

La cibercriminalidad como peligro esencial para empresas y personas

Los programas "corporate compliance" pueden operar como causa eximente de responsabilidad penal corporativa

Autores: **Casimiro Nevado Santano**, inspector de la Policía Nacional y profesor de la Escuela Nacional de Policía, coordinador del Proyecto C1b3rWall, y **Pedro Fernández-Villamea Alemán**, abogado y coordinador del Departamento Legal & Compliance y asesor de la Sección de Derecho Militar y Seguridad ICAM.

Gobernar conlleva liderar. A su vez, liderar es saber guiar. El mejor guión: la Gobernanza Operativa de Riesgos Corporativos. Las cifras conocidas en este Informe mueven y conmueven.

Asumamos una realidad incuestionable: la seguridad legal operativa (ISO 31022 Gestión de Riesgos Legales) aporta y potencia todo crecimiento, tanto nacional como empresarial.

Hablamos, por lo tanto, de tres mecanismos claves: líneas de defensa (ISO 37301), Sistemas Integrados de gestión y el estado de información no financiera (se incluye aquí el control general de tecnologías de la información: Ley Seguridad Servicios de la Información y Reglamento Unión Eurepea número 881 de 17 de abril de 2019).

Todo plan conlleva, a su vez, una táctica y una estrategia. Se resume en las tres P: personas, procesos y procedimientos. En otras palabras: talento, hábito y método. A todo ello contribuyen los sistemas integrados de gestión. En definitiva, empresas con un mismo comportamiento sin compartimentos.

A día de hoy, los ciberataques constituyen la segunda amenaza real para España, junto con la pandemia, según el último informe del Departamento de Seguridad Nacional.

En este sentido, como riesgo nacional y corporativo diario, la ciberdefensa debe considerarse siempre como riesgo estratégico incuestionable. Por lo tanto, se incluirá en la primera línea de defensa en la elaboración de las matrices algorítmicas. En su defecto, las alarmas saltarán con el enemigo ya en casa. Recordemos al sabio Pedro Calderón de la Barca: Casa con dos puertas, mala es de guardar. Imaginemos si haya tantas puertas como mails corporativos tiene la empresa.

En este sentido, abordemos un aspecto que preocupa más que ocupa en todos los departamentos de cualquier empresa: la responsabilidad civil ex delicto del empleado (art.120.4º Código Penal). Véase la sentencia del Tribunal Supremo 647/2021, de 19 de julio.

La imputación requiere acreditar un vínculo o relación jurídica entre el infractor y el empleado de dicha persona jurídica imputada. A su vez, el delito se debe cometer dentro del ejercicio de las obligaciones establecidas al empleado imputado.

A sensu contrario, no se imputará si la acción del empleado, objeto de la imputación, era ajena al ejercicio de sus funciones.

En definitiva, los programas corporate compliance pueden operar como causa eximente de responsabilidad penal corporativa (STSS 2947/2018 de 28 de junio y 334/2018 de 5 de febrero), si se demuestra la inserción real de la cultura de cumplimiento normativo en la empresa imputada. En definitiva, las dos dobles CC: conciencia de cumplimiento y corporate compliance.

En este sentido, si hay un actor que se ha adaptado mejor que nadie a las reglas del ciberespacio y a la sociedad de la información es el crimen organizado. Estas organizaciones han sabido desplegar una estrategia de transformación digital más rápidamente que la mayoría del resto de actores.

Velocidad que demuestran con la adaptación de sus técnicas, tácticas y procedimientos, siendo capaces de modificar el código malicioso para evitar que este sea detectado o trasladando sus infraestructuras de la darkweb en tiempo récord.

Este es uno de los condicionantes que marcan las nuevas reglas. Sumemos la cantidad de información disponible para captar y analizar y con ella perfilar los objetivos a atacar. En un mundo donde cada vez existen más datos, ser capaz de manejarlos eficientemente es fundamental para cualquier organización, incluidos los delincuentes.

Cantidad y velocidad propician el aprovechamiento de otra característica de la red, la escalabilidad. Si tengo datos y los manejo a gran velocidad puedo atacar a un objetivo determinado que me proporcionará grandes beneficios o a centenares de miles de ellos, obteniendo pequeñas cantidades, pero sumando un montante igual de importante.

A estos condicionantes debemos añadir la joya de la corona, el talento. Por muy románticos que se quieran poner algunos, el talento se capta y se retiene con dinero, el resto son añadidos, interesantes sí, pero no determinantes.

Los grupos delincuenciales obtienen beneficios y los reinvierten en nuevas capacidades y más talento que desarrolle mejores armas cibernéticas, con ello cierra un ciclo perfecto.

Ante esto, se está luchando ferozmente por parte de los profesionales de Fuerzas y Cuerpos de Seguridad y empresas, pero se necesita más. Con mejores presupuestos se conseguiría más talento y más capacidades, pero es que, además, seguimos fallando en lo más básico. La cadena es tan fuerte como su eslabón más débil, de nada sirve tener excelentes profesionales en ciberseguridad si cualquiera abre la puerta y sienta en el salón al delincuente.

Hoy nadie puede ser sujeto pasivo en seguridad, la implicación y corresponsabilidad de todos es fundamental. De concienciación y preocupación debemos pasar a ocupación y la mejor herramienta es la formación.

Policía Nacional, con la participación ciudadana en su ADN, lanza una nueva edición del curso C1b3rWall-Academy, con más de 30.000 inscritos ya, consolidándose como la acción formativa de referencia en ciberseguridad de nuestro país, destinada a todos los ciudadanos, profesionales o no de la ciberseguridad, con objetivo de prevenir y combatir el cibercrimen.

Fuente: *Cinco Días*