Auditar el impacto del COVID-19 desde la perspectiva de los Riesgos Tecnológicos

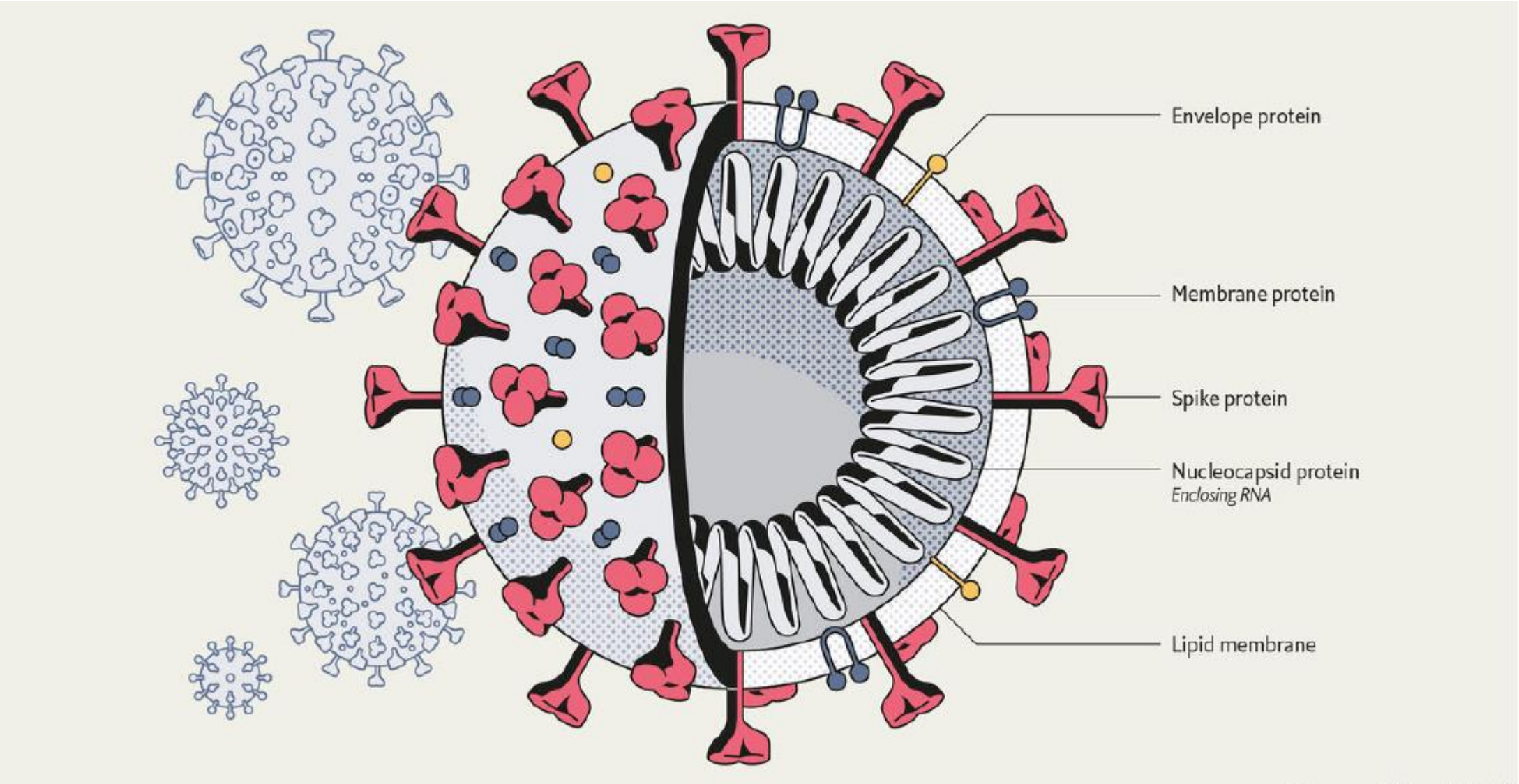
Manuel Mendiola Antona
CIA, CRMA, CISA, CISM, CGEIT, CRISC
Responsable Riesgos Tecnológicos
manuel.mendiola@pkf-attest.es

Instituto de Auditores Internos de España

PKF Attest

15 de abril de 2020

Introducción



Fuente: The Economist, 14 de marzo de 2020

Introducción

Objetivo de este Webinar

Ofrecer pautas para evaluar si el impacto tecnológico, derivado de COVID-19, se está gestionando adecuadamente

Riesgos derivados de COVID-19 relacionados con la tecnología

Un posible enfoque de auditoría

Ejemplos de recursos y guías metodológicas

Introducción

Algunos handicap

Disponibilidad del auditado

Capacidad de ejecutar pruebas

Limitaciones a la observación

Acceso a evidencias

I. Riesgos específicos COVID-19

Principales riesgos

Fuente: https://www.osi.es

Incapacidad de trabajar con normalidad / Interrupción del negocio

Fugas de información

Funcionamiento incorrecto de procesos de negocio / errores de integridad

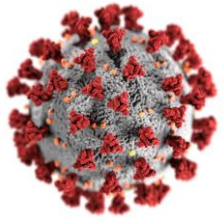
Fraude / Chantaje

Incumplimiento normativo

Impacto en la estrategia de la organización

II. Posible enfoque de auditoría

Ámbitos de evaluación



A. Continuidad de negocio

B. Ciberseguridad

C. Infraestructura tecnológica

D. Control interno

E. Auditoría interna

A. Continuidad de negocio

1. Plan de continuidad de negocio

A. Continuidad de negocio

2. Teletrabajo

Procedimientos

Equipos (Corporativos vs Particulares / BYOD)

Canales de apoyo

Mecanismos de supervisión

Evaluación de la política adoptada

A. Continuidad de negocio

3. Procesos

Dependencia de:

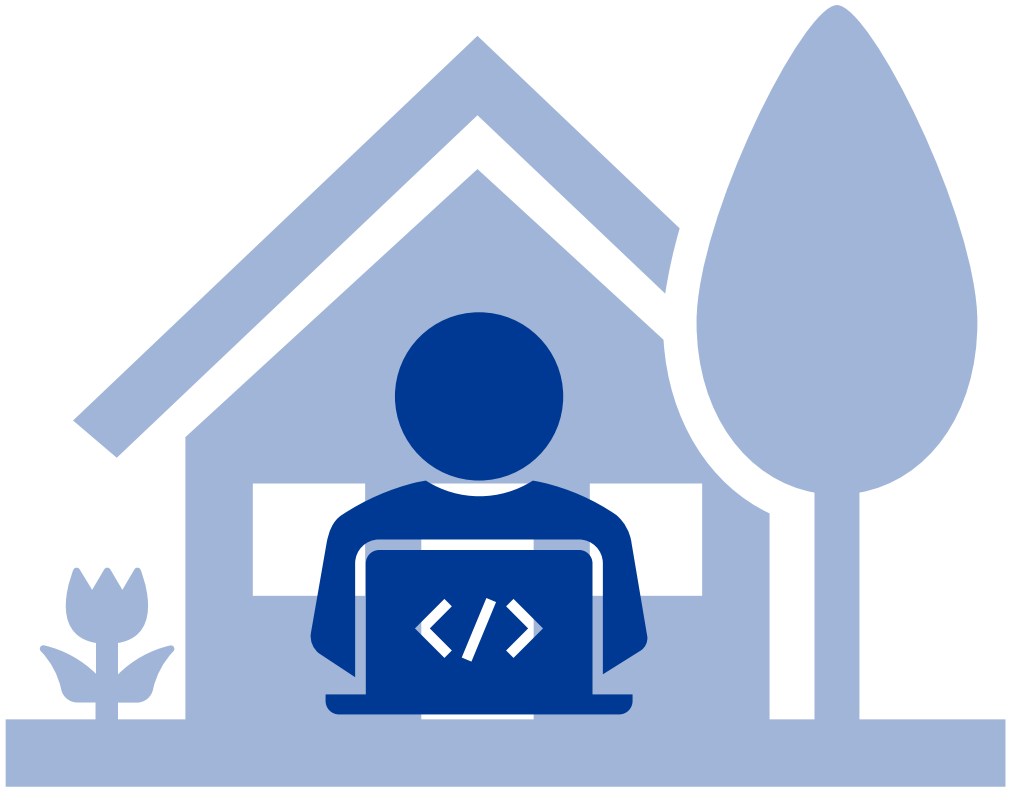
Recursos

Proveedores

A. Continuidad de negocio

3. Procesos

¿Se pueden ejecutar de forma remota?



A. Continuidad de negocio

3. Procesos

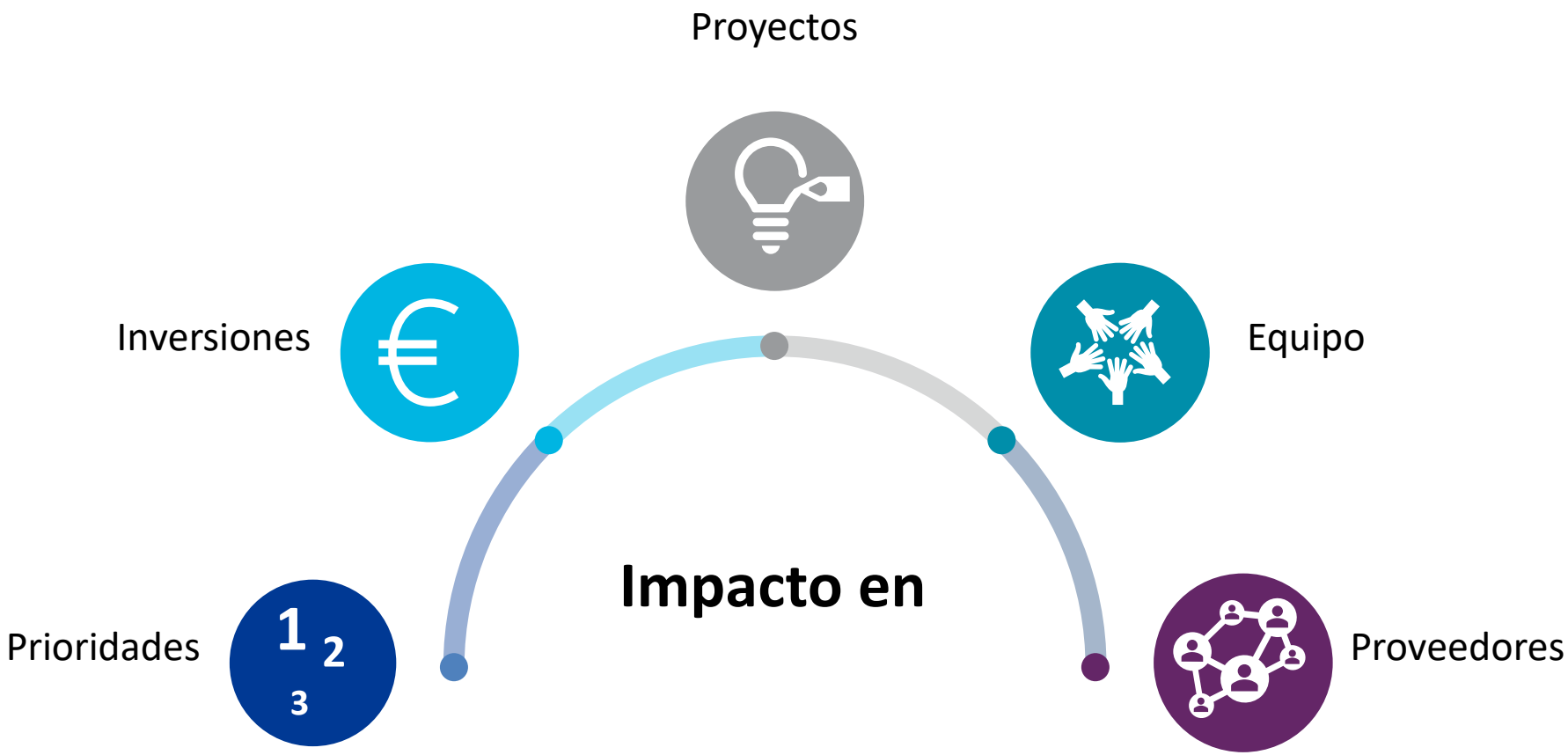
Digitalización

A. Continuidad de negocio

4. Objetivos y planificación

A. Continuidad de negocio

4. Objetivos y planificación

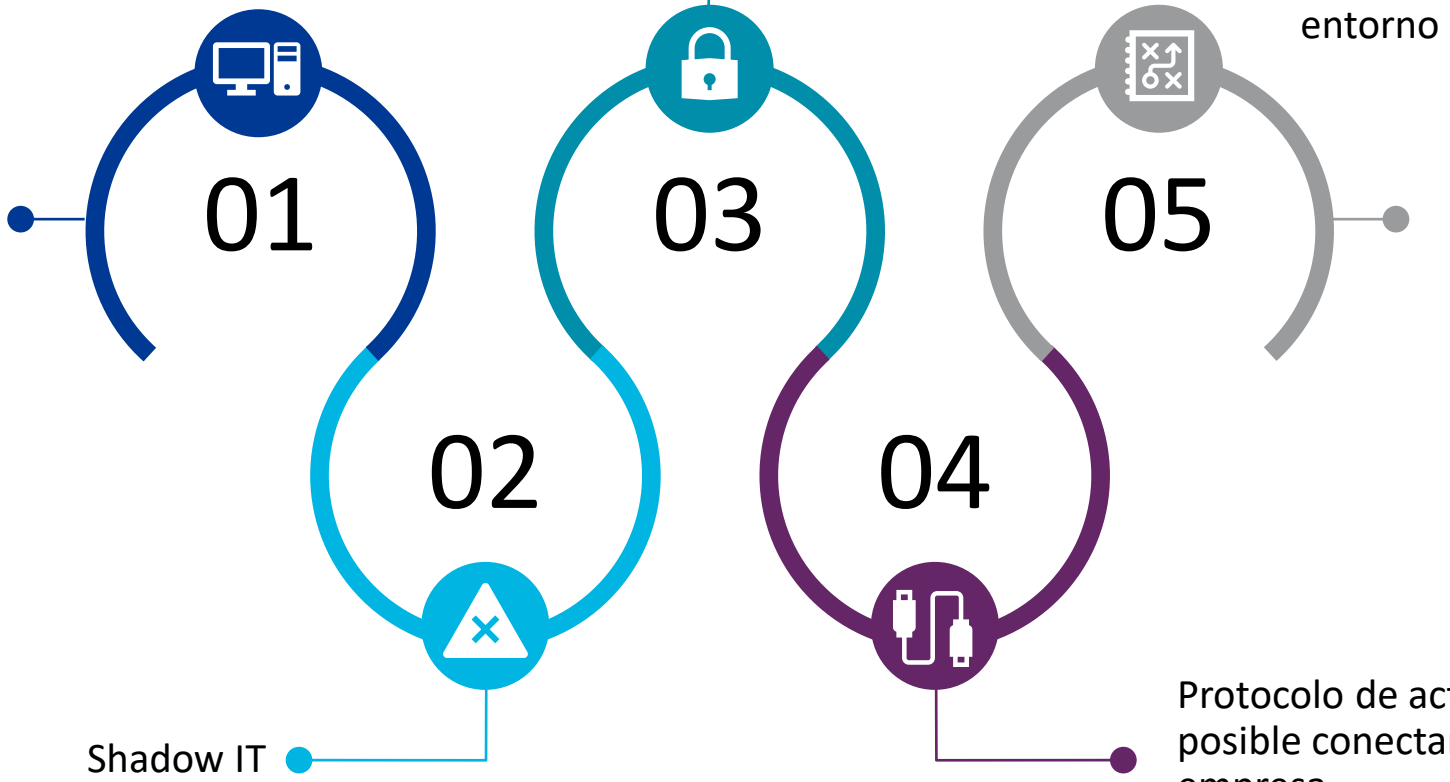


Plan de acción post-crisis

A. Continuidad de negocio

5. Copias de seguridad

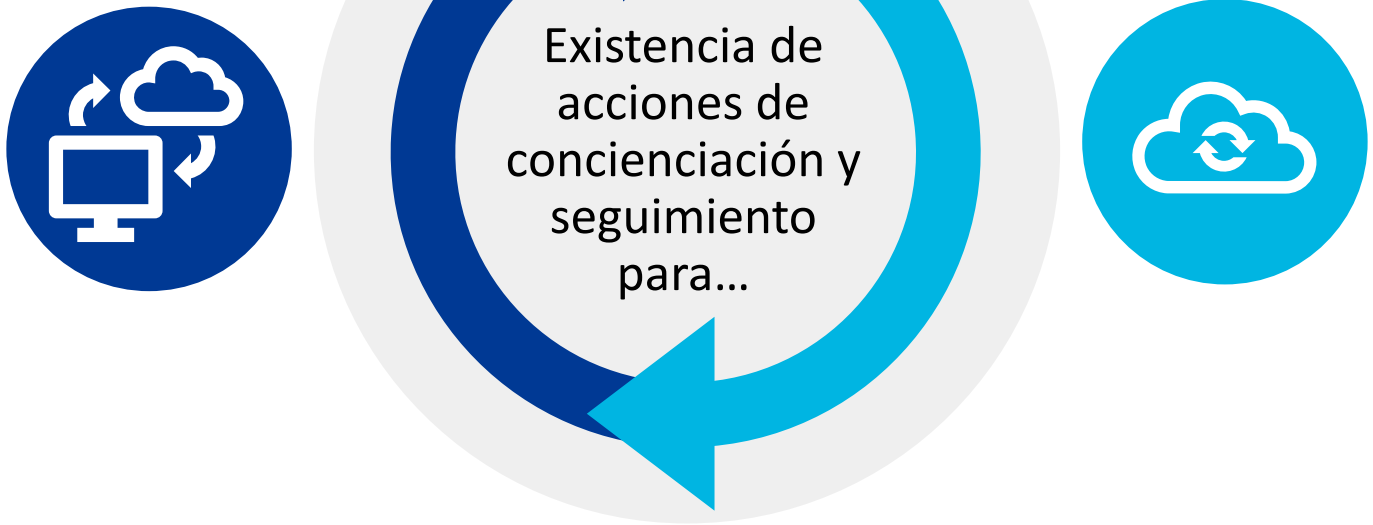
Revisar si la política de back-up considera:



A. Continuidad de negocio

5. Copias de seguridad

Que se trabaje en los servidores de la empresa y no en local



No utilizar servicios de backup en la nube *(no corporativos)*

A. Continuidad de negocio

6. Ciberseguros

¿Lo necesitamos?

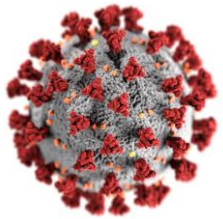
¿Disponemos de alguno?

¿Contempla situaciones derivadas de una pandemia?

¿Sus coberturas son suficientes? ¿Hay ofertas mejores?

¿Qué obligaciones supone?

Ámbitos de evaluación



A. Continuidad de negocio

B. Ciberseguridad

C. Infraestructura tecnológica

D. Control interno

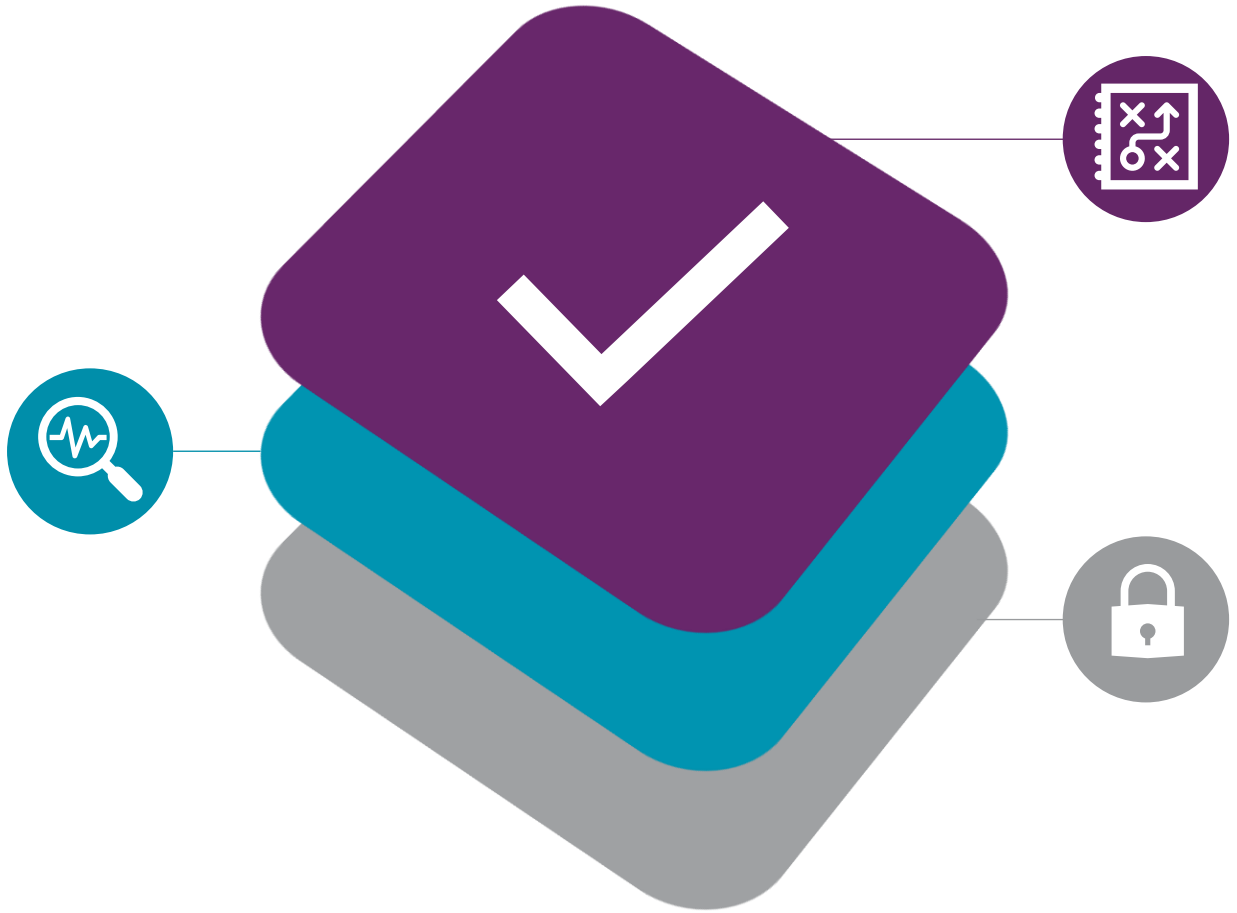
E. Auditoría interna

B. Ciberseguridad

1. Estrategia

¿Cómo se está afrontando? ¿Qué se ha hecho hasta el momento?

Controles establecidos para mitigar riesgos derivados (o incrementados) por COVID-19



Planes de acción

Gestión de posibles incidentes de seguridad y su impacto…

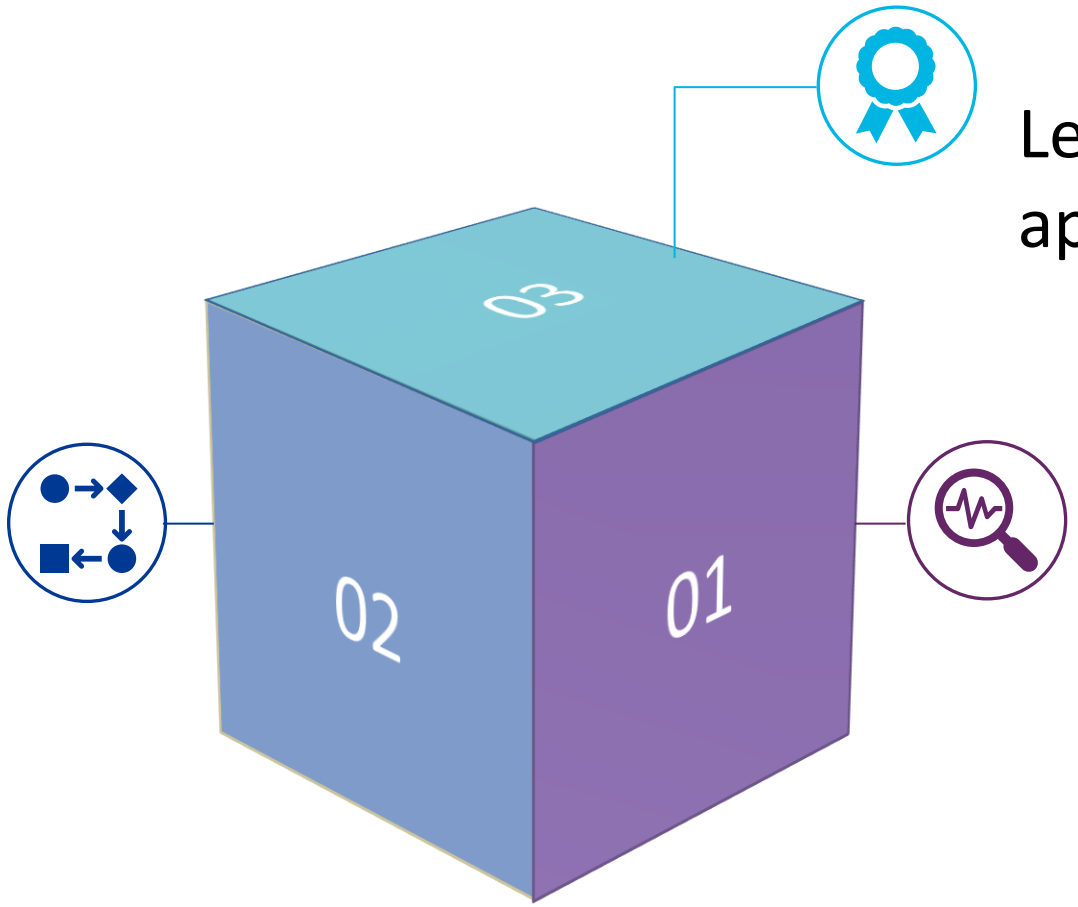
B. Ciberseguridad

2. Formación / concienciación de usuarios

¿Se está sensibilizando al personal sobre los riesgos del teletrabajo?

B. Ciberseguridad

3. Análisis y gestión de riesgos



Lecciones aprendidas

Nuevos escenarios

Reevaluación de riesgos

B. Ciberseguridad

4. Controles y procedimientos

- Política de seguridad de la información
- Gestión de identidades y credenciales
- Sistemas de autenticación. Autenticación multifactor
- Canales de comunicación (email, videoconferencia…)
- Gestión y control de accesos
- Seguridad física
- Monitorización. Seguimiento Shadow IT
- Gestión de eventos
- Segregación de redes
- Configuración de dispositivos móviles / políticas BYOD
- Parches y actualización sistemas acceso remoto
- Protección de la integridad y confidencialidad. Cifrado de datos
- Mecanismos para prevenir ransomware, phising, virus, robos de información…

B. Ciberseguridad

5. Cumplimiento RGPD / LOPDGDD

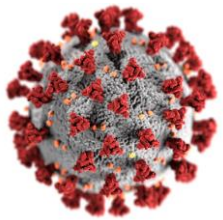
Protocolo notificación brechas de seguridad

Protección de datos de empleados

Ámbitos de evaluación

A. Continuidad de negocio

B. Ciberseguridad



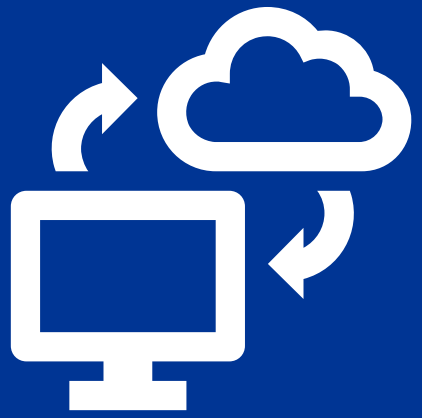
C. Infraestructura tecnológica

D. Control interno

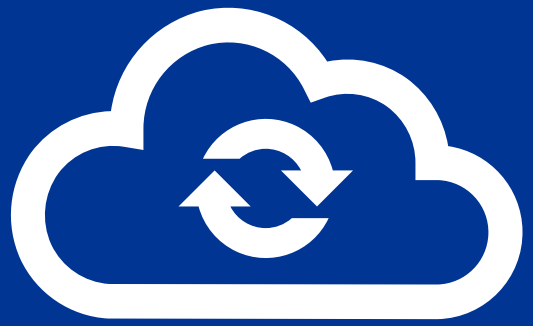
E. Auditoría interna

C. Infraestructura tecnológica

1. Capacidad y dimensionamiento



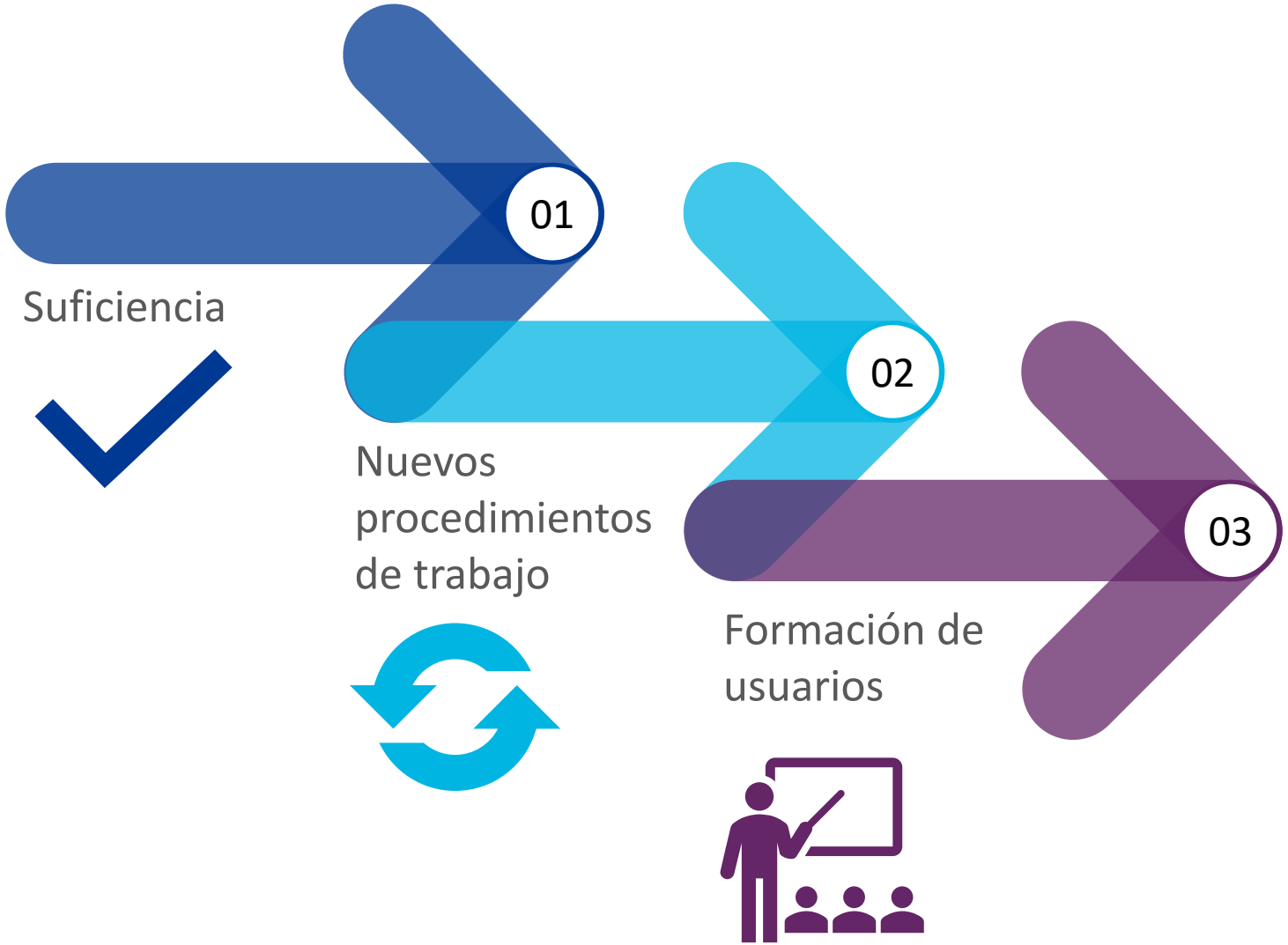
Acceso remoto



Carga de trabajo (propia / SaaS)

C. Infraestructura tecnológica

2. Herramientas colaborativas

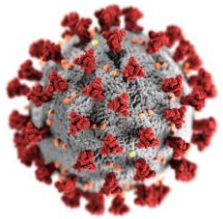


Ámbitos de evaluación

A. Continuidad de negocio

B. Ciberseguridad

C. Infraestructura tecnológica



D. Control interno

E. Auditoría interna

D. Control interno

1. Impacto

¿Cómo afecta al control interno?

D. Control interno

2. Oportunidad de mejora

Innovación y digitalización en los sistemas de gestión del control interno

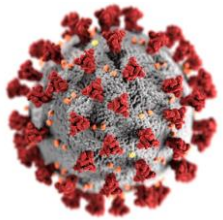
Ámbitos de evaluación

A. Continuidad de negocio

B. Ciberseguridad

C. Infraestructura tecnológica

D. Control interno



E. Auditoría interna

E. Auditoría interna

1. Plan anual de auditoría

2010 – Planificación

El director de auditoría interna debe establecer un plan basado en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dicho plan deberá ser consistente con las metas de la organización.

Fuentes: Marco Internacional para la Práctica Profesional de la auditoría interna
https://marmolblum.wordpress.com/2017/01/23/claves-del-plan-estrategico-de-auditoria-basado-en-riesgo/

E. Auditoría interna

2. Capacidad de auditar a distancia

Evolución tecnológica de la auditoría

E. Auditoría interna

2. Capacidad de auditar a distancia

RIESGO AUDITORIA A DISTANCIA		RIESGO ÁREA AUDITADA		RIESGO ÁREA AUDITORÍA INTERNA
Riesgo derivado de realizar la auditoria de forma remota en vez de presencial	=	Riesgo asociado a que los sistemas, procesos y personal del área auditada no estén preparados para una auditoria remota	+	Riesgo asociado a que los sistemas, procesos y personal de auditoria interna no estén preparados para conducir una auditoría remota

Auditoría a distancia

E. Auditoría interna

2. Capacidad de auditar a distancia

Sistemas

- Grado de digitalización
- Capacidad de acceso
- Herramientas de colaboración

Procesos

- Controles automáticos
- Papeles electrónicos
- Automatización pruebas / Continua / Data Analytics

Recursos

- Conocimientos técnicos
- Resilencia

Auditoría a distancia

E. Auditoría interna

2. Capacidad de auditar a distancia

Galvanize

IDEA
Software para Análisis de Datos

ARBUTUS

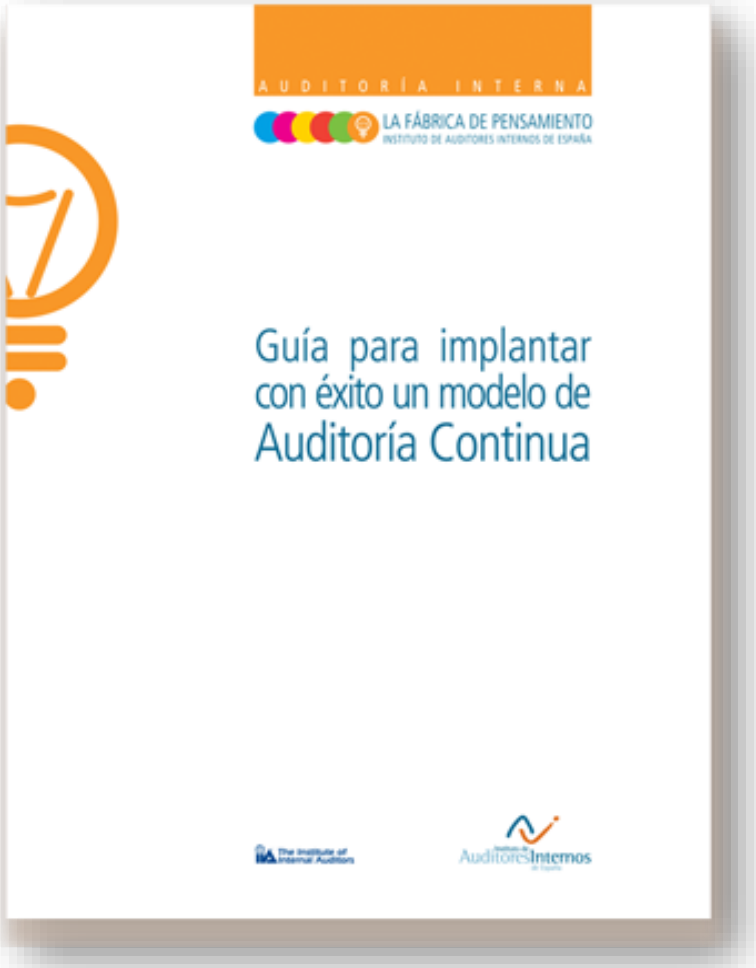
sas

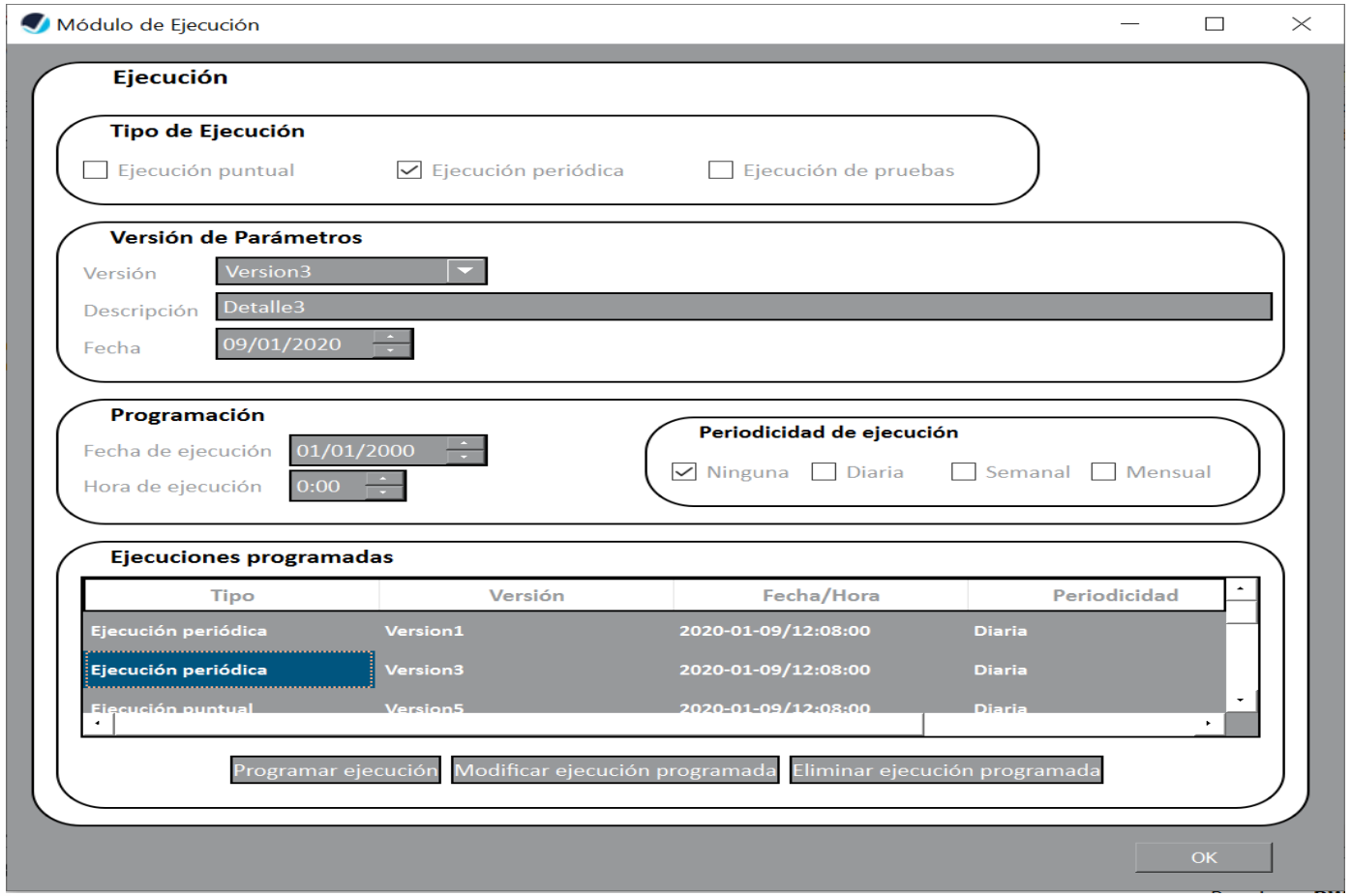
alteryx

Auditoría tecnológicamente avanzada

E. Auditoría interna

2. Capacidad de auditar a distancia





https://auditoresinternos.es/uploads/media_items/f%C3%A1bricaaudcontinuaweb.original.pdf

Auditoría continua

E. Auditoría interna

2. Capacidad de auditar a distancia

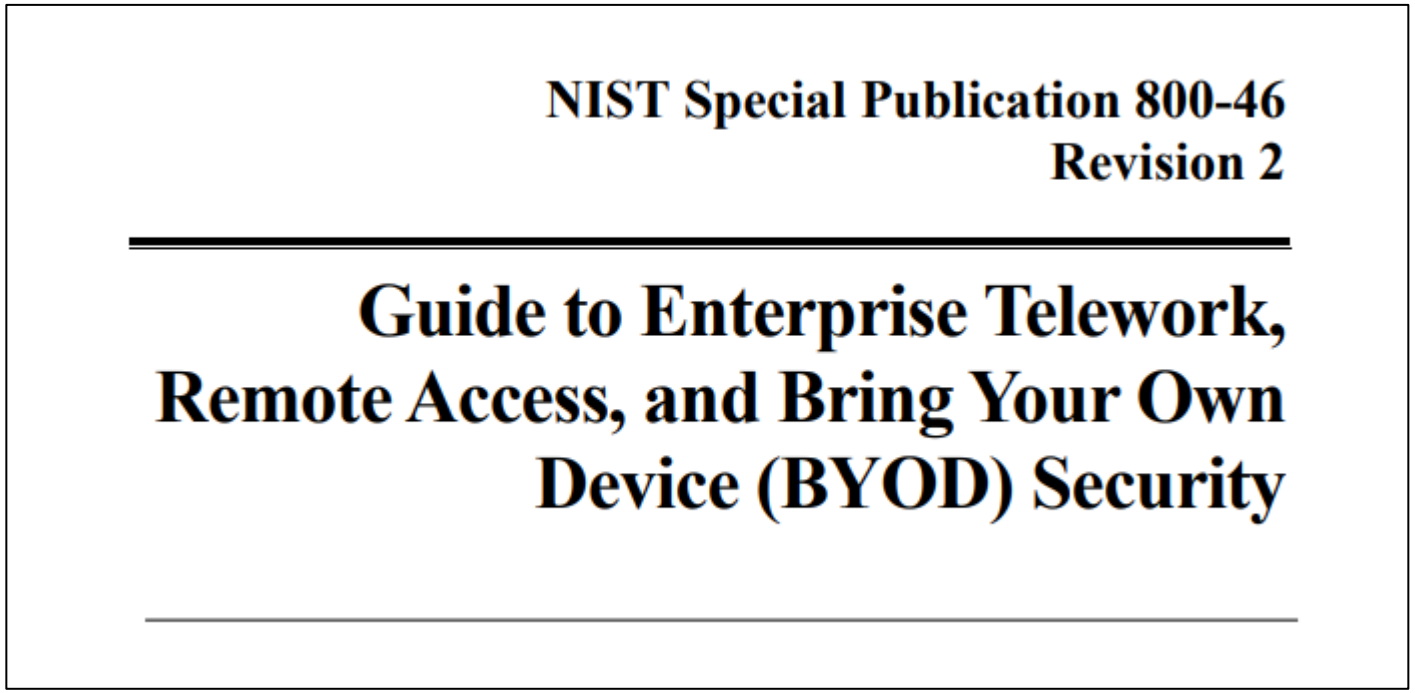
Data Analytics

III. Marcos metodológicos y otros recursos

Ejemplos

NIST SP 800-46 Revision 2

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf



NIST Special Publication 800-46
Revision 2

Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Ejemplos

CiberCOVID19

https://www.ccn-cert.cni.es/cibercovid19

Concienciación

Teletrabajo

Alertas y avisos

Indicadores de compromiso

Formación

Informes

Ejemplos

CCN-CERT BP/18

https://www.ccn-cert.cni.es/cibercovid19

Ejemplos

Protección de datos y coronavirus

https://www.aepd.es/es/areas-de-actuacion/proteccion-datos-y-coronavirus

Ultima modificación: 7 de Abril de 2020

Protección de datos y coronavirus

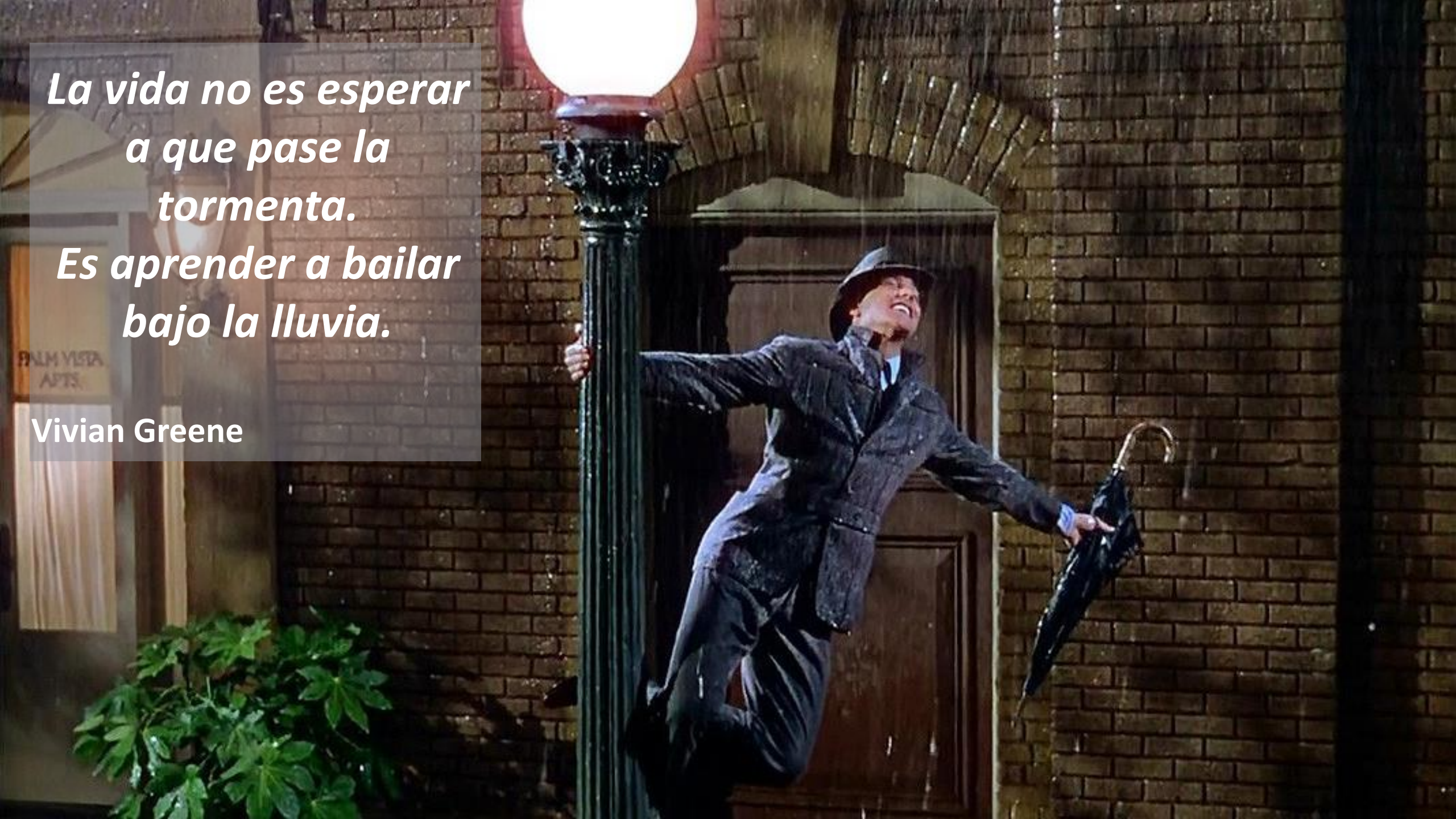
Ante la situación de emergencia de salud pública derivada de la extensión del coronavirus, la Agencia Española de Protección de Datos ha elaborado varios recursos en relación con el COVID-19 para dar respuesta a las dudas que han ido surgiendo en estos días. Esta sección aglutina todos estos recursos publicados por la AEPD.

- Informe sobre los tratamientos de datos en relación con el COVID-19 (english version)
- Nota de prensa (english version)
- Preguntas frecuentes dirigidas tanto a ciudadanos como a empresas y otros sujetos obligados al cumplimiento de la normativa de protección de datos (english version)
- Comunicado de la AEPD en relación con webs y apps que ofrecen autoevaluaciones y consejos sobre el coronavirus
- Comunicado de la AEPD sobre apps y webs de autoevaluación del Coronavirus (english version)
- Nota Técnica: Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo
- Blog de la AEPD:
  - Brechas de seguridad: El Top 5 de las medidas técnicas que debes tener en cuenta
  - Notificación de brechas de seguridad de los datos personales durante el estado de alarma (english version)
  - Campañas de phishing sobre el COVID-19

Ejemplos

Protección de datos y coronavirus: Nota técnica

https://www.aepd.es/es/areas-de-actuacion/proteccion-datos-y-coronavirus



La vida no es esperar a que pase la tormenta.
Es aprender a bailar bajo la lluvia.

Vivian Greene

¡¡Gracias!!

Síguenos en

www.auditoresinternos.es

@Auditorinterno

Instituto de Auditores Internos de España