ESPECIAL

“América Próxima”

DE Tecnología & Sentido Común

AGOSTO
2021

ESPECIAL

"América Próxima"

DE Tecnología & Sentido Común

EQUIPO DIRECTO:
Javier Peris - Piloto
Manuel D. Serrat - Copiloto
Alberto Rodríguez - Equipo Directo
Juan Carlos Muria - Equipo Directo

MICRO-ESPACIOS
Marlon Molina - Es Tendencia
Ricard Martínez - Ojo Al Dato
Catalina Valencia - Ecosistema Emprendedor
Víctor Almonacid - La Nueva Administración
Shirley Villacorta - América Próxima
Fernando Ley - Geo Energía

PUBLICIDAD Y CONTRATACIÓN
Carmen Usagre
carmen.usagre@businessandcompany.com
Teléfono: +34 96 109 44 44

GABINETE JURÍDICO
Jesús López Peláz

ATENCIÓN AL LECTOR
tecnologiaysentidocomun@businessandcompany.com

EDITA
Business, Technology & Best Practices, S.L.

Av. San Onofre, 20
46930-Quart de Poblet (Valencia)
Teléfono: 96 109 44 44
Fax: 96 109 44 45
https://businessandcompany.com
soluciones@businessandcompany.com

SHIRLEY ARISTONDO

Consultor y ejecutiva senior con más de 14 años de experiencia profesional en diversas empresas del sector privado y público del mercado peruano. Ha sido Coordinador Académico y catedrático de la Universidad de Lima en Ciberseguridad, Auditoría de Sistemas y Gestión de Riesgos. Desde el 2017 brinda asesorías profesionales independientes en auditorías SOC 2 tipo 2, exigidas por los reguladores locales y bajo rigurosos estándares de calidad. Desde este año, lidera un emprendimiento local de asesoría y consultoría a empresas que buscan lograr el máximo potencial de sus procesos con premisas éticas, comprometiéndose en la adopción de mejores prácticas que permitan empoderar a sus líneas de control a través de sus áreas de auditoria de sistemas, ciberseguridad y seguridad de la información.

LinkedIn:
https://www.linkedin.com/in/svillacortaa/

Twitter:
https://twitter.com/svillacortaa

PREPARA A TU ORGANIZACIÓN PARA RETOS FUTUROS CON ITIL® 4

Los avances tecnológicos han transformado la forma en la que adquirimos e interactuamos con bienes y servicios; creando nuevos comportamientos, expectativas y experiencias.
Pero ¿estás preparado para esos retos?

El mundialmente reconocido ITIL 4, es el método de gestión de servicios que proporciona, a organizaciones y profesionales, un modelo operativo digital / de TI de extremo a extremo para la entrega y operación de productos y servicios habilitados por tecnología y permite a los equipos de TI continuar desempeñando un papel crucial en una estrategia de negocios más amplia.

¿Quieres conocer más?

AXELOS.com/ITIL4-futuro
(Página en inglés)

ESPECIAL AGOSTO 2021

índice
DE CONTENIDOS

https://tecnologiaysentidocomun.com

Índice de Contenidos

#TYSC

Recomendaciones en tiempos de incertidumbre para la tercera línea de control

La pandemia es un caso de estudio “en vivo” que ha traído aprendizaje en tiempo real sobre la A nivel mundial, la línea de tiempo que han vivido las empresas en los últimos seis meses la resumo como una etapa de reinvención y toma de decisión acelerada que ha tenido como principal objetivo contener los efectos disruptivos de un problema cuya dimensión no termina de definirse. El efecto de COVID-19 en la sociedad, la economía, la salud, la política y el desarrollo empresarial sigue capturando nuestra atención, y todos los días tenemos una radiografía de sus resultados. A veces alentadores, otros días con mensajes que nos indican que aún hay mucho por trabajar.

Tomar decisiones es un arte complejo y es materia de estudio de muchas disciplinas. Su origen y naturaleza está muy ligada a nuestro comportamiento como seres humanos. En el campo de la gestión empresarial, su protagonismo marca el ritmo de la continuidad del negocio, se nutre de la información, es adaptativo y su valor es innegable cuando buscamos mejorar procesos. Y en coronavirus no ha sido la excepción, pero hay que reconocer que se sumaron matices de intensidad junto con puntos de quiebre casi a diario: las empresas planificaron paralizaciones de quince días, pero se extendieron los tiempos, sectores que de un momento a otro se vieron paralizados con muy pocas opciones de reactivación y otros que cayeron en cuenta que el cierre era la mejor opción.

En este contexto y junto con las vivencias de cada empresa, el rol de la tercera línea de control también fue transformándose y adaptándose a los cambios. Cada día medimos el impacto de las decisiones y trabajamos en adaptar nuestras herramientas al ritmo de la empresa, pero ninguna literatura o formación nos había preparado para este contexto y así que hace dos meses, al iniciar la semana me enfrenté a la siguiente pregunta para mi plan de trabajo: ¿Qué enfoque debemos considerar cuando realicemos las evaluaciones?

CONTINÚA EN PRÓXIMA PÁGINA

PARA BUSCAR RESPUESTA, INICIÉ BÚSQUEDA EN LAS RECOMENDACIONES Y GUÍAS DE LOS INSTITUTOS DE LA PROFESIÓN, CONSULTORAS Y LÍDERES NORMATIVOS. RECOMIENDO QUE PARTAN POR ACÁ, EN CASO AÚN NO HAYAN INICIADO EL PROCESO.

SIN EMBARGO, ALGO FALTABA, UN EXTRA MILE QUE HE COMPARTIDO CON COLEGAS Y HA SERVIDO COMO PUNTO DE APOYO Y SE RESUME EN TRES INICIATIVAS:

1

Tómese un tiempo y haga un reconocimiento de los cambios que impactaron en su empresa.

2

Identifique los factores de incertidumbre sobre el cual se tomaron decisiones

3

Finalmente, ubique las nuevas prioridades en los proyectos

Cibercoherencia y Cibercolaboración

Frente a la pandemia, todos somos ahora parte de una generación que ha vivido un gran evento disruptivo, el cisne negro que no se previó, el cambio que definió una nueva normalidad. No importa la etiqueta de lo que aun vivimos, lo importante es que cada uno podrá compartir una experiencia sea desde la perspectiva personal o profesional. Hoy quisiera compartir con ustedes una lectura que he agrupado en cuatro fases asociadas a la pandemia y cómo cada una de ellas describe ciertas condiciones que también vivimos frente a la gestión de riesgos y la cultura de ciberseguridad en la empresa.

Días antes de que la pandemia fuera confirmada en la región se podía sentir en la atmósfera el inicio de la incertidumbre; y como es usual, la opinión que cada empresa e individuo empezó a forjar sobre la existencia del virus y su impacto cobró diversas posturas de riesgo. Cuando la llegada del virus se hizo más real y los canales interna- cionales de noticias emitían notas sobre cómo la propagación empezaba a extender- se fuera de Asia-Europa, aplicar medidas de cuarentena sonaban drásticas y difíciles de asimilar. Fuimos escépticos. ¡Calles vacías! ¿Cuarentena¡? ¡Vamos!

(FASE 1): POSTURA ESCÉPTICA DE LAS EMPRESAS FRENTE A LOS RIESGOS DE CIBERSEGURIDAD.

Entonces llegó ese día en el que cada uno de nosotros, en diversos momentos y desde diversas ubicaciones (países) en la región, conocíamos del caso 0. Escuchábamos a nuestros mandatarios / presidente y poníamos atención a las medidas que cada uno definía como apropiado: cierre de aero- puertos, cuarentena en casa, uso de mascarillas, entre otros. Vivimos un acelerado diseño de planes de emergencia. Y cada país demostró que el nivel de preparación jugó un rol importante en la capacidad de adaptación al cambio.

(FASE 2): RESILIENCIA Y CAPACIDAD DE CIBERSEGURIDAD.

Ante la inminente e innegable cuarentena, los primeros días escuchamos las pautas de cuidado de manera clara y sencilla: estar en casa, tomar precauciones, lavarse las manos. Voluntad y compromiso para las nuevas reglas. Era indiscutible que todos debíamos colaborar, era para el bien común, para el bien de todos. Por lo menos los primeros días. Y cosas memorables pasaron: todos éramos conscientes del riesgo y la adopción de las medidas fueron tomadas con creatividad y gran efectividad.

(FASE 3): LA ORGANIZACIÓN SE COMPROMETE.

Entonces, a medida que los días pasaron, se trazaron hojas de ruta para la reactivación de actividades en cada país, pero las personas debilitaron su postura frente a las medidas. Un fenómeno interesante empezó a surgir. Las pautas de protección empezaron a ser evaluadas y los comportamientos empezaron a cambiar. Tomemos un ejemplo concreto. El virus existe, es real y el impacto es innegable. No obstante, todos hemos pasado por esa pregunta tentadora de si debemos seguir usando mascarilla para salir o no. ¿Tomaste el riesgo? ¿Qué decidiste? Cualquiera sea la respuesta, lo maravilloso es que este proceso expuso como nuestras decisiones individuales tuvieron impacto en el hogar o comunidad. Y que la postura frente al riesgo tuvo un impacto de valor en la estrategia de sanidad y protección de tu localidad. ¿Y en las empresas? Bueno, la pregunta rondó sobre ¿cuántas medidas de seguridad debían brindar para el retorno? La respuesta: están las que adoptaron medidas de manera proactiva, las que adoptaron medidas en cumplimiento con la ley y un poco más, las que solo habilitaron lo que la ley exigía, los que interpretaron la ley con diversos matices grises y finalmente las que decidieron trasladar el riesgo.

(FASE 4): POSTURAS SEPARADAS GENERAN CONFLICTOS Y AUMENTAN LA PROBABILIDAD DE OCURRENCIA DE LOS CIBER RIESGOS.

CONTINÚA EN PRÓXIMA PÁGINA

Las cuatro fases descritas, tienen muchos elementos sobre los cuales podemos desarrollar aprendizajes en relación con las estrategias de gestión de riesgo y ciberseguridad. Y lo más interesante es que la cadencia y orden en la que se han presentado es única. El principal aprendizaje es que el esfuerzo que desarrollamos las áreas especialistas solo tendrá éxito si el C-Level muestra coherencia, un enfoque colaborativo de compromiso.

En la ciberseguridad creo que todos buscamos estar en la fase 3 de manera continua. El nirvana de los CISO. Pero el terreno empresarial que vivimos es un amplio pareto compuesto por diversos escenarios de "fase 1", "fase 4" o los híbridos entre ambas. Escepticismo y negación de a pesar de las estadísticas, webminars, instancias, comités o mesas de trabajo. Y en fase 04, la interpretación particular que hacen las empresas sobre propuestas transitorias.

No pretendo disertar sobre los marcos, estrategias, herramientas o uso de enfoques que han sido diseñados para llegar a la fase 3 en la implementación de la cultura de ciberseguridad (el éxito de estas va directamente relacionadas a la preparación de los equipos de seguridad y al constante proceso de evangelización que realizamos. Y sin dudar existen casos de éxito) Sin embargo, para aquellas empresas que no están en el estadio de la fase tres, no parece coherente que el C-Level mantenga una postura adversa a la que busca proteger los activos de información. Es primordial que C-Level tenga un enfoque colaborativo frente a la cultura de la ciberseguridad.

Sobre la fase 2, seré breve. En ciberseguridad, su desarrollo se da en escenarios de crisis. Lo que asombra de esta fase, es que las empresas esperan niveles de continuidad y ciber resiliencia que no construyeron previamente. La eficiencia de estos planes está en relación directa con la preparación, diseño e inversión que la empresa haya decidido tomar. Si no se habilitaron recursos y la empresa se transformó sin incorporar la gestión de riesgo de ciberseguridad, el impacto será inminente. Es primordial que C-Level tenga un enfoque coherente frente a lo que autorizó construir como estrategia de soporte.

Ambas condiciones de voluntad, que denomino ciber coherencia y ciber colaboración del CLevel frente a la cultura de ciberseguridad son las piezas que darán sentido y éxito a los programas de ciberseguridad. Así como frente a la pandemia, la postura coherente y colaborativa que cada uno de nosotros tenemos nos acercará a llegar al nivel de protección que requerimos.

más información en:
https://javierperis.com/bpm

Y tú ¿Transformas o Trastornas tu Organización?

Aprende a:

- ✓ Modelar
- ✓ Mejorar
- ✓ Automatizar Procesos de Negocio

Curso Oficial de Certificación en
Gestión de Procesos de Negocio
ISO/IEC 19510
BPM Professional

Si quieres Aprender, Certificarte, Practicar y recibir posteriormente Ayuda para Liderar con Éxito la Transformación Digital en tu Departamento, Startup, Empresa o Administración, no te quede la menor duda de que este es tu Curso y esta es tu Certificación.

Business&Co.®
Business, Technology & Best Practices, S.L.

Errores comunes que dificultan la ejecución exitosa de las estrategias de Ciberseguridad en Latinoamérica

Estamos por cerrar el 2020, y muchas empresas, así como colegas en la región estamos en el proceso de planificación de cara al 2021. Revisamos el camino ejecutado, las estadísticas y resultados bajo un claro objetivo: mejorar y planificar nuestras estrategias. Soy un ferviente creyente de la planificación y sus resultados. Estar preparados para un mejor comienzo es revitalizante para los líderes y sus equipos, en particular este año determinaremos cuánto han madurando nuestros procesos, valoraremos si logramos las metas tantas veces «estresadas» durante esta pandemia, estableceremos trazabi lidad de nuestros progresos e identificamos las desviaciones que afectan el logro de nuestras metas bajo nuevos escenarios de riesgo.
En ciberseguridad, como las buenas prácticas nos recomiendan, una de las fases del planeamiento es evaluar el estado vigente del entorno. Dicha evaluación debe ser realizada tanto con data interna como con data externa (estadísticas, reportes y estudios emitidos del sector y entorno empresarial).Y es producto de la revisión de fuentes externas públicas, que quisiera compartir con ustedes los 3 errores principales que sugiero evitar para asegurar el éxito de las estrategias de ciberseguridad en Latinoamérica:

Error #1:
REALIZAR TRANSFORMACIÓN DIGITAL SIN CONTAR CON UNA CULTURA DE CIBERSEGURIDAD

La cultura de ciberseguridad es «el habilitador» que siempre debe estar presente, porque conecta y alinea de manera armónica a todas las partes de la empresa. Sin embargo, las estadísticas muestran que las empresas en América Latina están dando pasos en la dirección contraria:

- Sólo el 36% de las compañías a nivel global incluye a la ciberseguridad en sus iniciativas empresariales desde la etapa de planificación (22° Encuesta Global de Seguridad de la Información de EY)
- Que se han dado reducciones en los presupuestos de ciberseguridad en casi el 35% de empresas durante la pandemia (Lumu Technologies)
- El 39% de las organizaciones no cuenta con políticas de seguridad (Informe anual ESET Security Report 2020).
- No existe claridad sobre la independencia que requiere la posición del CISO en la empresa.

Los factores que fortalecen una adecuada cultura de ciberseguridad son el desarrollo de políticas, la colocación independiente del responsable de seguridad / ciberseguridad frente a TI, la asignación de recursos y presupuestos, capacitación del personal y asegurar la participación del equipo de ciberseguridad en el desarrollo de los proyectos claves (que este año han sido liderados por proyectos de transformación digital). Es importante que revisemos si estos factores existen en nuestro entorno empresarial. De no estar, es clave que podamos incluirlos en la planificación de ciberseguridad.

Error #2:
NO INCORPORAR EL ANÁLISIS DE CIBERRIESGOS Y SU ENLACE EN LA ESTRATEGIA EMPRESARIAL

No existe rol en el ámbito profesional que no haya escuchado o conozca los términos Transformación Digital, Trabajo Remoto e Innovación Digital. Hemos dado un salto incremental en el desarrollo de sites de e-commerce, digitalización y aplicaciones mobile, y a la par los ciberataques han aumentado significativamente en la región. Sin embargo, las empresas parecen haber priorizado lo urgente y no lo importante, sin haber contemplado el impacto de las decisiones y riesgos tomados. Así, las estadísticas nos muestran que:

Las empresas aún presentan una débil gestión de parches extendida. Si ya teniamos desafíos en servidores, el reto se extendió al entorno de móviles corporativos, routers en casa y aplicativos de comunicación como Zoom. En la edición 2020 del Panorama de Amenazas en América Latina de Kaspersky las cifras son alarmantes: «dos de cada tres dispositivos en América Latina tienen vulnerabilidades críticas. Según nuestros datos, el 55% de las computadoras en la región todavía usan Windows 7 y el 5% Windows XP»

No todas las empresas pueden seguir prácticas adecuadas de codificación segura, sin embargo la intensidad de los ataques en pandemia ha crecido de manera exponencial. Por ejemplo, en el report «Threat Intelligence Insider Latin America de Fortine» se identificó que las plataformas digitales de Panamá fueron objeto de 655 millones de intentos de ciberataques durante el primer semestre de 2020.

La ciberseguridad debe estar enlazada con el marco empresarial de gestión de riesgos. No desplaces la construcción de la matriz de ciberriesgos. Y si ya tienes una construida, es vital cuestionar las definiciones de tolerancia y apetito de riesgo en el contexto empresarial y enlazarlo a la estrategia de negocio.

CONTINÚA EN PRÓXIMA PÁGINA

Error #3:
NO HABER RENOVADO LAS ESTRATEGIAS DE CIBERSEGURIDAD

En el informe 2020 «Ciberseguridad, Riesgos, Avances y el camino a seguir en América Latina y el Caribe», Moisés J. Schwartz Gerente de Instituciones para el Desarrollo del BID señala que «Hasta principios de 2020, solamente 12 países habían aprobado una estrategia nacional de ciberseguri- dad». Por otro lado, el vicepresidente regional de operacio- nes en Latinoamérica de Check Point, Ramón Jimenez señaló que "las empresas no sólo deben centrarse en implementar las herramientas y métodos de trabajo que permitan mantener su negocio activo, sino que estos procesos deben ir acompañados de una estrategia de ciberseguridad consolidada, hiper escalable y enfocada en la accesibilidad y movilidad de los datos». Ambos expertos refuerzan en sus opinio- nes que la postura de ciberseguridad de las empresas en latinoamérica deben atravesar un cambio inmediato.

El reto para la región, es que muchas empresas aún están aplicando conocimientos tradicionales de ciberdefensa, y pronto encontrarán un descalce. Lo que se propone es que transformemos e innovemos nuestras estrategias. Por ejemplo, la adopción del modelo Zero Trust.

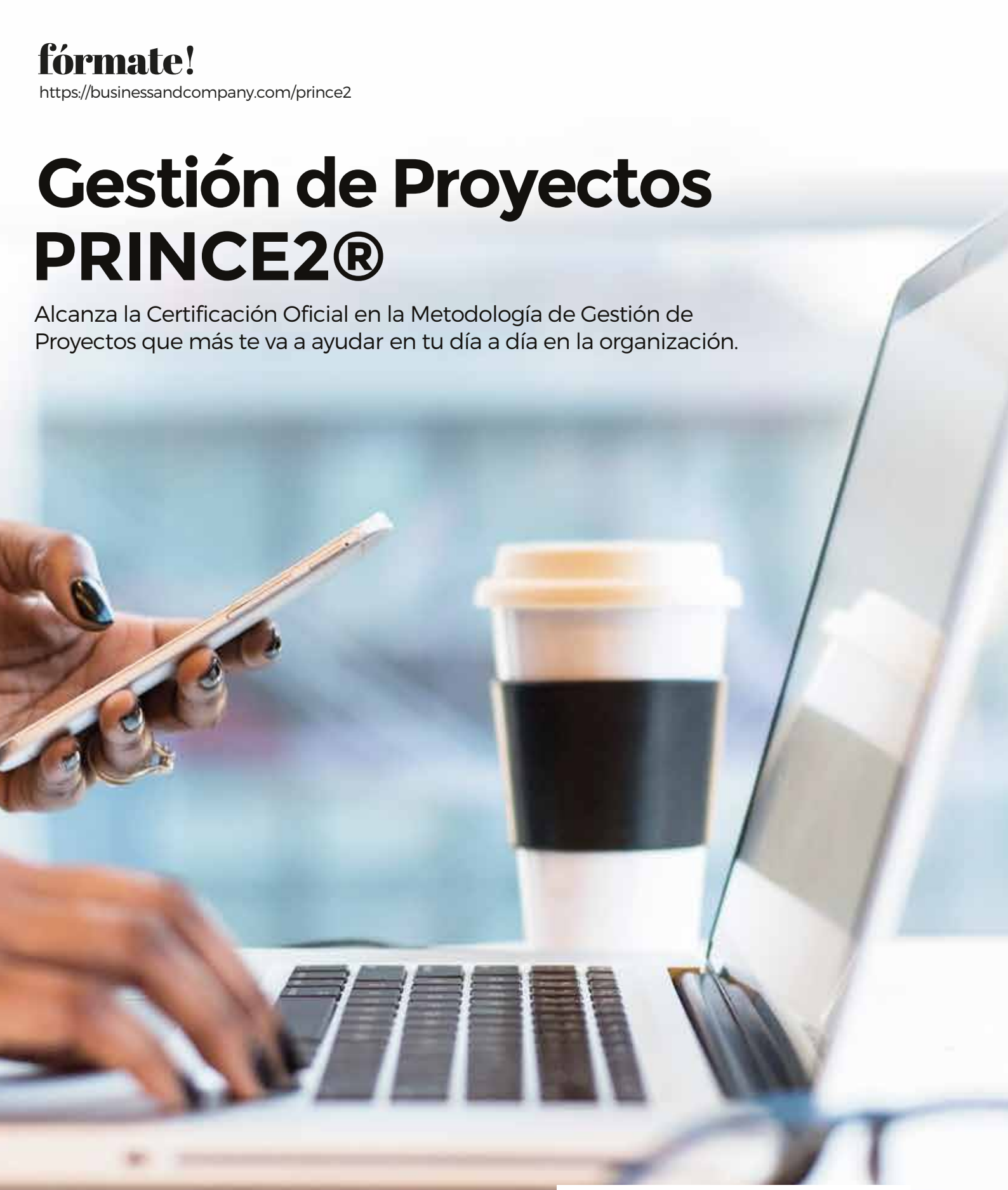
Albert Einstein lo tenía claro: Si buscas resultados distintos, no hagas siempre lo mismo. Para lograr el éxito deseado debemos dejar de cometer los mismos errores. Sugiero que hagamos un primer compromiso: 2021 debe ser el año en que los tres errores citados deben estar erradicados.

fórmate!

https://businessandcompany.com/prince2

Gestión de Proyectos PRINCE2®

Alcanza la Certificación Oficial en la Metodología de Gestión de Proyectos que más te va a ayudar en tu día a día en la organización.



Business&Co.®
Business, Technology & Best Practices, S.L.

PRINCE2®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

Carta de un CISO en Latinoamérica a los reyes magos

Queridos Reyes Magos, 2020 fue un año difícil por el Coronavirus para Latinoamérica. Al cierre del 2019 teníamos claro que aún con las brechas de cada sector/país el comienzo de este año nos deparaba momentos de innovación tecnológica. Recordemos que muchas empresas tenían definidas hojas de ruta hacia la industria 4.0, block chain, inteligencia artificial, banca virtual, automatización de las cadenas productivas, la modernización del transporte, entre otros. Así, los CISO de la región teníamos claro que era un año de cambios.

Claro está, llegó la pandemia y cada CISO en su ámbito empresarial tuvo que adaptarse a otro tipo de cambio, a uno con un escenario no previsto. Pero avanzar sin reconocer lo positivo de este largo camino que hemos realizado no sería equilibrado. No solo enfrentamos retos, sino que sumamos aprendizaje. La oportunidad de conocer aún más de cerca las preocupaciones del C-level, cada momento de incertidumbre donde los caminos pusieron en jaque inclusive a los más expertos. Se tomaron decisiones difíciles, algunas empresas pudieron salir adelante, pero no todos lo logramos.

Este año algunos tuvimos que despedirnos de amigos y colegas, sin embargo, sabemos que nuestra misión no ha acabado y estamos buscando siempre nuevas maneras de compartir conocimiento.

Antes de empezar mi lista de deseos quiero agradecerles por el talento profesional en Latinoamérica y que nos ha acompañado este año en cada uno de los ámbitos empresariales de la región. Ver que las nuevas generaciones de profesionales que persiguen como línea de carrera ser un CISO es alentador. Los países cada vez más están integrando y poniendo a disposición centros capacitación (por ejemplo, en noviembre de este año, el órgano adscrito al Ministerio de Trabajo en Colombia, el Sena, realizó un convenio con Mnemo, consultora española líder global y experta en Tecnologías y Seguridad, con el objetivo de formar cerca de 23.000 aprendices en ciberseguridad a 2024), también se están dando sinergias en grupos de expertos (tal es el caso del convenio firmado entre 8.8 Computer Security Conference, con el CSIRT Chile), y las certificaciones nos ayudan a profesionalizar la especialización requeridas.

También quiero agradecerles por las empresas que ya empiezan a dar sus primeros frutos como resultado de los programas de concientización en seguridad de la información. Aún nos falta mucho por recorrer, pero debemos reconocer los logros obtenidos. Latinoamérica ya cerró una brecha importante con la digitalización de industrias expandiendo soluciones de e-commerce, somos parte de la transformación digital que necesitaba la región y esto ha llevado a los equipos de seguridad a realizar el ansiado *unboxing* a nuevas habilidades, sacamos a relucir nuestra agilidad dejando atrás el cascarón del lado técnico, pensamos fuera de la caja y estamos adoptando cada vez mejores prácticas.

Este año, mi carta tiene tres pedidos para todos los CISO de estas lattudes:

1. Que no perdamos el radar nuestro propósito.

Al cierre de año técnicamente hemos aprendido a surfear más de un *Maverick*. Los CISOs hemos madurado en conocimiento y posturas de valor para las empresas.

Mi deseo es que este nivel de claridad nos ayude a seguir creciendo en prácticas profesionales y que nuestro propósito en la empresa sea cada vez más firme.

CONTINÚA EN PRÓXIMA PÁGINA

2. Que las empresas puedan integrar la labor del CISO en el desarrollo de sus objetivos.

Cada vez más se difunden a través de medios, redes sociales y reportes que somos el C-Level reconoce que el CISO es el socio estratégico que la empresa necesita para asegurar la salvaguarda de sus activos de información en un entorno digitalizado. Sin embargo, como compartía en el artículo anterior de América Próxima, las encues tas muestran con preocupación que no todas las empresas en la región no cuentan con un CISO. El CISO no solo está en compañías multinivel o grandes empresas reguladas, somos parte del ecosistema empresarial de los startups, mypes y pymes.

3. Que en 2021 podamos trabajar en lanzar un marco de prácticas para la región.

Nuestras realidades y contextos son tan cambian tes. Cada país de Latinoamérica tiene barreras, desafíos y oportunidades únicas que nos lleva a un vasto campo de conocimiento que merece ser difundido. Mi deseo es que empecemos a trabajar para lanzar el primer marco de mejores prácticas en seguridad para Latinoamérica. Cuando mencionaba esto en las cátedras locales de Perú, los alumnos me miraban algo consternados, pero siempre les decía ¿Por qué no?

Estos son mis deseos para el 2021 para todos mis colegas en la región. Agradezco mucho que hayan podido leer esta carta queridos Reyes Magos.
Finalmente, para ti amigo y colega lector, quisiera agradecer tu empatía con este humilde microes pacio (que no sería posible si no fuera por el talentoso equipo de Tecnología y Sentido común y por líderes como Javier Peris). Y pedir a los Reyes Magos para que tengáis lindas fiestas en compa ñía de sus seres queridos, con salud y que estas fechas sirvan para renovar sus energías y empe zar con pie derecho el 2021.

fórmate!

https://businessandcompany.com/msp

Managing Successful Programmes MSP®

Curso de Gestión de Programas de Proyectos MSP® Fundamentos

MSP®

ACCREDITED TRAINING ORGANIZATION

PeopleCert ON BEHALF OF AXELOS

Business&Co.®

Business, Technology & Best Practices, S.L.

Tomar decisiones informadas en la era de la desinformación

El anuncio de los nuevos términos y condiciones de WhatsApp para sus usuarios fuerade la Unión Europea y Reino Unido ha sido el “tech business epic fail” de inicio de año, en escala y con efecto
dominó. Pero toda relación usuario – empresa, tiene dos lados, en el presente artículo abordaré brevemente qué paso con la propuesta de actualización de WhatsApp, cuál es el rol que tenemos frente al uso de los aplicativos móviles y una modesta propuesta que busca mejorar nuestro conocimiento antes de decidir la instalación y uso de aplicativos a fin de desarrollar decisiones racionales en la era de la desinformación.

El epic fail y un breve resumen sobre lo que pasó.

WhatsApp emitió una confusa comunicación denominada “principales updates” de la nueva propuesta de Términos de Servicios (Term of Services - ToS por sus siglas en inglés) que aplicaría a partir del 8 de febrero (fecha que ha sido aplazada a mayo de 2021), donde: se dejaba entrever que los chats iban a ser almacenados y adminis- trados por las empresas del conglomerado de Facebook Inc.(1)y donde de manera asolapa se anunciaba que la aceptación era “necesaria”, es decir obligatoria. Enton- ces el pánico colectivo llegó y la interpretación general fue que la información de nuestros chats iba a ser accesible a múltiples terceros de no aceptar tales términos, y considerando que amablemente el comunicado también invitaba a visitar el Help Center para borrar la cuenta de no estar de acuerdo, pues más de 25 millones de usuarios expresaron su rechazo descargando y activando Telegram y otros 1.3 millones de usuarios descargan- do y activando Signal. (Jack Nicas, 2021)

Luego, los expertos y curiosos notaron al revisar el detalle de los ToS que se recopilaría la dirección IP de los usuarios y metadatos de nuestro comporta- miento (catalogando ambos como “datos necesarios” para prestar el servicio de mensajería). Lo cual es altamente cuestionable frente a otros aplicativos de mensajería como Telegram y Signal (aplicación recomendada por la Unión Europea) (2), que brindan el mismo servicio que WhatsApp sin necesidad de recopilar la extensa lista de datos que declara necesi- tar. Y como remate final, la ola de recomendaciones de migración a otros aplicativos por parte de diversos expertos en privacidad, líderes del sector tech y empresarios como Elon Musk.

El rol que tenemos frente al uso de aplicativos móviles. Como mencionaba, se requiere dos partes en la relación usuario – aplicativo móvil (la cual recuerden está gestionada por una empresa), y como en cualquier relación ambos deben estar informados. El problema, del cual tenemos entera responsabilidad, es que en general muy pocos usuarios leen los ToS/ Políticas de Privacidad y optan por evadir el proceso(3) , y al aceptar algo que no leemos estamos aceptando estar desinformados; a lo que se suma una extensa crítica que viene resonando en Sillicon Valley donde nos recuerdan que “Cuando un producto es gratis, el producto eres tú” en un contexto de desinformación (recomiendo que puedan ver el docudrama The Social Dilemma)(4).

Así es inevitable preguntarse, si WhatsApp no es el único aplicativo móvil que tenemos instalado que potencialmente recopila o recopilará una larga lista de datos personales que no requieren para brindar el servicio, entonces ¿cuántos de nosotros hemos revisado los ToS de estos aplicativos? ¿Estamos buscando alternativas? En adelante, ¿nos aseguraremos de conocer qué datos cedemos, ¿cómo serán tratados si tenemos opciones adecuadas para minimizar su exposición? Si aun no comienza el proceso, lo invito a leer el short paper publicado en 2017 en la IEEE “How Much Privilege Does an App Need? Investigating Resource Usage of Android Apps”

Si la libertad de poder elegir es una capacidad invaluable en el ser humano, y muchos de nosotros celebramos nuestra destreza al seleccionar lo mejor para nosotros en términos de salud, educación, estilo de vida, entre otros; no cedamos nuestra toma de decisiones a terceros o solo cuando la polémica llega a puntos álgidos.

CONTINÚA EN PRÓXIMA PÁGINA

Lo que podríamos hacer. La opción inmediata es la lectura, pero en Latinoamérica es una variable con diversos matices y el comportamiento de los usuarios frente a este hábito puede tomar más tiempo del requerido. Eso sí, no dejaremos de lado la evangelización de mejores prácticas en nuestras instituciones y comunidades, pero necesitamos un punto de apoyo con efecto "WoW". Es por eso, que propongo la construcción de un semáforo (similar al de los alimentos) en los que podamos distinguir el grado de "recopilación de datos" que requieren los aplicativos. Este semáforo, resumirá de manera gráfica y sencilla cuáles serían los riesgos y podríamos transformar nuestro proceso de decisión de instalación y uso de aplicativos a una toma de decisión informada. ¿Qué opinan?

REFERENCIAS:

1- "cómo las empresas pueden usar los servicios alojados de Facebook para almacenar y administrar sus chats de Whatsapp" - Recuperado el 16 de enero de 2021 desde https://www.elnuevotiempo.com/cua- les-son-y-como-afecta- ran-las-nuevas-condiciones-de-whatsapp/

2-European Commission to use open source messaging service Signal. Recuperado el 16 de enero de 2021 desde https://joinup.ec.europa.eu/- collec- tion/open-source-observatory-osor/news/signal-messaging-ser- vice

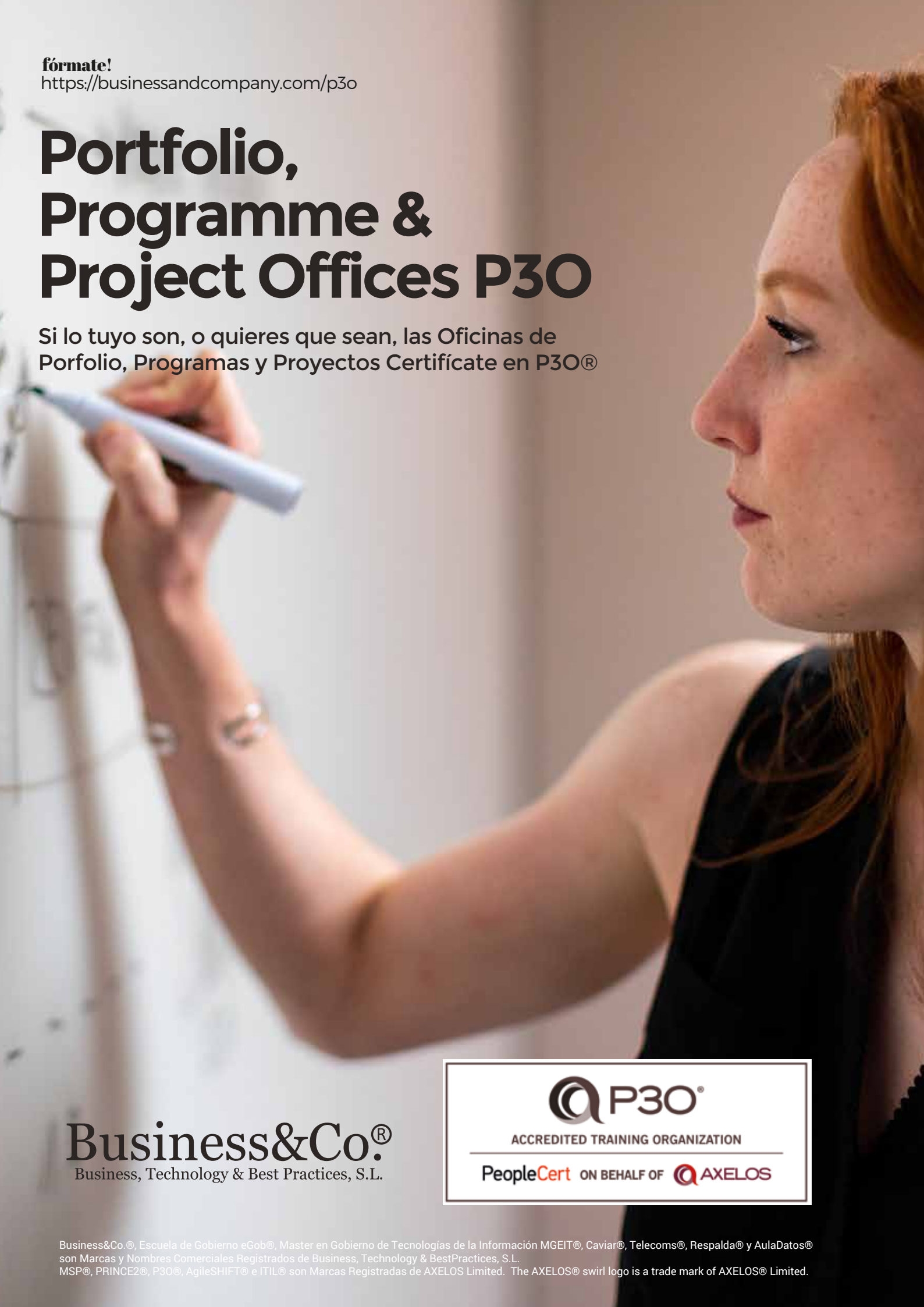
3-Jonathan A. Obar & Anne Oeldorf-Hirsch (2020) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services, Information, Communication & Society, 23:1, 128-147, DOI: 10.1080/1369118X.2018.1486870

4- Tristan Harris And "The Social Dilemma:" Big Ideas To Fix Our Social Media Ills , Recuperado el 16 de enero de 2021. https://www.nytimes.- com/2020/09/09/mo- vies/the-social-dilemma-review.ħtml

fórmate!
https://businessandcompany.com/p3o

Portfolio, Programme & Project Offices P3O

Si lo tuyo son, o quieres que sean, las Oficinas de Porfolio, Programas y Proyectos Certifícate en P3O®



Business&Co.®
Business, Technology & Best Practices, S.L.

P3O®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

Diez pautas claves en la gestión de seguridad de la información para Latinoamérica

Deepak Chopra mencionó que "Todos los grandes cambios vienen precedidos por el caos", y ciertamente la teoría del caos forma parte de todos los ecosistemas empresariales con ritmos cíclicos. Hoy, el coronavirus aún sigue siendo un símbolo de caos. Los cambios no cesan, y con las nuevas medidas de cuarentena seguimos creando nuevas maneras de hacer negocios. Es innegable que lo que llamábamos nueva normalidad y que percibíamos como transitorio en 2020, perdió esta característica y se transformó en nuestra realidad.

En Latinoamérica el contexto de caos ha ido materializado transformaciones de impacto profundo y raudamente. Los ejemplos más notorios están en cómo se llevan a cabo los reclutamientos de personal (100% online), los puestos en su mayoría detallan que las funciones se ejercerán de manera remota, el delivery se ha vuelto el circuito principal que articula las ventas, el cierre de locales por modelos de e-commerce y los nuevos conceptos de market place, las pequeñas y medianas empresas han volcado su acercamiento a clientes a través de redes sociales, la adopción masiva de canales de comunicación por bots, y todo esto viene abriendo camino al "Internet of Behaviour".

Y en este compás de cambios, los responsables de seguridad de Latinoamérica estamos llamados a tomar estrategias efectivas de adaptación, pero en **modo urgencia**. ¡Vamos! Comenzamos el partido con una brecha de entendimiento del rol y la priorización de las estrategias de ciberseguridad; sin embargo, el negocio no se detuvo y los riesgos se han complejizado de manera exponencial porque las elecciones tecnológicas tomadas por el negocio han ido de la mano con restricciones económicas del contexto. Y ahora, tenemos sobre la mesa tres grandes retos:

1. Proteger la privacidad de la información con las posibles limitaciones regulatorias que tenemos en las nuevas infraestructuras.

2. Las relaciones contractuales con proveedores que han hecho posible la transformación digital (por ejemplo, de e-commerce), con manejos de componentes que probablemente no hayan pasado por una evaluación integral de riesgos.

3. La profundización de la falta de experiencia en los equipos de seguridad frente a la adopción de nuevas tecnologías (recordemos que en 2019 estábamos preparándonos para un proceso de adaptación de 3 a 5 años, lo que en pandemia se aceleró a 3 o 6 meses en promedio)

CONTINÚA EN PRÓXIMA PÁGINA

¿Cómo enfrentar estos desafíos? Si bien los cambios, requieren que de manera innovadora establezcamos planes de acción existen 10 pautas que deben estar presentes para abordar con éxito el Plan de Seguridad de la Información en el contexto de cambio que estamos viviendo.
El desarrollo de la gestión de Seguridad de la Información o Ciberseguridad debe cumplir el siguiente decálogo:

1. Es y será exitoso solo si existe compromiso y colaboración de toda la empresa, por lo que el apoyo de la línea gerencial es clave, sobre todo en contextos de cambios.

2. Puede ser implementada de manera evolutiva (marco de madurez), pero no puede ser implementada de manera selectiva. La velocidad de salir al mercado no debe relajar la evaluación de los equipos de seguridad.

3. Es un proceso core del negocio interrelacionado con todos los demás procesos de este y se integra a la gestión de riesgo empresarial.

4. Genera valor, de manera indiscutible, mientras protege a la empresa. Dejar de lado los conceptos asociados a que representa un gasto es fundamental, para ellos debemos mantener un enfoque basado en riesgos.

5. No es aislada y es parte de la cultura empresarial, por lo que debe ser promovida con la misma intensidad e importancia que los valores / principios definidos.

6. Está basada en principios, los cuales acompañan a la empresa aún en los procesos de transformación más drásticos, base fundamental para el despliegue de estrategias y procedimientos

7. Nos exige estar informados y alineados de manera continua con el negocio, así la existencia de comités ejecutivos es mandatario.

8. Está y estará presente en todos los momentos de cambio que decide emprender la empresa, ahora más que nunca.

9. No será posible, ni el plan de seguridad de la información podrá desarrollarse, con el equipo de tecnología trabajando en dirección contraria.

10. Debe adoptar un enfoque holístico, integrados y de excelencia para sostener de manera adecuada al negocio.

Si tenemos en cuenta los 10 pasos, habremos construido un contexto coherente y sólido para desplegar las acciones que requiera la empresa.

¿Está viviendo el síndrome del acumulador de vulnerabilidades?

Hace poco tuve la oportunidad de ver nuevamente la película Deepwater Horizon y no dejaba de pensar en las coincidencias de lo sucedido con los escenarios de ciberataques causados por vulnerabilidades conocidas y que por decisión empresarial fueron desatendidas o no remediadas. Es curioso cómo el ser humano olvida el valor de las tareas preventivas y de gestión de riesgos en tiempos de aparente calma.

Es bien conocido que todos los días se emiten estudios, guías, reportes, webminars y artículos de proveedores, consultoras, institutos especializados y profesionales que nos explican la importancia de contar con una adecuada gestión de vulnerabilidades y la aplicación de parches. Sin embargo, las estadísticas revelan que las empresas no están aplicando planes de remediación a vulnerabilidades críticas conocidas. Por ejemplo, al cierre de 2020 Kasperky Latinoamérica comunicaba: "la situación es tan crítica en la región que WannaCry sigue siendo la familia de ransomware número uno. Este ataque explota la vulnerabilidad MS17-010, la cual cuenta con un parche desde 2017, pero las organizaciones aún no han actualizado sus sistemas".

¡Vaya situación! Porque el subtexto de esta decisión es que la adopción de mejores prácticas solo se realizará cuando la empresa se vea comprometida, en tanto se puede convivir con el riesgo. Lo pernicioso de este entendimiento es que va gestando en la cultura empresarial una suerte de síndrome emergente a la que denomino "El acumulador de Vulnerabilidades.

¿Cuáles son las características de una empresa con el síndrome del acumulador de vulnerabilidades?

El escenario más crítico que describe el síndrome, algo así como un DEFCON 1, son empresas donde existe una pobre implementación del marco de gestión de riesgos empresarial y de tecnología, y sin dudar el gobierno y gestión empresarial va en contra corriente a todos los objetivos orgánicos de la seguridad de la información. A nivel de indicadores podría estar representado por entornos tecnológicos que soportan operaciones core, y que corren en software en "End of Life" o con vulnerabilidades no remediadas por más de 90 días, sin planes de mitigación. Suelen convivir con las vulnerabilidades activas, categorizando el riesgo de ataque como bajo a pesar de la criticidad descrita en los CVE, debido a que no hay indicios de que estén siendo atacados. Asimismo, tienen como mantra de justificación que no hay presupuesto a corto plazo para dar solución a estas vulnerabilidades.

Este tipo de empresas solo dejará atrás las trabas que regularmente retrasan la gestión de vulnerabilidades o la aplicación del parche de seguridad si vive el *journey* del ciberataque. De ser el caso, hará exactamente lo contrario a lo que sostiene, detendrá el negocio para atender el incendio, activará presupuestos no planificados, el backlog de pases a producción cambiará y colocará de manera temporal en el podio de honor las propuestas de seguridad/ciberseguridad para la foto. Inclusive, no verá a profundidad la cadena de ataque, entendiendo que si ha dejado de recibir un ataque activo entonces ha salido "bien librada". Eso sí, esta experiencia no será lo suficiente memorable, pues eventualmente volverá a la costumbre.

CONTINÚA EN PRÓXIMA PÁGINA


MSA

Si hasta esta parte, su empresa no se encuentra bajo esta descripción, ¡enhorabuena! No obstante, lo/la invito a que hagamos una evaluación más profunda y descartemos en dos frentes si las siguientes alertas podrían estar o no presentes:

Alertas del síndrome acumulador en la postura del gobierno empresarial: El C-level ha malentendido que la gestión de ciberseguridad es costosa y que el fin de esta es únicamente asegurar que la empresa no será atacada. No encuentra relación entre la gestión de vulnerabilidades y la gestión de riesgos empresarial, y podría considerar que sus indicadores son únicamente de carácter técnico. El presupuesto de ciberseguridad puede ser inexistente o muy austero, por lo que no se realizan evaluaciones de vulnerabilidades y la arquitectura de seguridad podría carecer de elementos claves.

Alertas del del síndrome cuando seguridad y tecnología no encuentran un lenguaje común: Aunque irónico, porque indiscutiblemente ambas áreas enriquecen sustancialmente al negocio y buscan estar alineadas a los objetivos de este, aún encontramos empresas en las que en lugar de encontrar dialogo entre las áreas de seguridad y tecnología, escuchamos constantes "Dracarys" entre ellos. Algunos ejemplos

1- No tenemos entornos de prueba para ningún servidor o servicio y no hay presupuesto para implementarlos. Pueden seguir colocando tickets, pero serán atendidas cuando no haya carga o sea prioridad para el negocio.

2- Desplegar actualizaciones hacia los usuarios finales interrumpe la productividad. Y con el teletrabajo, la actualización desde casa requiere un consumo elevado de ancho de banda.

3- Los encargados de alertar sobre vulnerabilidades son los de seguridad, nosotros hacemos lo que ellos deciden.

¿Cómo evitamos caer en el síndrome del acumulador de vulnerabilidades?

Curar el síndrome no sucederá de la noche a la mañana, pero existen elementos fundamentales que debe fortalecer o implementar: gestión del cambio en relación con la seguridad de la información (sugiero seguir los 8 pasos de Kotter) y la implementación de un robusto marco de gestión de riesgos empresarial y de Tecnología. Asimismo, sugiero revisar son:

1- Del Instituto Nacional de estándares y Tecnología del gobierno de estados unidos (NIST – por sus siglas en inglés), la Publicación Especial 1800-31A, Improving Enterprise Patching for General IT Systems, el Critical Cybersecurity Hygiene y la publicación especial 800-40 v3 Guide to Enterprise Patch Management Technologies

2- De Garner, The New Vulnerability Management Guidance Framework. Y del Instituto Georgia Tech el modelo de madurez propuesto para la gestión de vulnerabilidades.

1) Narra la tragedia sucedida en el Golfo de México el 20 de abril de 2010 cuando la plataforma Deepwater Horizon de la multinacional British Petroleum (BP) derramó casi cinco millones de barriles de petróleo en un incendio. - 2) Por mencionar algunos NIST, ISACA, ENISA, INCIBE, CIS, entre otros. 3) En 2021 casos como los de SolarWind y las vulnerabilidades de día 0 en los servidores on-premise de Exchange hicieron nuevamente un efecto campana. 4) https://security.gatech.edu/vulnerability-management

fórmate!
https://businessandcompany.com/cobit

Tu vida puede depender de la tecnología

COBIT® 2019 Marco de Gobierno y Gestión de la Tecnología

La Implementación de un Marco de Gobierno y Gestión de Tecnologías de la Información permite conocer la salud global de los Sistemas de Información de los que depende los procesos habituales de una organización, sin un adecuado Marco de Gobierno y Gestión se podrá trabajar la seguridad, privacidad y otros aspectos de manera disociada tampoco se podrá garantizar que se estén teniendo en cuenta todos los factores necesarios para una adecuada operación. COBIT® aporta confianza.

Business&Co.®
Business, Technology & Best Practices, S.L.

La importancia de dar continuidad al desarrollo de Smart City en Latinoamérica

El término Smart City o Ciudad Inteligente (CI en adelante) es sinónimo de modernidad, innovación, bienestar y desarrollo. Fue introducido por primera vez en el desarrollo urbano a inicios en los años 70 cuando en Los Ángeles, Estados Unidos, se creó el primer proyecto urbano usando Big Data denominado "A Cluster Analysis of Los Angeles".

Desde ese entonces, su definición y alcances han estado en constante evolución. Si bien a la fecha no se cuenta con una única definición, todas las fuentes coinciden que de cara al 2021 el objetivo principal es el desarrollo del ser humano en un entorno (ciudad o territorio) sostenible., y la importancia de su implementación se ha visto acelerada con la pandemia. Así, las CI en los próximos años debe ser resiliente, con políticas de espacios verdes, segura, con estrategias que optimicen el transporte público, con condiciones económicas adecuadas, con iniciativas medioambientales, con espacios que promuevan la retención de talento local, con marcos regulatorios que permitan un uso equilibrado de la tecnología y con plataformas que faciliten la cohesión e interconexión de los datos (Open Data).

Latinoamérica tiene casos notables de éxito en la implementación de CI y que gratamente no han paralizado su desarrollo a pesar de los retos de la pandemia. A continuación, analizaremos brevemente el ranking de CI en la región, la importancia de quitar el carácter tecnocentrista que muchos podrían asociar a su concepción y comunicar cuáles son los factores seguidos por ciudades/países líderes a fin de dar continuidad a las metas de transformación.

RANKING DE CIUDADES INTELIGENTE AL 2020

Los reportes coinciden en resaltar los logros sostenidos de Chile, Colombia y Brasil en la región. Así, vemos que el índice ICIM[1] ratifica el liderazgo de Santiago de Chile y a Caracas como la ciudad con menor evolución. El Índice de IMDB[2] posiciona a Medellín como líder en la región, y el estudio del SMRW[3] agrupa a Bogotá, Buenos Aires, Santiago de Chile, Monterrey, Montevideo, Ciudad de Panamá, Quito, Sao Paulo y Rio de Janeiro como ciudades con progresos intermedios a nivel mundial.

El reconocimiento de Chile, Colombia y Brasil es producto de estrategias de trabajo holísticas y el desarrollo de planes nacionales que han

cumplido los hitos definidos de manera consistente. El éxito radica en la inclusión de factores que trascienden los marcos legales y la sana ambición de estos países por desarrollar una marca ciudad, logrando una participación de diversos actores de las ciudades (no solo el gobierno). Tal es el caso de Chile con el plan nacional "Chile: Territorio Inteligente" y el "Plan Maestro: Modelo para el Desarrollo de Infraestructura Habilitante de Ciudades Inteligentes Abiertas"[4]. En tanto que Medellín "la Silicon Valley de Latinoamérica" ha incentivado la aplicación de un modelo de madurez para promover en más urbes la implementación de CIs. Finalmente, Brasil cuenta con el apoyo de instituciones financieras nacionales que promueven el desarrollo de ciudades inteligentes como el Banco Nacional de Desenvolvimiento Económico e Social (BNDES) y La Caixa Económica Federal [5] .

LA TECNOLOGÍA COMO HABILITADOR DE CIUDADES INTELIGENTES:

Es indudable que la tecnología es un facilitador importante y que el uso de Blockchain, IoT, Big Data, Inteligencia Artificial, Gemelos Digitales y las iniciativas de Revolución Industrial 4.0 que está en marcha en la región, son necesarias para innovar y acelerar los beneficios de CI. Sin embargo, no es la tecnología por si sola la que da carácter desSmart a una ciudad. El enfoque es hacia el ciudadano y no hacia los dispositivos. Esta afirmación, es vital para las ciudades que en la búsqueda de mejorar aún asocian las CI como proyectos tecnológicos, dejando de lado dimensiones como las que son medidas por el ICMI [6] , o factores que son definidos en la familia de la norma ISO 37120 (ISO 37120, 37122 y 37123).

El riesgo, es el fracaso y la pérdida de valor. Por ejemplo, implementar semáforos inteligentes sin tener una infraestructura digital viable, cambios en el presupuesto o que no sea utilizado para tomar decisiones por falta de personal capacitado. De igual manera, está el asociar el crecimiento de aplicativos de delivery de comida al bienestar ciudadano, sin revisar el marco legislativo del tratamiento de datos o calidad de servicio.

CONTINÚA EN PRÓXIMA PÁGINA

¿CÓMO DAR CONTINUIDAD AL DESARROLLO DE SMART CITIES?

Aunque simple en definición, pero complejo en su ejecución, existen tres factores que darán continuidad a los planes de desarrollo de CI en Latinoamérica: (1) la voluntad de los líderes en priorizar los planes existentes independiente de los cambios político, (2) el desarrollo de legislaciones que permitan integrar los planes hacia una visión e-government, (2)crear planes nacionales y legislar términos de seguridad – privacidad para las soluciones tecnológicas elegidas. Es importante reconocer que los países líderes no han paralizado sus avances aún en pandemia ¿Por qué deberían paralizar los otros países? El Foro Económico Mundial insta al 2021, que las ciudades a nivel mundial deben impulsar la Transformación Digital para enfrentar con mejor postura lo que queda de la pandemia u otras crisis, dando paso a mejorar las Infraestructuras Digitales y resaltando que las ciudades digitales deben ser "un paraguas donde muchas tecnologías se unan para el enriquecimiento de las personas y la sociedad [7] .

REFERENCIAS:

1- Índice IESE Cities in Motion" 2020 del IESE Business School de la Universidad de Navarra. De las 174 ciudades evaluadas, 25 ciudades son de Latinoamérica. https://dx.doi.org/10.15581/018.ST-542.

2- "Smart City Index 2020" elaborado por el IMDB en colaboración con la Universidad de Tecnología y Diseño de Singapur. De las 109 ciudades evaluadas, 6 ciudades son de Latinoamérica

3- Reporte Smart City Solutions for a Riskier World, elaborado por ESI ThoughtLab. Evaluó a 167 ciudades a nivel mundial.

4 - Publicado por la Universidad de Santiago de Chile en septiembre 2020. Es una guía metodológica que brinda pautas a los municipios en sus procesos para transformarse en territorios inteligentes.

5 - Estudio de Mercado "El mercado de las Smart Cities en Brasil", diciembre 2020. Publicado por la Oficina Económica y Comercial de la Embajada de España en Brasilia

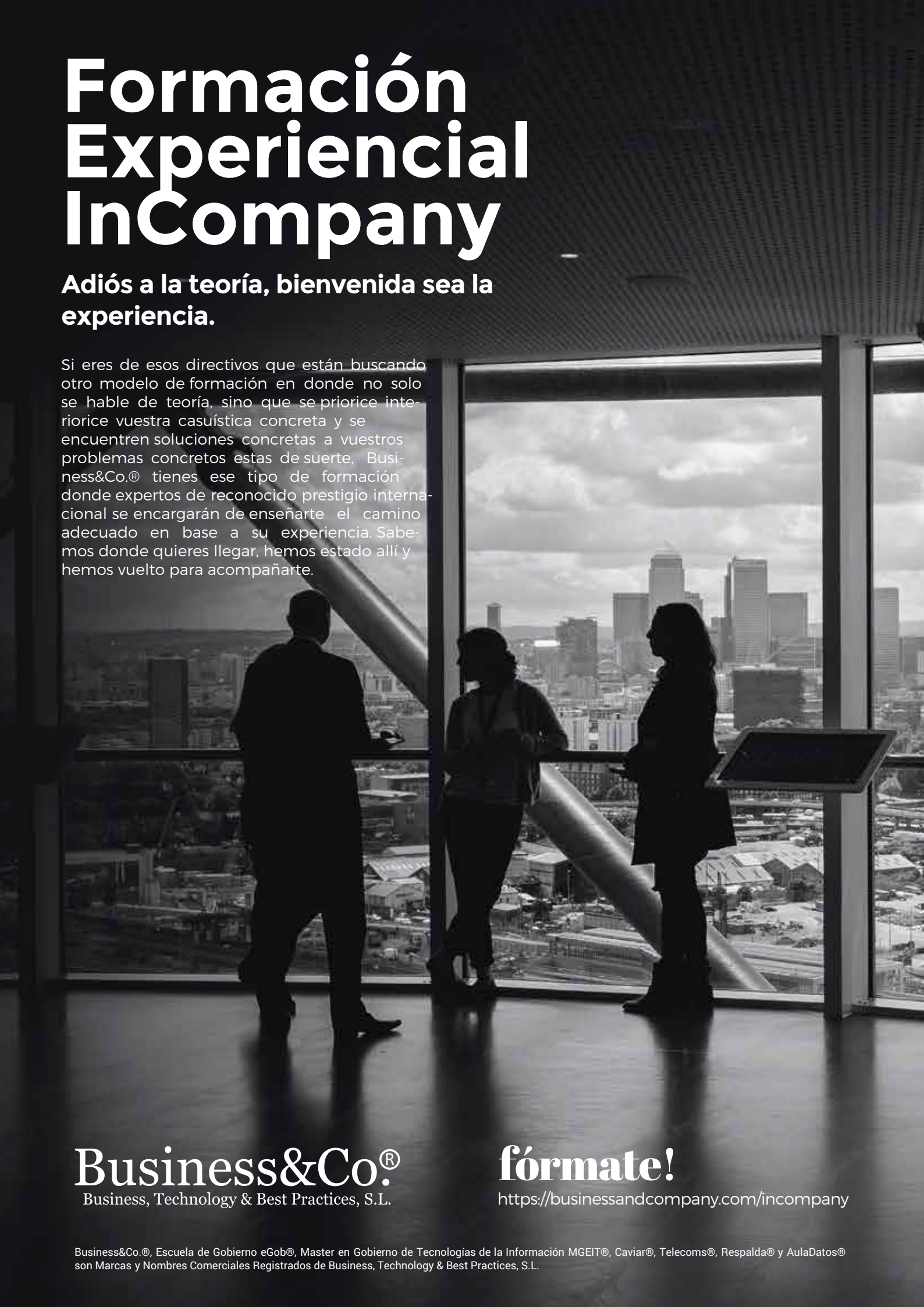
6 - El Índice Cities in Motion, plantea 9 dimensiones claves: Gobernanza, Planificación Urbana, Medio Ambiente, Proyección Internacional como Marca Ciudad, Cohesión Social, Movilidad Y El Transporte, Capital Humano, Economía y Tecnología,

7 - https://www.weforum.org/agenda/2021/04/future-of-smart-cities-covid-19-digital/

Formación Experiencial InCompany

Adiós a la teoría, bienvenida sea la experiencia.

Si eres de esos directivos que están buscando otro modelo de formación en donde no solo se hable de teoría, sino que se priorice interiorice vuestra casuística concreta y se encuentren soluciones concretas a vuestros problemas concretos estas de suerte, Business&Co.® tienes ese tipo de formación donde expertos de reconocido prestigio internacional se encargarán de enseñarte el camino adecuado en base a su experiencia. Sabemos donde quieres llegar, hemos estado allí y hemos vuelto para acompañarte.



Business&Co.®
Business, Technology & Best Practices, S.L.

fórmate!
https://businessandcompany.com/incompany

Postura Ética de los Programas de Seguridad de la Información

Ser ético y actuar de manera honesta es una huella que dejó mi madre tatuada en mi alma, y es que, con total certeza, ella era una real creyente de que el mundo sería mejor si las personas actuábamos de manera ética y honesta. Inspirada en esta enseñanza, el presente artículo nos invita a reflexionar sobre la vigencia de los programas de ética empresarial en pandemia, la importancia de estos sobre la postura ética que deben mantener los roles de seguridad de información y qué opciones tenemos frente a posibles dilemas éticos que podríamos estar enfrentando.

Las empresas establecen componentes éticos, con el objetivo de promover integridad en sus talentos/colaboradores y en la búsqueda de continuar de manera sostenida las mejores prácticas conocidas promueve la existencia de cinco frentes: a) validar la integridad del personal mediante antecedentes y pruebas psicológicas b) desarrollar un código de ética (laboral, de conducta y/o de ética profesional; c) ejecutar con frecuencia y de manera obligatoria un curso de ética y evaluar el grado de comprensión del mismo; d) contar con instancias, como los comités de ética y líneas de denuncia para recibir alertas o incumplimientos; e) definir roles y responsabilidades que promuevan el cumplimiento ético de las funciones.

Prepandemia, los cinco frente mencionados ya presentaban retos que alertaban a los responsables de los programas éticos sobre la necesidad de rediseñar, actualizar y añadir nuevos enfoques. Es bien conocido, por ejemplo, que ciber atacantes han encontrado en los programas de selección de personal debilidades, buscando llegar a puestos claves para obtener información y luego renuncia. De igual manera, se empezó a cuestionar la estandarización que se había adoptado en la estrategia de concientización ética, poniendo en evidencia que roles como los de tecnología, seguridad de la información y ciberseguridad requerían un código ético especializado. Y finalmente, se evidenció que un alto porcentaje de empresa en Latinoamérica carecían de líneas o comités éticos que pudieran respaldar la adecuada evaluación de los casos potenciales que se pudiera presentar.

¿Qué paso en pandemia? En síntesis, la crisis trajo incertidumbre y con ello nuevos riesgos, y en esta vorágine también trajo nuevos escenarios donde las decisiones tomadas debían ser contrastadas para determinar si estaban en el marco ético empresarial. Por ejemplo, los pagos a proveedores.

Ahora bien, las decisiones frente a las decisiones de seguridad de la información también han pasado por momentos de tensión, desafiando la postura ética de muchos responsables. Es bien conocido que el CISO y el personal que compone el organigrama de las áreas bajo su gestión, sean funciones tercerizadas o no, tienen acceso a información confidencial, datos privados de colaboradores y conocimiento clasificado sobre hechos de importancia suscitados en la empresa por lo que su comportamiento ético es obligatorio.

Sin embargo, y aunque la verdad pueda incomodar, la experiencia profesional me ha llevado a conocer en este periodo de primera mano que, los profesionales de seguridad han tratado con mayor intensidad, escenarios de dilema ético durante la pandemia que en prepandemia. Es importante tener en cuenta que los dilemas éticos no solo han sido recibido desde las áreas usuarias, sino que también han sido planteadas desde el C-Level. A continuación, cito las cinco situaciones más recurrentes que han sido trasladas al responsable de seguridad:

-¿Qué alcance de información se debe presentar ante los entes reguladores sobre el real estado de madurez o capacidad del plan de seguridad de la información durante la crisis pandémica?

-Sabiendo que la empresa está en crisis, ¿se deben reportar todos los incidentes de ciberseguridad sufridos al comité o instancias reguladoras? O, ¿solo se deben reportar los altamente críticos?

-¿Es factible "flexibilizar" la aplicación de la política de seguridad de la información en ciertos escenarios, para no paralizar las nuevas estrategias comerciales de la empresa y regularizar posteriormente las acciones que se debieron realizar?

-¿Se debe contar con controles de seguridad de la información en dispositivos personales usados por el personal al cual no se le pudo asignar equipos para realizar teletrabajo?

-¿Es posible retirar ciertos controles de seguridad a roles claves o gerenciales y aceptar el riesgo?

CONTINÚA EN PRÓXIMA PÁGINA

Como compartía en el párrafo de reflexiones previas, cuando nos enfrentamos a situaciones nuevas y complejas, se debe usar el juicio y el sentido común, elementos que apelan a atributos de formación profesional y valores morales. Los cinco escenarios narrados, no debieron ser difíciles de abordar si el líder empresarial mantuvo la postura ética de manera consistente en pandemia, si los cimientos de ética empresarial fueron lo suficientemente robustos durante la crisis pandémica y si el CISO tuvo clara la postura ética de los programas de seguridad de la información.

No obstante, para los que enfrentaron los retos con un escenario adverso, la recomendación es que las decisiones tomadas deben estar documentadas, enfatizando la comunicación de riesgos y la aceptación de estos. De igual manera, será necesario revisar las situaciones tratadas y las lecciones aprendidas, con el objetivo de actualizar las estrategias de ética empresarial que preservarán la postura ética de los programas de seguridad de la información. Finalmente, reforzar con el equipo las conductas esperadas frente a situaciones similares.

fórmate!
https://businessandcompany.com/itil

El Sistema de Valor del Servicio de ITIL®4

...o todavía andas pensando en el ciclo de vida del Servicio.

Business&Co.®
Business, Technology & Best Practices, S.L.

ITIL®
ACCREDITED TRAINING ORGANIZATION
PeopleCert ON BEHALF OF AXELOS

Iniciativas latinoamericanas para acortar las brechas digitales

El uso y acceso a la Internet se convirtió en el habilitador universal más importante que los países a nivel mundial ubicaron como actor central para el diseño de estrategias en la reactivación económica, salud, educación y servicios al ciudadano durante la pandemia. Dichas estrategias no solo tuvieron que habilitarse en tiempo récord, sino que además debieron ser redefinidas sobre proyectos en marcha e inversiones que ya tenían hojas de ruta para acortar las brechas de accesibilidad digital y aumentar la capilaridad debido a que hay carencias de accesibilidad en la región.

El presente artículo, el último de esta temporada, busca acercar a usted amigo lector, algunas cifras que nos permitirán entender el estado de las brechas digitales y qué casos de éxito en la región pueden ser tomadas como buenas prácticas a fin de no debilitar el compromiso que deben tener las entidades gubernamentales en la región para acortar las brechas digitales.

DIFICULTADES EN LA TRANSFORMACIÓN DIGITAL Y ACERCAMIENTO DE SERVICIOS HACIA EL CIUDADANO

Tal como se dio la transformación digital acelerada en las empresas del sector privado, el estado tuvo que poner F1 y crear en tiempo récord estrategias para dar continuidad a servicios básicos para el ciudadano, siendo que todas ellas reposaban en que la existencia y acceso a la Internet iba a ser el mayor facilitador. Pero las condiciones no estaban dadas y no fueron óptimas para Latinoamérica y el Caribe, por ejemplo, el Banco Mundial en diciembre 2020 mostraba que casi el 50% de países de la región no tenía acceso a banda ancha de Internet. Sumada a esta limitante, también mostraban otras carencias sobre todo en zonas rurales tales como la falta de acceso a equipos informáticos, equipos celulares, televisión o radio.

La combinación de todos estos factores elevó el nivel de desafío para llevar a cabo las estrategias de digitalización y la visión de cada país sobre el acercamiento de servicios a través de la Internet, dejando atrás a todos aquellos que no tenían acceso a Internet y ha generado retrocesos severos en países donde no había condiciones para la virtualidad. Uno de los casos más criticados fue el de Bolivia, país que cerró el año escolar en 2020 porque no tenía condiciones para la teleeducación o el hecho de que casi 46% de los niños y las niñas de cinco a doce años de América Latina viven en hogares no conectados.

Conocidos los problemas y puntos de dolor, ¿cuáles son las iniciativas deben concretarse sin lugar a duda para acortar la brecha en la región? A continuación, citaré las tres iniciativas más importantes que se están desarrollando y que requieren con sentido de urgencia desarrollarse.

DECLARACIÓN DE LA INTERNET UN SERVICIO PÚBLICO DE CARÁCTER ESENCIAL Y UNIVERSAL.

Para acortar la brecha de acceso a Internet, diversos países buscan garantizar el acceso a Internet, con tarifas asequibles y competitivas. Así Brasil, Chile y recientemente Colombia han impulsado a través de sus legislaciones la necesidad de ampliar coberturas a fin de llegar a los lugares más alejados, agilizar los procesos de designación de licencias y la ejecución de infraestructura.

Este paso es esencial para dar continuidad a las metas de Industria 4.0, reactivación económica y digitalización. Por ejemplo, en junio recibimos con

alegría la noticia de que El Salvador es el primer país del mundo en adoptar bitcoin como una moneda de curso legal. Sin embargo, varios medios han evidenciado que la brecha digital frena la adopción de esta moneda. Una vez más se evidencia que sin Internet, no se puede avanzar. De esta manera, la iniciativa de declarar la Internet como un servicio de carácter esencial debe ser adoptado en bloque.

CHILE, Y LA VISIÓN EJEMPLAR DE SER EL HUB DIGITAL LATINOAMERICANA.

La ambición de ser el mejor, es un impulsor estratégico y ejemplar para la región. Si algo debemos apreciar de Chile es que viven y desarrollan la transformación bajo un enfoque de efectividad y eficiencia de lujo. No solo buscan solucionar los problemas a corto plazo, sino que además lo hacen con el objetivo de ser los referentes de la región y construyen estrategias que perduran aun con los cambios políticos.

Y este ámbito no ha sido la excepción. A través de la Fundación País Digital, en mayo de este año, Chile abrió un foro que buscó fomentar el dialogo abierto sobre las estrategias de desarrollo de una cultura digital, la realización de proyectos público-privados, además de la generación de contenidos que aporten al debate en el ámbito de la economía digital y el desarrollo del país de cara a la cuarta revolución industrial. Siendo el foco de interés la búsqueda de criterios sobre cómo debe avanzar el país en el despliegue de redes de alta velocidad, reducción de brechas digitales y nuevos modelos de desarrollo para la industria tales como impulsar 5G y la relación de provecho que significa esto en términos del PBI en los próximos 10 años (USD$ 14,8 mil millones).

CONTINÚA EN PRÓXIMA PÁGINA

CONSTRUYENDO CAPACIDADES DE CONEXIÓN A TRAVÉS DEL PROGRAMA BUILDING EUROPEAN LINK WITH LATIN AMERICA (BELLA)

Finalmente, y no menos importante es necesario hacer una mención al programa BELLA de EllaLink. Empresa que viene desarrollando un proyecto emblemático para la implementación de un cable submarino de fibra óptica de alta capacidad entre Fortaleza (Brasil) y Sines (Portugal). Este proyecto, es sumamente significativo para Latinoamérica en cuanto a estrategias para acortar brechas digitales, pues creará oportunidades para los intercambios y acceso de datos en diversos frentes.

El cable submarino cuenta con una longitud de 6.000 km y ha significado una inversión privada de 150 millones de euros. BELLA está siendo implementado por el Consorcio de Redes Regionales de Investigación y Educación conformado por GÉANT (Europa) y RedCLARA (América Latina), que incluye Redes Nacionales de Investigación y Educación (RNIE o NREN) de Chile, Colombia, Ecuador, Francia, Alemania, Italia, Portugal y España, además de la Red Nacional de Investigación (RNP), vinculada al Ministerio de Ciencia y Tecnología de Brasil.

LOGRANDO RESULTADOS

Los programas / proyectos citados no sólo serán decisivos para lograr los impulsos económicos, de salud, de educación y de gobierno que buscan los países en la región para recuperarse del COVID. Sino que delimitarán qué países estarán listos para seguir el ritmo que ya adoptó Europa, Asia y Estados Unidos en la transformación de sus industrias y el rol que jugarán las tecnologías disruptivas en la evolución empresarial y del sector gubernamental.

#BestPractices #BetterProfessionals

Cursos oficiales de Certificación

septiembre

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 3 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 4 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 10 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 11 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Martes 7 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 9 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 14 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 16 de Septiembre de 2021 de 16:00 a 21:00 horas

GESTIÓN POR PROCESOS

BPM PROFESIONAL ISO/IEC 19510

PRIMERA SESIÓN:
Viernes 17 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 18 de Septiembre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 24 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 25 de Septiembre de 2021 de 09:00 a 14:00 horas

GESTIÓN DE SERVICIOS

ITIL® 4 STRATEGIST: DIRECT, PLAN & IMPROVE

PRIMERA SESIÓN:
Martes 21 de Septiembre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 23 de Septiembre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 28 de Septiembre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Jueves 30 de Septiembre de 2021 de 16:00 a 21:00 horas

octubre

GESTIÓN DE SERVICIOS

ITIL® 4 FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 1 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 2 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 8 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN
Sábado 9 de Octubre de 2021 de 09:00 a 14:00 horas

GOBIERNO I&T

COBIT® 2019 FUNDAMENTOS + ISO 38500 PROFESIONAL

PRIMERA SESIÓN:
Martes 5 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 7 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 12 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
ISO/IEC 38500 a elegir por el Alumno.

GESTIÓN DE PROYECTOS

PRINCE2® FUNDAMENTOS

PRIMERA SESIÓN:
Viernes 15 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Sábado 16 de Octubre de 2021 de 09:00 a 14:00 horas

TERCERA SESIÓN:
Viernes 22 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Sábado 23 de Octubre de 2021 de 09:00 a 14:00 horas

GESTIÓN OFICINAS DE PROYECTOS

P3O® FUNDAMENTOS

PRIMERA SESIÓN:
Martes 19 de Octubre de 2021 de 16:00 a 21:00 horas

SEGUNDA SESIÓN:
Jueves 21 de Octubre de 2021 de 16:00 a 21:00 horas

TERCERA SESIÓN:
Martes 26 de Octubre de 2021 de 16:00 a 21:00 horas

CUARTA SESIÓN:
Jueves 28 de Octubre de 2021 de 16:00 a 21:00 horas

Business&Co®
Business, Technology & Best Practices, S.L.

Más información en
https://javierperis.com/formacion-oficial/