G55CIO

EL PUNTO DE ENCUENTRO DEL CIO Y CEO

Año 1
Nº 27
Agosto 2017

Es NECESARIA una visión estratégica de la SEGURIDAD

La ciberseguridad es una tarea diaria y constante para las personas y las empresas, afirma Franz Erni Montes, country manager de Fortinet para Perú, quien sostiene que en la actualidad las tecnologías son fundamentales para el desarrollo de las firmas.

SUMARIO

4

EN PORTADA
Martín Hoz, Fortinet
Vivimos una época muy emocionante

6

TIEMPOS DEL CIO Y CEO
Franz Erni Montes - Fortinet
Es necesaria una visión estratégica de la seguridad

8

ARTÍCULO
Armando Cuyubamba Pereda - G55CIO
Ciberseguridad e infraestructuras físicas

10

MAS ALLÁ DEL NEGOCIO
Martín Iván Vilchez Vitela
Faonet System
Desafíos cumplidos

11

MUJERES EN TECNOLOGÍA
Yolanda Rojas Semorile
Evolve Systems
Esencia de éxito

G55CIO

G55CIO es una publicación semanal, editada en Perú por Grupo Bitácora

Director Ejecutivo
Manuel Díaz
manuel.diaz@grupobitacora.biz

Gerente General
Beatriz López
beatriz.lopez@grupobitacora.biz

Redacción
Armando Cuyubamba
armando.cuyubamba@grupobitacora.biz

Redacción - Colaboradora
Elizabeth Ururi Prinz

Arte y Diseño
Karelín Reyes
karelin.reyes@grupobitacora.biz

Fotografía y Banco de Imágenes
Fabricio Díaz López
fabricio.diaz@grupobitacora.biz

Atención al cliente y Suscripciones
suscripcion@grupobitacora.biz

Publicidad
publicidad@grupobitacora.biz

Se prohíbe la reproducción total o parcial del contenido de esta revista sin autorización del Director Ejecutivo. Los anuncios, artículos firmados y las opiniones de los entrevistados no refleja necesariamente la opinión del medio.

Una publicación de:
Grupo Bitácora

EDITORIAL

Alcances sobre ciberseguridad

En diversas ediciones de G55CIO nos hemos ocupado de la ciberseguridad (un mínimo de riesgos para el ciberespacio) y los ciberataques. Nuestro propósito es clarificar el panorama y promover la proactividad y la resiliencia (capacidad para recuperarse frente a la adversidad para seguir proyectando el futuro) en el sector.

Sobre la ciberseguridad podemos afirmar que es un asunto que debemos plantearnos a escala global, ya que los ciberataques se producen normalmente desde países lejanos donde resulta muy difícil su persecución. Por algo, el reciente ransomware denominado WannaCry afectó a más de 45.000 sistemas informáticos en 74 países (incluyendo el Perú) alrededor del mundo.

Es vital, entonces, proteger la confidencialidad, la integridad y la disponibilidad de la información digital que circula en este ambiente, tanto del Estado como de los ciudadanos.

Se sabe que la vía de entrada de los ciberdelitos es por electrónico, redes sociales y smartphone. Asimismo, los datos más susceptibles de robo son información personal y claves bancarias.

Por otro lado, -informa Amcham Chile-, según la Cumbre Latinoamericana de Analistas de Seguridad, entre agosto de 2015 y agosto de 2016, Latinoamérica alcanzó un millón cien mil ataques de malware al año, 12 por segundo. En tanto, el Informe de Ciberseguridad desarrollado por el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA), indica que cuatro de cada cinco países de la región no tienen estrategias de ciberseguridad o planes de protección de infraestructura; dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética y -lo que es peor- la gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos.

Frente a esta realidad, países de la región como Uruguay, Brasil, México, Argentina, Colombia y Chile se encuentran en un nivel intermedio de madurez de ciberseguridad, pero lejos de referentes como Estados Unidos, Israel, Estonia y Corea, donde su protección es alta y es prioridad para los gobiernos. Es evidente que los impactos de no contar con adecuadas medidas a nivel personal y empresarial son muchos y van más allá de lo económico.

A manera de reflexión, ¿qué medidas de ciberseguridad emplea Ud. en su vida diaria y en su ambiente laboral? Por nuestra parte, le sugerimos que antes de compartir un selfie en sus redes sociales tome conciencia sobre la información visual que podría divulgar y al público que potencialmente alcance a visualizar la imagen que captó con su dispositivo.

El Director

Vivimos una época muy emocionante

Martín Hoz, vicepresidente de Soporte Técnico e Ingeniería de Ventas de Fortinet para Latinoamérica y el Caribe dice que, en la cuarta revolución industrial, época inusual por los grandes cambios en la humanidad generados por las tecnologías, las organizaciones deben prepararse para el presente y el futuro.

Los smartphones, las tabletas, los wereables, entre otros dispositivos, nos permiten el acceso a datos y la recolección de información, los cuales se identifican con la Tercera Plataforma -la actual era de la evolución de las Tecnologías de la Información (TI).

Como sabemos, los pilares en los que se asienta esta Plataforma (tecnología social, dispositivos móviles, big data y computación en la nube) han modificado por completo las actividades humanas, los ecosistemas empresariales y los desarrollos de los mercados.

"Todo eso ocurre en la cuarta revolución industrial donde se despliega la transformación digital, una evolución de los procesos de negocios de las organizaciones para adaptar las tecnologías disponibles que les permitan mejorar, ser más eficientes, más rápidas, más personales, más móviles y más sociales", señaló Martín Hoz, vicepresidente de Soporte Técnico e Ingeniería de Ventas de Fortinet para Latinoamérica y el Caribe.

Aseguró que los sistemas tecnológicos penetran cada vez más las cadenas de valor de todas las organizaciones y es necesario que aprendamos cómo se realiza este proceso.

Asimismo, anotó que los referidos cuatro pilares de la Tercera Plataforma promueven el desarrollo de nuevas tecnologías que, a su vez, permiten ofrecer innovadores productos, bienes, servicios y soluciones. "Por eso, la cuarta revolución industrial es un movimiento económico y no tecnológico. En tal sentido, así como se mueven los negocios y se genera dinero, también los delincuentes están a la expectativa", advirtió.

Hoz subrayó que en la actualidad el ciberdelito es una actividad organizada que se estima tiene ganancias monetarias similares o superiores -según organizaciones mundiales- que otras ocupaciones criminales como la trata de personas y el narcotráfico.

Expresó que, con el acceso masivo a Internet, una mayor disponibilidad de las tecnologías y el desarrollo de los dispositivos móviles al alcance de los usuarios, se "han abierto varias ventanas a los ciberatacantes".

"Al emplear la tecnología masivamente también se debe proteger la reputación de los clientes, recolectando su información adecuadamente y protegiéndola", enfatizó.

Tecnologías para todos

Para Martín Hoz, la humanidad está viviendo una época muy emocionante, y el mundo que vivimos cuando nacimos será muy diferente al que dejaremos. "No existe otra generación en la historia de la humanidad que haya experimentado varios cambios. Sin duda, la tecnología se aproxima cada vez más a la vida de los seres humanos, y es imprescindible que este acercamiento sea seguro, adecuado y tranquilo para las personas, las empresas y la sociedad en general", afirmó.

En otro momento del diálogo con G55CIO, recordó que antes las computadoras personales solo se empleaban como plataformas de procesamientos de datos, sin embargo, "ahora la tecnología de cómputo es una plataforma que nos permite hacer muchas actividades; incluso el trabajo en oficina se puede sintetizar en interactuar mediante correos electrónicos, chat y llamadas telefónicas".

Indico que al margen de la ocupación o actividad que cada persona tiene, es necesario el empleo de las tecnologías en el presente, situación que hace más relevantes a los tecnólogos, quienes deben crear espacios adicionales en sus compañías para que innoven sus modelos de negocios.

"La tecnología es permeable en todos los segmentos sociales y eso origina que las empresas generen sinergias, aprovechamientos y optimizaciones en áreas nuevas de negocios. Todos empleamos las tecnologías, en consecuencia, las organizaciones esperan convertirse en empresas tecnológicas", precisó.

El ejecutivo agregó: "Las compañías que aprovechan las tecnologías -sin importar el segmento económico en el que se encuentren- pueden generar más valor a sí mismas, captar más clientes, llegar a donde antes no tenían presencia comercial, y generar productos y servicios que antes no existían".

"Todo más rápido"

Sobre la participación de los ejecutivos empresariales en la toma de decisiones, Martín Hoz comentó que cada vez los gerentes de Marketing tienen menos relevancia, a diferencia de otros cargos (directores de seguridad de la información, responsables de la seguridad de las organizaciones, gerentes de sistemas y directores de tecnología), cuyos responsables empiezan a ser escuchados por los máximos directivos.

> "La tecnología es permeable en todos los segmentos sociales y eso origina que las empresas generen sinergias, aprovechamientos y optimizaciones"

"Ahora los usuarios queremos todo más rápido cuando vamos al banco a realizar una transacción, o a una tienda para cancelar los productos adquiridos, o cuando realizamos un trámite en una entidad pública. Es necesario pensar en la agilidad, la simplicidad y la compatibilidad de las actividades que se pueden hacer con el respaldo de las TI", apuntó.

"La cuarta revolución industrial es un movimiento económico y no tecnológico"

Es necesaria una visión estratégica de la seguridad

La ciberseguridad es una tarea diaria y constante para las personas y las empresas, afirma Franz Erni Montes, country manager de Fortinet para Perú, quien sostiene que en la actualidad las tecnologías son fundamentales para el desarrollo de las firmas.

"Es vital repensar y concebir la seguridad en las compañías donde laboramos"

Las Tecnologías de la Información (TI) cumplen un rol protagónico en la cuarta revolución industrial, medio que está influenciado a las personas, las empresas, los mercados y las naciones.

En esta era histórica -la actual- es impresionante cómo se desarrolla y beneficia una organización directamente con el empleo de las TI. Así lo dijo Franz Erni Montes, country manager de Fortinet para Perú y Bolivia, tras señalar que cada vez las empresas dependen mucho de las tecnologías.

"Esta situación en sí es buena. Sin embargo, genera otro tipo de riesgos como la ciberdelincuencia ejecutado por los hackers y otro tipo de delincuentes que se proponen llegar a los sistemas empresariales", aseguró.

La masificación de la Internet ha originado un mayor acceso a la información de las personas, pero también ha promovido el desarrollo de los virus, malware, spyware, spam, phishing, pharming, ransomware, entre otros tipos de ciberataques. "Incluso, -advirtió Erni- cada cierto tiempo se informa en los medios que piratas cibernéticos roban películas de estudios cinematográficos exigiendo altas sumas de dinero para no divulgar los largometrajes en Internet".

Integración digital

En conversación con G55CIO, Franz Erni expresó que la Red Dorsal Nacional de Fibra Óptica (RDNFO) es fundamental para la integración digital del país porque a través de la conectividad es posible llegar a los lugares recónditos del territorio nacional y reducir la brecha entre las personas y las empresas.

"Internet habilitó a los individuos y a las organizaciones para que realicen nuevas actividades que las ayuden a transformarse, trabajar mejor, emplear las nubes privadas y públicas, ser más productivos, etc. Todo ello genera retos de ciberseguridad que deben asumirse para afrontar los cambios", subrayó.

Asimismo, enfatizó que cuando el usuario abre puertas digitales para ser más efectivo y eficiente en sus labores, potencialmente puede ser vulnerable en el campo de la seguridad de su información. Al respecto, acotó: "Es vital repensar y concebir la seguridad en las compañías donde laboramos. Eso va más allá de la implementación de productos y soluciones para mejorar una infraestructura tecnológica empresarial, por eso, es necesaria una visión estratégica de la seguridad".

> "Internet ha habilitado a los individuos y a las organizaciones para que realicen nuevas actividades que las ayuden a transformarse"

En el top of mind

De otro lado, Erni Montes apuntó que su representada está en el top of mind de los Chief Information Officer (CIO) y ejecutivos empresariales. "En consecuencia, Fortinet tiene un lugar bien ganado y los gerentes confían mucho en nosotros. Como fabricantes queremos que nos vean como un socio estratégico de negocios de cara hacia su ciberseguridad", anotó.

Fortinet se creó en el 2000 en los Estados Unidos y luego de dos años -tiempo dedicado a la investigación y desarrollo- lanzó su primer producto. La compañía multinacional se originó bajo el concepto de simplificar, consolidar y hacer que sus clientes empresariales tengan un nivel de seguridad alto, sin que este proceso sea complejo.

El entrevistado manifestó que hace siete años Fortinet estableció una oficina local en Lima y consideró que en el mercado corporativo se sitúan en el primer lugar.

"Fortinet, en este ámbito, no tiene competencia porque somos los únicos que ofrecemos al mercado mundial un portafolio completo de soluciones de seguridad integral, así como la mejor estrategia de arquitectura de seguridad TI", refirió.

Precisó, además, que la compañía se adaptó a la realidad de la seguridad de la información y lo hizo con innovación. "Eso es muy importante porque nos permite estar un paso adelante. Nuestro mensaje como fabricante es que los clientes no ignoren la ciberseguridad en sus agendas diarias", puntualizó.

El Entrevistado

Como gerente de Territorio de Perú y Bolivia, Franz Erni lidera el desarrollo comercial de Fortinet en dichos mercados, asimismo, es el responsable del desarrollo y la ejecución de estrategias con canales de venta y distribución, y de los equipos de profesionales de la compañía en ambas naciones. Erni se ha desempeñado en una gran variedad de posiciones relacionadas con la visión global de las Tecnologías de la Información y la seguridad. Cuenta con la certificación de Jefe Auditor ISO 27001 de BSI Group, entre otras de distintas tecnologías.

Ciberseguridad e infraestructuras físicas

Es indispensable que la ciberseguridad se despliegue en casi todas las actividades humanas vinculadas con las Tecnologías de la Información, con mayor razón en ámbitos estratégicos para el desarrollo de la sociedad como las infraestructuras críticas. Armando Cuyubamba, nuestro redactor principal, nos aproxima a esta realidad.

Probablemente Ud. acostumbra tomarse un selfie (autofoto hecho por uno mismo con un teléfono inteligente, una cámara web o una cámara digital, para ser compartida, a través de redes sociales) en el cine, la playa, algún evento o en su casa y lo comparte a través de las redes sociales en las que participa activamente. Tenga cuidado con lo que publica, con mayor razón si acostumbra divulgar información (escrita o imágenes) desde su centro de labores, ya que puede facilitarles la labor a los cibercriminales.

Las áreas de infraestructura crítica para un país y su entorno comprenden plantas de tratamiento de aguas (presas y redes de distribución); centrales eléctricas y de gas natural (incluye redes); hospitales; transportes (aeropuertos y terminales de autobuses); plantas químicas y nucleares (incluye el transporte de mercancías de manejo riesgoso como materiales químicos, biológicos y radiológicos); sistemas financieros (bancos, bolsas de valores) y recaudadores de impuestos; plantas de reciclaje; sistemas de control de tráfico, entre otras. Todos estos locales son potenciales objetivos para los cibercriminales, quienes pueden obtener de las redes sociales información divulgada por los colaboradores de estos centros de trabajo.

Cabe señalar que, para la Estrategia Digital Nacional, en Materia de las TIC, y en la de Seguridad de la Información de México, las infraestructuras críticas, son "infraestructuras de información esenciales consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales, y cuya afectación pudiera comprometer la Seguridad Nacional en términos de la Ley de la materia".

¿Cuáles son los motivos que originan los ciberataques en las infraestructuras críticas? Al margen del aumento de estos ciberdelitos en el mundo, los motivos -entre otros factores- son porque la superficie de ataque es mayor; además la cantidad de vulnerabilidades va en aumento afectando a este tipo de infraestructuras, sumando a los canales tradicionales, las comunicaciones IP, las inalámbricas, los dispositivos móviles. Asimismo, el manejo de sistemas operativos y aplicaciones comunes ha generado una mayor eficiencia en las operaciones y las mediciones, además de promover nuevos riesgos.

Muchos selfies

Según informa Panda Security, aunque parezca mentira, los expertos en seguridad informática han dado ya la voz de alarma: están encontrando en plataformas como Twitter, Facebook o Instagram demasiados selfies de empleados en este tipo de instalaciones. ¿Qué consecuencias puede tener este suceso?

De acuerdo con expertos de la seguridad informática en el sector industrial, que frecuentan exponer en foros especializados, han sido capaces de localizar en Instagram y Facebook, entre otras redes sociales, selfies de empleados en sus centros de trabajo en los que se veían claramente datos valiosos sobre los sistemas SCADA (por las siglas en inglés de Supervisión, Control y Adquisición de Datos).

Además, los especialistas han descubierto fotos panorámicas y hasta visitas virtuales por las salas de control y las instalaciones de infraestructuras críticas disponibles en las propias webs oficiales de estos sitios, al alcance de cualquiera que, con buenas o malas intenciones, sepa utilizarlas para extraer información (listas de trabajadores, cuadrantes de turnos, etc.).

Sistemas SCADA

Los sistemas informáticos que podrían resultar comprometidos por culpa de la indiscreción de los trabajadores se denominan SCADA y se utilizan comúnmente para gestionar todo tipo de procesos industriales, por lo que su seguridad es un asunto especialmente sensible.

> "Los especialistas han descubierto fotos panorámicas y hasta visitas virtuales por las salas de control y las instalaciones de infraestructuras críticas disponibles en las propias webs"

Permiten obtener -advierte Panda Security- información desde cualquier parte, y en tiempo real, sobre las operaciones automatizadas de una fábrica, de tal forma que la toma de decisiones y la gestión a distancia de este tipo de instalaciones resulta más sencilla y económica.

Como contrapartida, una intrusión en los sistemas por parte de un ciberatacante, sobre todo si llega a tomar el control o alterar el funcionamiento de las máquinas, podría resultar en daños muy graves o irreparables.

Caso en Ucrania

El 23 de diciembre de 2015 alrededor de 80.000 personas se quedaron sin electricidad durante seis horas abandonadas al frío de Ucrania, producto de un ataque de BlackEnergy, un virus informático (tipo troyano) considerado el primero de su género en originar un apagón eléctrico generalizado.

Como se recuerda, antes el virus Stunet -obra de Israel y Estados Unidos- dañó seriamente diversas centrales nucleares iraníes, pero no dejó a nadie sin luz.

Una de las consecuencias del BlackEnergy fue que el gobierno de Ucrania señaló a Rusia como responsable del apagón. Incluso, en su momento, este virus hizo saltar las alarmas al ser detectado en la red que controla el tráfico aéreo del aeropuerto de Ucrania.

BlackEnergy es sólo una de las piezas usadas en el ataque, realizado por mercenarios informáticos del más alto nivel, lo que hace suponer que quien puede pagar sus salarios tiene mucho dinero, posiblemente un gobierno. Por eso, Ucrania después de dos años de guerra con Rusia, no duda en señalar a este país como culpable. Los expertos no confirman ni desmienten esta hipótesis.

Recomendaciones

Por su parte, y sobre el tema, McAfee ha elaborado recomendaciones para proteger la infraestructura crítica.

Debido a que la protección de la infraestructura crítica es un problema de seguridad nacional es necesario crear una estrategia de ciberseguridad en cada país y así formar un frente de defensa que permita intercambiar eficientemente información de alertas, vulnerabilidades y amenazas para actuar rápida y coordinadamente.

Las autoridades podrían mejorar la capacidad de inteligencia al incluir la protección de la infraestructura crítica dentro de las responsabilidades del Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT).

Continuar con la implementación del Manual Administrativo de Aplicación General en las materias de Tecnologías de la Información y Comunicaciones (TIC), y en la de seguridad (MAAGTICSI).

Proseguir con la actualización del Catálogo de infraestructuras críticas, así como con la actualización del concepto, lo cual es un avance notable.

Realizar auditorías regulares que además de revisar el estado de la seguridad de la infraestructura crítica, permitan conocer el nivel de conocimiento de la cultura de seguridad al utilizar las TIC entre todos los empleados relacionados directa o indirectamente con las dependencias que administran infraestructuras críticas.

No hay fronteras

Es evidente que prácticamente ya no existen fronteras entre la seguridad física y digital. Igualmente, los ataques a la infraestructura crítica son una potencial amenaza a organizaciones (instituciones, empresas y entidades públicas) en todo el mundo, por los perjuicios económicos que pueden causar y por los riesgos potenciales a las vidas humanas.

A la par de este riesgo externo, existe un asunto interno relacionado con las debilidades en la cultura de seguridad en las TIC que podría resolverse con capacitación, política de seguridad claras y la creación de una conciencia de las amenazas, para la mejora de la postura de ciberseguridad.

Al mismo tiempo, la innovación en tecnología está borrando las diferencias entre los equipos de seguridad física y cibernética que regularmente actuaban de manera independiente. Actualmente las herramientas empleadas para la protección física están relacionadas o dependen de las redes digitales, la nube, el software y el hardware; elementos que están expuestos a amenazas cibernéticas.

Desafíos cumplidos

Martín Iván Vilchez Vitela, chiclayano de nacimiento, ha desarrollado una fructífera carrera laboral en el sector. Sin embargo, se vienen nuevos compromisos que él asume con responsabilidad en los ámbitos profesional, académico y familiar.

Entre los desafíos laborales cumplidos de Martín Iván Vilchez Vitela se incluyen el cambio de la conciencia de pago de los usuarios, contar con un nuevo software para la empresa que sea más confiable y amigable al usuario, e instalar 600 medidores en un mes.

Adicionalmente, con paciencia, trabajo y perseverancia, nuestro entrevistado ha logrado bajar del 50% de usuarios deudores al 20%, instalar un software para la gerencia comercial, aumentar la recaudación mensual de 700.000 soles a 900.000 soles, y en saneamiento se instalar 700 medidores en un mes con solo dos cuadrillas.

De otro lado, las proyecciones del supervisor de Operaciones del Consorcio Latino Actividades Comerciales (LAC) se orientan a tener su propia empresa y gerenciarla, así como ser un buen líder de su propia compañía.

AMIGO DE LA COMPUTACIÓN

Martín es natural de Chiclayo. Cursó sus estudios en el Centro Educativo 10014 “San Martín de Porres” (primaria) y en el Colegio Particular “San Agustín” (secundaria).

Descubrió su vocación cuando se enteró a través de un programa de televisión todo lo que se podía hacer con una computadora. Para él, la computación representaba “una ventana hacia el futuro”, por eso, ingresó a la Universidad Nacional Pedro Ruiz Gallo, para estudiar ingeniería en Computación e Informática.

Su primera experiencia preprofesional fue en el Hogar Clínica San Juan de Dios, de Chiclayo, en donde apoyo labores en la caja registradora, realizó aplicaciones para mejorar el sistema informático de atención al cliente, y realizó el estudio para la instalación de la red de la clínica.

Actualmente está estudiando un diplomado en Gestión Pública y posteriormente se preparará en el diplomado en Gestión de Proyectos para obtener la certificación del Project Management Professional (PMP).

PATERNIDAD RESPONSABLE

Para salir de la rutina laboral, Martín Iván se entretiene viendo, a través del televisor, partidos de fútbol y otros programas. Igualmente, sale a pasear con su familia y juega con su menor hijo de apenas cinco meses de nacido.

“Lo que más espero con ansias al final del día es haber cumplido como padre en hacer feliz tanto a mi hijo como a mi esposa. Quiero asumir con responsabilidad y alegría el papel de padre”, sostiene Vilchez, quien considera que para mantener una familia sólida hay que ser perseverante, y también espera en el futuro tener una hija y llamarla Isabel.

Esencia de éxito

La igualdad de género es esencial en la sociedad, en las organizaciones y en la vida diaria. Esa es la visión de Yolanda Rojas, quien afirma que el éxito personal se identifica con la conciencia de incluir en todas las actividades los valores y los principios.

Curiosamente, no todas las mujeres han experimentado una competencia de género en el ámbito de las Tecnologías de la Información (TI). “En mi caso personal, siempre he sentido igualdad de condiciones a lo largo de mi trayectoria profesional”, manifiesta Yolanda Rojas Semorile.

Para la directora de Evolve Systems, la igualdad de género es un derecho humano fundamental, “y promoverlo es esencial en todos los ámbitos de una sociedad sana”.

“Estudios indican, por ejemplo, que cuando las mujeres ocupan una proporción significativa de los puestos directivos, las empresas obtienen mejores resultados financieros y de productividad. También se descubrió que las organizaciones y los departamentos de tecnología con diversidad de género tienen más probabilidades de cumplir con los cronogramas, de mantenerse por debajo del presupuesto y de mostrar un mejor desempeño de los empleados”, enfatiza.

A lo largo de su trayectoria laboral, Yolanda siempre ha brindado las mismas posibilidades a profesionales (indistintamente del género), celebrado sus logros, vivido y acompañado el embarazo de muchas de sus trabajadoras siempre con mucha alegría y jamás lo ha identificado como una carga o un problema. Al respecto, expresa: “El mejor aporte que puede existir en las empresas y en la sociedad en general, es que no exista diferencia alguna de género”.

DAR MUCHO DE SÍ

Los resultados del éxito pueden ser innumerables, de acuerdo con cada persona. En tal sentido, Yolanda Rojas considera que el éxito en el plano profesional y personal se vincula con la conciencia que implica saber en todo momento si lo que hacemos está alineado a nuestros valores y principios. “La gente que busca un empleo solo por necesidad, está siendo absolutamente inconsciente, por lo tanto, deja de lado el éxito personal y profesional porque no tiene pasión por lo que hace”, señala a manera de ejemplo.

Asimismo, esta destacada ejecutiva advierte que para asegurar el éxito es indispensable desarrollar personalmente un equilibrio entre las ocupaciones profesionales, la familia, el descanso y la recreación, situación que no siempre es fácil de obtener, pero no es imposible de alcanzar. En su caso, el deporte la ayuda mucho a disciplinarse en general y lograr un sano equilibrio en la vida.

“En general, para conseguir cosas buenas en la vida es necesario dar mucho de sí, esforzarse al máximo y tener pasión por lo que se hace”, expresa.

Un nuevo tiempo trae consigo cambios.....

Bienvenido al Cambio

G55CIO

EL PUNTO DE ENCUENTRO DEL CIO Y CEO

Todos los martes en su bandeja de entrada.....

Una publicación de:
Grupo Bitácora