Carta de presentación

Lic. Layla Delgadillo Aguilar

CEO & founder Silent for Business

Semblanza:

Formada en la Universidad La Salle en la licenciatura de tecnologías de la información y con estudios especializados en Seguridad Informática, ha forjado una carrera de más de 16 años de experiencia, a través de la cual ha desarrollado habilidades para dirigir equipos especializados en normatividad, seguridad informática, auditoría, gestión de servicios y proyectos.

Las instituciones que han consolidado las aptitudes y formado su perfil de alto desempeño van desde instituciones de Gobierno cómo el SAT hasta empresas financieras transnacionales cómo CITIBanamex y Accival. En los últimos años ha construido una estable y sobresaliente presencia en empresas con un alto enfoque en la transformación digital cómo motor de innovación de las cuales podemos mencionar, Prosa, Scitum, Canon, etc.

Durante su desarrollo profesional ha liderado y desarrollado proyectos de implementación de mejores prácticas como ITIL, COBIT, MAAGTICSI, PCI y TOGAF, auditorías de TI y contractuales, certificaciones ISO9001, 27001, 20000-1, 22301, gestión de proyectos y seguridad informática.

Con esta trayectoria encontró una gran oportunidad para las empresas en la protección del activo más valioso de la humanidad del siglo XXI: La información, siendo este el parteaguas, paso de ser una líder de grandes corporaciones a construir una empresa con enfoque en la protección de la información de ciber ataques, continuidad en el flujo de la información, seguridad en la información de la operación.

Entrevista en Medios

TEMA: CIBERSEGURIDAD

ROL	PREGUNTAS Y RESPUESTAS
Entrevistadora	¿Qué es Silent 4 Business y a qué se dedica?
Layla Delgadillo	Silent 4 Business es una empresa 100% mexicana, especializada en servicios de ciberseguridad y monitoreo de siguiente generación en seguridad de la información. Cuenta con una amplia gama de servicios administrados en materia de seguridad y monitoreo, soportados por metodologías y estrategias, para aportar valor real a nuestros clientes a través del análisis inteligente de datos y la prevención proactiva de amenazas. Silent 4 Business pone especial énfasis en la protección de su información, por lo que implementamos estrategias y tácticas contextualizadas a su organización, que faciliten la toma de decisiones y mantengan una alta disponibilidad de sus servicios.
Entrevistadora	¿Qué es la ciberseguridad?
Layla Delgadillo	De acuerdo ISACA (Asociación de Auditoría y Control de Sistemas de Información), asociación internacional en seguridad de la información con autoridad en el tema; La **Ciberseguridad** es la Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
Entrevistadora	¿Hay alguna diferencia entre ciberseguridad y seguridad de la información?
Layla Delgadillo	Sí, aunque se tiene una idea general de lo que representa la ciberseguridad y se utiliza como sinónimo de seguridad de la información, esto no es del todo correcto. La Seguridad de la Información tiene un alcance mayor que la ciberseguridad, puesto que ésta busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados. Por el contrario, la ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.
Entrevistadora	¿Los ciber ataques a quien afectan principalmente?
Layla Delgadillo	En un mundo dominado por la constante conectividad de las personas, las organizaciones y las cosas (Internet of Things), las vulnerabilidades se multiplican y nadie está exento de ser víctima de un ciber ataque. Los ciber ataques van dirigidos al Estado (Gobierno), las organizaciones y los individuos; Por ello es imperativo contar con sólidos sistemas de ciberseguridad y éstos deben circunscribirse a la banca, empresas y a toda la sociedad en general. Solamente el primer trimestre del 2017, se realizaron alrededor de 50,000 ataques cibernéticos a escala global, las finalidades de estos fueron variadas y sus objetivos fueron múltiples. A nivel Empresas, las del sector Energía (Compañías de Electricidad) fueron las que reportaron mayor cantidad de ciber ataques registrando casi el 40% de ataques de malware, mientras que cerca del 35.3% fueron a las redes de ingeniería e integración de Sistemas de Control Industrial (ICS) quienes también padecieron este tipo de ataques según cifras dadas a conocer por Kaspersky Lab. A nivel individuos son los niños y adolescentes las principales víctimas de ciberataques, en forma progresiva. Por ejemplo, un abusador que está buscando a menores sólo tiene que acceder a las redes sociales para captar a sus víctimas.
Entrevistadora	¿Cómo es que Silent 4 Business entra al tema de Ciberseguridad?
Layla Delgadillo	Las Empresas e Instituciones requieren mantenerse a la vanguardia en temas de Ciberseguridad lo que se traduce en la adopción de tecnología de punta, adopción de mejores prácticas, infraestructura y equipo especializado para la protección de su información, esto en muchos casos no les es posible lograrlo, debido a la inversión económica y destinación de recursos que esto conlleva. Es justo ahí donde Silent 4 Business ofrece sus servicios para cubrir esta necesidad encargándose de fortalecer las estructuras de las empresas en materia de ciber

	seguridad, eliminando la inversión de infraestructura de nuestros clientes, incluyendo los costos de adquisición durante la implantación y los costos totales de propiedad a lo largo de su vida útil.
Entrevistadora	Específicamente con que herramientas cuenta Silent 4 Business para dar este servicio
Layla Delgadillo	Contamos con un Centro de Operaciones de Seguridad, SOC (por sus siglas en inglés de Security Operations Center), el cual es responsable del monitoreo, identificación y resolución de incidentes que afectan la seguridad de la información de nuestros clientes a través del uso de herramientas de monitoreo y administración de infraestructura de seguridad para detectar y reconocer amenazas y vulnerabilidades. También contamos con un Centro de Operaciones de Red (NOC), el cual es responsable del monitoreo, identificación y resolución de incidentes que afectan la disponibilidad de acceso y servicio de las redes que incluyen voz y datos.
Entrevistadora	¿Qué garantías ofrece Silent en temas de Ciberseguridad?
Layla Delgadillo	Para garantizar la ciberseguridad, confidencialidad e integridad de la información de nuestros clientes, los servicios que Silent 4 Business ofrece son operados por personal altamente calificado a través de procesos que se someten a los requerimientos de las principales acreditaciones internacionales en el ámbito de la seguridad como ISO/IEC 20000-1 “Sistema de Gestión de Servicios de Tecnologías de la Información” e ISO/IEC 27001:2013 “Sistemas de Gestión de Tecnologías de la Información”.
Entrevistadora	¿Cuáles son las fallas de seguridad o ataques más comunes en la red?
Layla Delgadillo	Algunos de los problemas de ciberseguridad más comunes en una Red Corporativa / Administrativa son: • **Spyware,** el cual es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento del propietario del ordenador. Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. • **Malware** o “Malicious software”, es un término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos (Trojans), Gusanos (Worm), keyloggers, Botnets, Adware, etc. • **Ransomware** o secuestradores es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera su información, debe pagar al atacante una suma de dinero. • **Fishing** o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria). • **Denegación de servicio (DDOS)** es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.
Entrevistadora	¿Cuánto tiempo toma resolver un ciber ataque?
Layla Delgadillo	No existe un tiempo definido ya que cada caso es particular y se le da tratamiento con diferentes estrategias dependiendo de la complejidad del ataque.
Entrevistadora	¿Cuáles son los riesgos que se corren en general al no contar con este tipo de seguridad?
Layla Delgadillo	Existen numerosas consecuencias negativas de no tomar las medidas de ciberseguridad pertinentes, por ejemplo: • El secuestro de información por falta de una correcta estructura de seguridad. • El Impacto monetario por verse forzados a hacer paros en la operación. • El robo de información personal como claves bancarias y números de tarjeta de crédito. • La pérdida de productividad al verse en la necesidad de parar las operaciones. • La afectación de la reputación de la empresa tras un ataque cibernético si ocurre una fuga de información de sus usuarios finales, ya que los clientes pueden dejar de confiar en ellos. • En base a los términos legales y regulatorios vigentes los usuarios pueden demandar a la empresa por no cuidar correctamente sus datos, lo que deriva en costosas multas.
Entrevistadora	¿Qué sectores se consideran más vulnerables a robo de información y ataques?
Layla Delgadillo	Cualquier sector es vulnerable de NO contar con las medidas de ciberseguridad adecuadas.

Entrevistadora	En tu experiencia, ¿La seguridad crece al mismo ritmo que la conectividad tecnológica?
Layla Delgadillo	Desafortunadamente No, lo anterior se debe a que la ciber delincuencia constantemente desarrolla nuevas formas de lucrar con la información y accesos de redes industriales y grandes corporaciones, sin embargo, la brecha se va acortando al aplicar mecanismos reactivos y metodologías progresivas, provisorias y replicables para cualquier industria.
Entrevistadora	¿Por qué debo de contratar a Silent y no a la competencia?
Layla Delgadillo	Tenemos un nivel muy alto en lo que al sector profesional de la ciberseguridad se refiere. Así como excelentes profesionales en esta materia. La decisión de contratarnos no es un tema de evaluar precios y presupuestos consideramos que el nivel de acompañamiento y las garantías de un manejo anticipado de los riesgos detonarán la toma de decisión de cualquier persona.