ISO27001 GESTIÓN DE INCIDENTES

COSO ISAE3402 ERP

ITIL

BCP

ISO38500

SERVICIOS GESTIONADOS

