

REVISTA PARA EMPRESAS

Soluciones

Tecnología, seguridad y gestión para hacer crecer su negocio



EN ESTA EDICIÓN

- Datos personales: las obligaciones que casi nadie conoce y a casi todos alcanzan
- WiFi que funciona: por qué se cae y qué hacer al respecto
- Renovar o reparar: cuánto cuesta realmente un equipo lento
- El eslabón humano: capacitar para que la tecnología rinda
- Cuando se cae internet: cómo armar el plan B de su empresa

EDITORIAL

Lo que ya tenemos, mejor aprovechado

La primera edición de **Soluciones** tuvo mejor recepción de la que esperábamos. Nos llegaron consultas, correcciones y —lo que más valoramos— preguntas nuevas. Varias de ellas dieron origen a los temas de estas páginas.

Si aquella edición habló de cimientos —proteger, respaldar, asegurar—, esta se ocupa de algo distinto y menos visible: **sacarle provecho a lo que la empresa ya tiene**, y ordenar las decisiones antes de que las ordene una urgencia.

Abrimos con un tema que sorprende a casi todos: las obligaciones que la ley de protección de datos personales impone a cualquier empresa que tenga clientes, empleados o cámaras. No es un asunto de grandes corporaciones; alcanza a comercios y talleres de nuestra ciudad, y casi nadie lo sabe. Lo tratamos de forma informativa, para que cada quien evalúe su situación con su asesor.

Después bajamos a tierra con lo cotidiano: por qué el WiFi se cae siempre a la misma hora, cuándo conviene reparar un equipo y cuándo ya no, cómo trabajar fuera de la oficina sin dejar la puerta abierta, y qué hacer el día que internet no vuelve.

Hay una nota que nos importa especialmente: la del eslabón humano. Después de veinte años instalando tecnología aprendimos que el mejor sistema, con personas que no saben usarlo, rinde la mitad. La capacitación no es un extra del proyecto: es parte del proyecto.

Cerramos con una autoevaluación de diez preguntas. Contéstelas con honestidad: probablemente le muestren, en cinco minutos, dónde está el eslabón más flojo de su empresa.

QUIÉNES SOMOS

2003

Año de fundación de Informática Arriba en Paso de los Toros.

7

Líneas de servicio: soporte técnico, cableado estructurado, alarmas y monitoreo, videovigilancia, venta de equipamiento, facturación electrónica y desarrollo de software propio.

+20

Años acompañando a empresas, comercios e instituciones de la región centro del país.

CERTIFICACIONES

- ▶ Hikvision HCSA / HCSP
- ▶ TP-Link Omada OCNA
- ▶ Nexxt ECC · Forza UPS
- ▶ Kaspersky Registered Partner

**Schurman González**

Director · Informática Arriba

SUMARIO

En esta edición

-
- 04** **Sus datos, su responsabilidad: la Ley 18.331 explicada**
Nota de tapa. Si su empresa tiene clientes, empleados o cámaras, la ley de protección de datos personales le aplica. Qué dice, qué obliga y qué mitos circulan.
-
- 06** **WiFi que funciona: por qué se cae y qué hacer**
La queja número uno de cualquier oficina. Por qué más router no es más cobertura y cuándo la solución pasa por el cable.
-
- 07** **Renovar o reparar: la vida útil del parque informático**
El costo invisible del equipo lento y cómo planificar el recambio antes de que algo muera en el peor momento.
-
- 08** **El eslabón humano: capacitar para que la tecnología rinda**
El mejor sistema, mal usado, rinde la mitad. Cómo formar al equipo sin frenar la operación.
-
- 09** **Trabajar fuera de la oficina sin abrir la puerta a cualquiera**
Acceso remoto, celulares y trabajo desde casa: qué es seguro, qué no, y el error que deja la empresa expuesta.
-
- 10** **Cuando se cae internet: el plan B de su empresa**
Sin conexión no hay facturación, ni cobros con tarjeta, ni monitoreo. Cómo seguir operando igual.
-
- 11** **¿Por dónde empezar? Diez preguntas para su empresa**
Una autoevaluación breve para descubrir cuál es hoy su eslabón más flojo.
-

SOLUCIONES es una publicación de **Informática Arroba** · Leandro Gómez 303, Paso de los Toros, Tacuarembó · Tel. 4664 5448 / 099 028 110 · infoarroba.com.uy · **Dirección:** Schurman González · **Comunicación y contenidos:** Verónica González · Los artículos tienen fines exclusivamente informativos y no constituyen asesoramiento jurídico, contable ni técnico particular. Para su caso concreto, consulte con un profesional.

NOTA DE TAPA

Sus datos, su responsabilidad: lo que la Ley 18.331 le pide a su empresa

Si su negocio tiene una lista de clientes, una planilla de sueldos o una cámara filmando la vereda, está tratando datos personales. Y eso, en Uruguay, tiene reglas desde hace más de quince años. Un repaso informativo por lo esencial.

Hay una idea instalada: que la protección de datos personales es asunto de bancos, mutualistas y grandes empresas. La realidad es más simple y más amplia. La Ley N° 18.331, de agosto de 2008, define como dato personal cualquier información que permita identificar a una persona o hacerla identificable: un nombre, una cédula, un teléfono, una imagen. Y define base de datos como cualquier conjunto organizado de esos datos, sin importar si está en un sistema, en una planilla o incluso en papel.

Con esas dos definiciones, el alcance queda claro: la lista de clientes del almacén, el registro de empleados del taller, la agenda de proveedores y las grabaciones de las cámaras son, todas, bases de datos personales.



Pieza de la campaña de difusión de la Unidad Reguladora y de Control de Datos Personales (URCDP), organismo que fiscaliza el cumplimiento de la ley en Uruguay.

El registro ante la URCDP. La ley crea la Unidad Reguladora y de Control de Datos Personales como organismo de contralor, y establece que las bases de datos personales deben inscribirse en su registro. El criterio se ordena por finalidad: en un mismo sistema pueden convivir varias bases distintas —clientes, empleados, proveedores, videovigilancia— y cada una se inscribe por separado. El trámite se inicia en el portal de la URCDP.

Los principios que ordenan todo. Más allá del trámite, la ley fija principios que valen para cualquier tratamiento de datos: legalidad, finalidad (los datos se usan solo para aquello que se declaró), consentimiento informado del titular, veracidad, reserva y seguridad. Este último obliga al responsable a adoptar medidas que eviten la pérdida, adulteración o acceso no autorizado a la información: acá la obligación legal y la buena práctica técnica coinciden exactamente.

Y los derechos del otro lado. Toda persona puede pedir acceder a los datos que una empresa tiene sobre ella, rectificarlos si están mal y solicitar su supresión cuando corresponde. La empresa debe estar en condiciones de responder.

Las cámaras también son datos personales. Este es el punto que más sorprende. En su dictamen 10/2010, la URCDP estableció que la videovigilancia —toda grabación, captación, transmisión y almacenamiento de imágenes— constituye información personal, y que por tanto le aplica toda la normativa de protección de datos.

De ahí se desprenden obligaciones concretas para quien tiene cámaras: inscribir la base de videovigilancia, informar a las personas que están siendo filmadas y adoptar un distintivo —el cartel— cuya matriz proporciona la propia URCDP, respetando sus colores y proporciones. Ese cartel debe indicar ante quién y en qué domicilio se pueden ejercer los derechos que la ley reconoce.

Hay además límites sobre dónde filmar. Las cámaras pueden instalarse en los recintos de trabajo, pero no en baños, vestuarios, espacios de descanso ni lugares destinados a la alimentación. A los empleados debe informárseles que se instalarán cámaras, dónde estarán ubicadas y si captan sonido. Y el equipo de grabación debe estar en un lugar de acceso restringido, accesible solo a personal autorizado — un detalle que en la práctica

se resuelve con un gabinete con llave, y que en muchos comercios simplemente no existe.

Cuando algo sale mal. Desde el Decreto 64/020, que reglamenta la reforma introducida por la Ley 19.670, existe una obligación que conviene conocer antes de necesitarla: constatada una vulneración de seguridad que afecte datos personales, el responsable debe comunicarla a la URCDP en un plazo máximo de 72 horas, con la fecha, la naturaleza del incidente, los datos afectados y los posibles impactos. Si la afectación a las personas es significativa, también hay que informarles a ellas, en lenguaje claro. Dicho de otro modo: el día del ataque informático no solo hay que recuperar los sistemas, también hay un reloj corriendo.

El mismo decreto incorporó la figura del delegado de protección de datos, obligatoria para las entidades públicas, las privadas que tratan datos sensibles como negocio principal y las que manejan grandes volúmenes de datos. La enorme mayoría de las pymes queda fuera de esa exigencia — pero no de las anteriores.

LO QUE SE ESCUCHA	LO QUE DICE LA NORMATIVA URUGUAYA
"Las grabaciones se guardan 30 días, es la ley."	Ese plazo pertenece a la normativa española, no a la uruguaya. Acá rige el principio de finalidad: agotada la finalidad que justificó el sistema, corresponde eliminar los registros. El plazo se define y documenta según cada caso.
"Esto aplica solo a empresas grandes."	Alcanza a toda persona física o jurídica que trate datos personales fuera del ámbito exclusivamente personal o doméstico.
"Si no está en un sistema, no cuenta."	La ley habla de tratamiento electrónico o no: un fichero en papel organizado también es base de datos.
"No pasa nada si no cumplo."	La ley prevé un régimen sancionatorio que va desde la observación y la multa hasta la suspensión y la clausura de la base de datos.

CINCO PREGUNTAS PARA HACERSE ESTA SEMANA

- ▶ ¿Qué bases de datos personales tiene mi empresa, y cuál es la finalidad de cada una?
- ▶ ¿Están inscriptas en el registro de la URCDP?
- ▶ ¿Tengo el distintivo de videovigilancia con los datos del responsable?
- ▶ ¿El grabador está en un lugar con acceso restringido?
- ▶ ¿Sabría a quién avisar, y en cuánto tiempo, si mañana sufro un incidente?

Nota: este artículo tiene fines informativos y divulgativos. No constituye asesoramiento jurídico. La información oficial y los formularios se encuentran en el sitio de la URCDP (gub.uy/urcdp); para la situación concreta de su empresa, consulte con su asesor legal.

CONECTIVIDAD

WiFi que funciona: por qué se cae y qué hacer

“Anda lento”, “se corta”, “en el depósito no llega”. Es la queja más repetida en cualquier empresa — y casi siempre tiene una causa concreta, identificable y solucionable.

Primero: distinguir dos problemas distintos. Que “no ande internet” y que “no llegue el WiFi” son cosas diferentes, y confundirlas lleva a gastar mal. El internet es lo que entra al local por el módem del proveedor: tiene una velocidad contratada que se reparte entre todos. El WiFi es cómo esa conexión se distribuye por el aire dentro del edificio. Si el problema es de velocidad contratada, cambiar el router no cambia nada. Si el problema es de cobertura, contratar más megas tampoco.



Un punto de acceso ubicado según el plano del local cubre mejor que un router potente puesto donde entra el cable.

Por qué un solo router no alcanza. El router del proveedor está pensado para un hogar y suele quedar donde entró el cable: un rincón, una oficina del fondo, detrás de una estantería metálica. Las paredes gruesas, los entrepisos, las cámaras frigoríficas y las estructuras metálicas absorben la señal. Sumar potencia no resuelve:

el equipo puede llegar a un dispositivo lejano, pero ese dispositivo —un celular— no tiene fuerza para responderle. La solución no es un router más potente, sino varios puntos de acceso bien ubicados y conectados por cable, que se reparten el trabajo y permiten que un dispositivo pase de uno a otro sin cortes.

El vecino también pesa. El WiFi funciona en canales compartidos. En una zona céntrica, con decenas de redes superpuestas, los equipos pierden tiempo esperando turno. Una configuración de canales correcta y el uso de la banda de 5 GHz —más rápida y menos congestionada, aunque de menor alcance— mejoran muchísimo sin comprar nada nuevo.

Cuántos dispositivos aguanta. Un router doméstico puede anunciar decenas de conexiones, pero en la práctica se degrada mucho antes. Y hoy una empresa chica conecta más de lo que cree: computadoras, celulares del personal, celulares de clientes, cámaras, POS, impresoras, televisores. Contar los dispositivos reales suele explicar la lentitud de las cinco de la tarde.

Lo que rara vez conviene: encadenar repetidores. Cada repetidor retransmite por el mismo aire que recibe y reduce la capacidad a la mitad; dos o tres en cascada terminan de arruinar lo que venían a mejorar.

ANTES DE COMPRAR OTRO EQUIPO, REVISE ESTO

- ▶ ¿El problema es de velocidad contratada o de cobertura? Son soluciones distintas.
- ▶ ¿Dónde está físicamente el router? ¿Hay metal o paredes gruesas alrededor?
- ▶ ¿Cuántos dispositivos hay conectados de verdad, contando celulares y cámaras?
- ▶ ¿La red de clientes está separada de la red de trabajo?
- ▶ ¿Hay repetidores encadenados? Suelen ser parte del problema.
- ▶ ¿Se puede llevar un cable hasta el punto conflictivo? Suele ser lo más barato y estable.

PLANIFICACIÓN

Renovar o reparar: el costo invisible del equipo lento

Una computadora que tarda en abrir todo no se siente como un gasto, porque no hay factura. Pero el tiempo que se pierde todos los días sí tiene precio — y suele ser mayor que el del equipo nuevo.

Hagamos la cuenta sin exagerar. Supongamos media hora perdida por día entre esperas, cuelgues y reinicios. Son unas diez horas al mes por persona; más de una jornada laboral entera. En un año, semanas completas de trabajo pago que no produjeron nada. Multiplíquelo por la cantidad de puestos de su empresa y va a entender por qué muchas veces renovar es más barato que aguantar.



Diagnóstico en banco: antes de decidir entre reparar o renovar conviene saber qué está fallando realmente.

Cuándo reparar tiene sentido. Hay mejoras de costo bajo y efecto enorme, sobre todo en equipos de pocos años. Cambiar un disco mecánico por uno de estado sólido suele transformar una máquina lenta en una perfectamente usable. Ampliar memoria, reemplazar una fuente o limpiar y reacondicionar térmicamente son

intervenciones que extienden la vida útil por bastante tiempo.

Cuándo la reparación deja de convenir. Cuando la falla está en la placa principal; cuando el equipo ya no admite el sistema operativo con soporte vigente; cuando los repuestos son difíciles o caros; cuando la máquina viene fallando repetidamente. Una regla práctica bastante buena: si el arreglo supera la mitad del valor de un equipo nuevo equivalente, o si la falla es la tercera del año, conviene renovar.

El punto que casi nadie mira: el soporte del sistema. Un equipo puede encender perfecto y aun así ser un problema, si su sistema operativo dejó de recibir actualizaciones de seguridad. Ahí no se trata de velocidad sino de riesgo: es una puerta que ya no se cierra más.

Renovar por tercios. El error más común es esperar a que todo muera junto y enfrentar un desembolso grande en el peor momento. La alternativa es simple: llevar un inventario con la antigüedad de cada equipo y renovar cada año el tercio más viejo. El gasto se vuelve previsible, nunca hay un parque completamente obsoleto y la empresa deja de comprar bajo presión.

SEÑALES DE QUE UN EQUIPO YA PIDE RELEVO

- ▶ Tarda varios minutos en estar operativo desde que se enciende.
- ▶ El usuario “aprovecha para hacer otra cosa” mientras abre un programa.
- ▶ Se apaga solo, se recalienta o hace ruidos nuevos.
- ▶ Su sistema operativo ya no recibe actualizaciones de seguridad.
- ▶ Es la tercera reparación en menos de un año.
- ▶ No puede con el sistema de gestión actualizado.

CAPACITACIÓN

El eslabón humano: capacitar para que la tecnología rinda

Se invierte en equipos, en sistemas y en licencias. Y después se entrega todo eso a personas que aprendieron a usarlo mirando por encima del hombro de un compañero. Ahí se pierde la mitad de la inversión.



Instancia de capacitación con clientes: cada función que el equipo no conoce es inversión que no rinde.

Es una escena que vemos seguido: una empresa compra un sistema de gestión completo y termina usando el veinte por ciento de sus funciones. No porque el sistema sea malo ni porque el personal sea reticente, sino porque nadie dedicó tiempo a enseñar. La capacitación se posterga —siempre hay algo más urgente— y el equipo se arregla con lo mínimo que descubrió solo.

Los tres costos de no capacitar. El primero es el más obvio: funciones pagas que no se usan. El segundo es el tiempo: tareas que el sistema podría hacer solo se siguen haciendo a mano, y se duplican datos en planillas paralelas. El tercero es el más caro: los errores. Un comprobante mal emitido, un cliente cargado dos veces, un descuento aplicado donde no iba. Nada de eso es culpa del usuario; es falta de formación.

Y el riesgo de seguridad. La estadística es contundente en todo el mundo: la mayoría de los incidentes informáticos empieza con una persona que hizo clic donde no debía. Ningún antivirus compensa a un equipo

de trabajo que no sabe reconocer un correo falso. Capacitar en seguridad es, hoy, la inversión de mejor retorno que puede hacer una empresa chica.

Cómo hacerlo sin frenar la operación. La capacitación no tiene por qué ser un curso de ocho horas que nadie puede tomarse. Funcionan mejor los formatos cortos y repetidos: media hora por tema, con casos reales de la empresa. Funciona designar un referente interno por área, que reciba formación un poco más profunda y sea la primera consulta de sus compañeros. Funciona documentar los procedimientos en una guía breve, con capturas de pantalla, que sobreviva a la rotación de personal. Y funciona incorporar la capacitación al alta de cada nuevo ingreso, antes de que aprenda mal.

Medirlo. Si después de una capacitación bajan las consultas repetidas al soporte y bajan los errores de carga, funcionó. Si no cambia nada, hay que cambiar el enfoque, no repetir la misma charla.

CUATRO MOMENTOS DONDE CAPACITAR RINDE MÁS

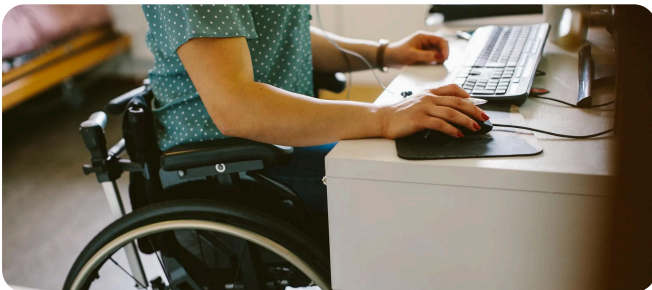
- ▶ **Al implementar** un sistema nuevo: antes de que se instalen las malas costumbres.
- ▶ **Al ingresar** una persona: media hora el primer día ahorra meses de errores.
- ▶ **Al actualizar:** las funciones nuevas no se usan solas.
- ▶ **Una vez al año** en seguridad: es lo que mantiene viva la atención del equipo.

TRABAJO A DISTANCIA

Trabajar fuera de la oficina sin abrir la puerta a cualquiera

Consultar el stock desde el celular, facturar desde casa, revisar las cámaras de viaje. Todo eso es posible y útil. El problema aparece cuando la puerta que se abre para entrar queda abierta también para los demás.

La necesidad es legítima y cada vez más común. El tema es cómo se resuelve. Y en la práctica hay dos caminos: el que un técnico diseña, y el que alguien improvisa un viernes a la tarde porque necesitaba entrar desde casa. El segundo es el que genera los incidentes.



El acceso a distancia amplía las posibilidades de trabajo: la clave es que esté diseñado, no improvisado.

El error más peligroso: publicar el escritorio remoto directamente a internet. Es decir, dejar el equipo de la empresa accesible desde cualquier parte del mundo con solo un usuario y una contraseña. Los atacantes recorren internet de forma automática buscando exactamente eso, y una vez dentro tienen el mismo acceso que el dueño. Muchos casos de ransomware en pymes empiezan así.

El camino correcto tiene tres capas. Primero, una VPN: un túnel cifrado que conecta al usuario con la red de la

empresa como si estuviera sentado adentro, sin exponer nada al exterior. Segundo, *verificación en dos pasos*: además de la contraseña, un código en el celular. Aunque alguien robe la clave, no entra. Tercero, *permisos por persona*: cada usuario accede solo a lo que necesita para su tarea, y cuando alguien deja la empresa, su acceso se da de baja ese mismo día.

El celular es una computadora más. Si desde el teléfono personal se ve el sistema de gestión, el correo de la empresa o las cámaras, ese teléfono forma parte de la infraestructura. Debe tener bloqueo de pantalla, sistema actualizado y capacidad de desvincularse si se pierde o se cambia.

Los programas de escritorio compartido que tanto se usan para dar soporte son útiles, pero no deberían quedar instalados y permanentemente activos con una contraseña fija. Se habilitan para la sesión de soporte y se cierran al terminar.

Y una política escrita. Corta, de una carilla: quién puede acceder desde afuera, desde qué dispositivos, a qué información, y qué hacer si se pierde un equipo. Que exista y que el personal la conozca ya evita la mayoría de los problemas.

CONTINUIDAD

Cuando se cae internet: el plan B de su empresa

Hoy, sin conexión, muchas empresas directamente no pueden vender: no emiten comprobantes, no cobran con tarjeta, no consultan stock y no monitorean las alarmas. Y sin embargo, casi ninguna tiene previsto qué hacer.

Vale la pena hacer el ejercicio con honestidad: si mañana a las diez de la mañana se corta internet y no vuelve hasta la tarde, ¿qué puede seguir haciendo su empresa? En muchos casos la respuesta es incómoda. La conexión dejó de ser un servicio de oficina para convertirse en infraestructura crítica, al nivel de la energía eléctrica — pero rara vez recibe el mismo tratamiento.

Una segunda conexión, por otro camino. El principio básico de cualquier respaldo es que no comparta el punto

de falla. Dos servicios del mismo proveedor por el mismo cable se caen juntos. La combinación que funciona es una conexión principal por cable o fibra y una secundaria por red móvil: si se corta la calle, la señal celular sigue. Hoy existen routers que hacen ese cambio en forma automática, sin que nadie tenga que reconfigurar nada: el personal, en el mejor de los casos, nota una pausa de segundos.



Esquema de una red con conexión de respaldo: el equipo detecta la caída del enlace principal y conmuta automáticamente a la red móvil.

Qué priorizar si el respaldo es acotado. Una conexión de emergencia por red móvil no va a sostener el consumo completo de la empresa, y no hace falta que lo haga. Lo importante es definir de antemano qué es esencial —la facturación, el cobro con tarjeta, el monitoreo de alarmas— y qué puede esperar, y configurar los equipos para que respeten esa prioridad. Esa decisión se toma antes, con calma; nunca durante el corte.

El procedimiento en papel. La tecnología resuelve una parte; el resto es organización. ¿Quién avisa al proveedor y con qué número? ¿Qué le decimos al cliente que está esperando en la caja? ¿Cómo se registran las

operaciones para cargarlas cuando vuelva el servicio? Un instructivo de una carilla, pegado cerca del mostrador, vale más que cualquier equipo el día que hace falta. Y conviene incluir las previsiones que la normativa de facturación electrónica establece para operar en contingencia: su proveedor de facturación puede indicarle exactamente cómo proceder.

Un detalle que se olvida siempre: la UPS. De nada sirve una conexión de respaldo si el módem, el router y el switch se apagan con el corte de luz que provocó la caída. Los equipos de comunicación deben estar respaldados igual que el servidor.

CINCO MINUTOS

¿Por dónde empezar? Diez preguntas para su empresa

Los temas de esta edición, convertidos en preguntas concretas. Respóndalas con honestidad: no hay nadie mirando, y el resultado es solo para usted.

MARQUE CON SINCERIDAD	SÍ	NO
1. ¿Sé exactamente qué bases de datos personales tiene mi empresa y si están inscriptas ante la URCDP?	☐	☐
2. ¿Mis cámaras tienen el distintivo de videovigilancia y el grabador está en un lugar de acceso restringido?	☐	☐
3. ¿La red WiFi de clientes está separada de la red donde trabajan mis sistemas?	☐	☐
4. ¿Tengo un inventario con la antigüedad de cada equipo y un criterio de renovación?	☐	☐
5. ¿Todos mis equipos usan un sistema operativo que aún recibe actualizaciones de seguridad?	☐	☐
6. ¿Mi personal recibió alguna capacitación formal sobre el sistema de gestión y sobre seguridad en el último año?	☐	☐
7. ¿Quien accede desde afuera lo hace por un canal seguro, con verificación en dos pasos?	☐	☐
8. ¿Se dan de baja los accesos el mismo día que una persona deja la empresa?	☐	☐
9. ¿Tengo una conexión a internet de respaldo y un procedimiento escrito para trabajar sin conexión?	☐	☐
10. ¿El módem, el router y el switch están respaldados por UPS, igual que el servidor?	☐	☐

8 a 10

Su empresa está mejor preparada que la media. Conviene revisar lo pendiente antes de que se vuelva urgente.

4 a 7

La situación más habitual. Hay bases sólidas y huecos concretos: ordenarlos por riesgo y resolverlos de a uno.

0 a 3

Vale la pena tomarse un rato para revisarlo. No hace falta resolver todo junto, pero sí empezar.

“Ninguna empresa responde diez veces que sí. La diferencia no está en tenerlo todo resuelto, sino en saber qué falta.”

¿Marcó más de tres “no”?

Conversemos. Podemos revisar juntos cualquiera de los temas de esta edición y ayudarle a ordenar prioridades, sin compromiso.

4664 5448

099 028 110

infoaroba.com.uy

ACOMPANIAMIENTO TECNOLÓGICO

Cada nota de esta revista empezó con una consulta real

Los temas que leyó en estas páginas no salieron de un manual: salieron de preguntas que nos hicieron clientes como usted, en visitas, llamados y mensajes de WhatsApp. Si alguno le quedó dando vueltas, escribanos. Conversarlo no cuesta nada y suele ser el primer paso para resolverlo.



El equipo de Informática Arroba: tecnología con nombre, apellido y respuesta local.

TRABAJAMOS CON MARCAS CERTIFICADAS

HIKVISION



forza
POWER TECHNOLOGIES

NEXXT
SOLUTIONS
INFRASTRUCTURE



Conversemos sobre su empresa

Leandro Gómez 303 · Paso de los Toros, Tacuarembó
Tel. 4664 5448 · Cel. 099 028 110 · infoarroba.com.uy

Diagnóstico sin costo
para empresas de la región.

Solicite su visita.