EL ESPACIO Y EL CIBERESPACIO REQUIEREN **NUEVAS ESTRATEGIAS DE DEFENSA**

El espacio y el ciberespacio como campos de batalla **¿Qué debe saber Colombia sobre este tema?**

A las tradicionales fuerzas militares entendidas como el ejército de tierra, la fuerza aérea y la marina armada, se le deben agregar dos nuevas fuerzas que emergen para interactuar con las tres anteriores: **las fuerzas del espacio y el ciberespacio**.

Desde la década pasada, varias naciones, Colombia incluida, han tomado en serio el despliegue de estrategias para afrontar los riesgos de protección de la infraestructura de TI y de la información que fluye en ella, en su carácter de componentes vitales para el desempeño de las actividades cotidianas.

De hecho, hay múltiples ejemplos recientes de ataques que han puesto en riesgo la gestión del estado. El año pasado, Costa Rica recibió una serie de ataques de tipo extorsivo que afectó a varios ministerios e instituciones del estado, entre ellas el ministerio de hacienda y el de telecomunicaciones. Estonia, por su parte, ha sido víctima de ataques constantes por parte de una nación enemiga. Desde comienzos de siglo, Rusia ha atacado no solo la infraestructura de gobierno sino también bancos y medios de comunicación, entre otros.

La protección del espacio abarca lo que le corresponde a cada nación más allá de la atmósfera terrestre. En el ámbito tecnológico, los puntos de interés en este frente son los satélites y sus órbitas, así como las antenas para enviar y recibir la información.

Sumado a este frente, el estado necesita gestionar las ondas electromagnéticas vitales para las comunicaciones. En este sentido, se debe tener en cuenta la organización del espectro electromagnético para distribuirlo entre diversos usuarios y suplir necesidades específicas que abarcan desde los radioaficionados, las emisoras de radio, los sistemas de radio de tipo militar, los servicios de transmisión de señal de televisión digital y las antenas de las celdas para transmisión de comunicaciones móviles o celulares.

La infraestructura física que permite el aprovechamiento de este recurso también se convierte en un activo prioritario.

Por otro lado, el ciberespacio se define como este escenario por donde fluyen los *bits* y *bytes*, componentes mínimos para la generación de datos que forman la base de la información digital de las personas, las instituciones y las industrias, así como de los gobiernos.

La cuarta revolución industrial, a la que entramos a través de la automatización y robotización de muchos procesos, se hace más patente en el campo de la defensa si tenemos en cuenta la necesidad de conectar sofisticados equipos de comunicación, junto con naves y armamento.

Imagen: Sitio Comando General de Fuerzas Militares de Colombia

Por lo tanto, la nube, los centros de datos, los equipos móviles y de computación personal deben contar con una protección que garantice ese flujo de información de manera confiable, constante y segura.

Al respecto, el teniente coronel de la Fuerza Aérea de los Estados Unidos, Mark Reith, un experto en estrategia de defensa del espacio y el ciberespacio aclara tres supuestos que deben atenderse para entender el impacto de los ataques a través del espacio y el ciberespacio:

> Primero, las actividades ciberespaciales y espaciales se encuentran ocultas a menudo debido a su naturaleza muy secreta y después de que hayan ocurrido, y a menudo de forma anónima. A diferencia de las pruebas y operaciones nucleares que generalmente son observables por todos los adversarios, las actividades ciberespaciales y espaciales pueden ser detectables o no por parte del objetivo, y normalmente no por parte de terceros. Segundo, la descripción supone que todos los adversarios están prestando atención y entienden la amenaza. Dentro de los dominios espacial y ciberespacial, esto puede requerir herramientas especializadas que detecten perturbaciones en estos dominios, y lo que es más importante, que interpreten correctamente su situación. Por último, la descripción supone que ya se ha logrado el trabajo de preparación que apoya las acciones de amenaza.

La seguridad de la información comienza desde la infraestructura

La protección de esta infraestructura se sustenta principalmente en las TIC y, por esta razón, se han convertido en objetivos de ataque realizados por diversos frentes que arrancan en el crimen organizado y se extienden hasta los intereses de otras naciones.

James Ferraioli, vicepresidente de mercados de la firma de banca e inversiones Morgan Stanley, afirma que el número y la sofisticación de los ciberataques han estado creciendo durante años, impulsados por el aumento del *big data*, la computación en la nube y el trabajo remoto.

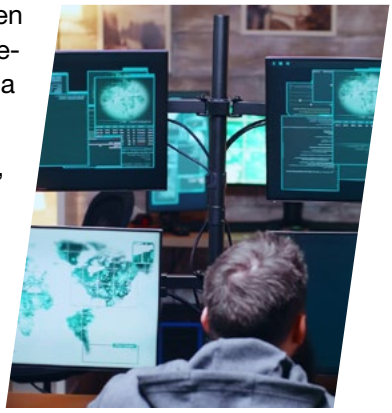
La razón es evidente: Con más lugares desde los que se accede a más datos que nunca, tanto por personas como infinidad de dispositivos, la complejidad de asegurar los sistemas digitales ha aumentado exponencialmente. **El resultado: una fuerte y creciente demanda de servicios de seguridad que podría impulsar las acciones relacionadas con ciberseguridad en los próximos años**.

Y para proteger ese frente digital no sólo se necesita presupuesto, también se requiere una estrategia innovadora.

Sai Ram, experto mundial en ciberdefensa, explica que

> las actividades de todas las empresas, agencias de seguridad pública y el gobierno son respaldadas por el sector de las comunicaciones, cruciales para la economía del país. Esta industria ha cambiado en los últimos 25 años, pasando de ser principalmente un proveedor de servicios de voz a uno que utiliza métodos de transmisión terrestre, satelital e inalámbrica, y que es diversificado, competitivo e integrado. Para llevar y terminar su tráfico, los proveedores de satélite, inalámbricos y de líneas terrestres ahora dependen unos de otros. Para mantener la interoperabilidad, las empresas intercambian regularmente instalaciones y tecnología

Colombia, como otros países, ha desarrollado nuevas estrategias de defensa para estar en el frente del campo donde se libran las batallas del presente, es decir, en el espacio y el ciberespacio. Esta estrategia requiere mantenerse activa y evitar cualquier distracción que pueda resultar desastrosa.



Por esta razón, se recomienda ver más allá de la implementación de sistemas diversificados, del uso de herramientas y de agregar productos en los planes de compra para reducir la probabilidad de fallas aplicando políticas de seguridad que abarquen procesos y procedimientos. En la actualidad se aplican múltiples capas de defensa para confirmar un sistema de seguridad a prueba de fallas.

Así, si una parte del sistema falla, habrá otro que lo supla y de esta manera se minimizan los riesgos de exponer todo el sistema.

La seguridad de la información comienza desde la infraestructura

En **Panduit** entendemos esta necesidad y la urgencia de abordar de manera holística las tecnologías informáticas y de telecomunicaciones. Por esta razón trabajamos con los estándares de la industria y contamos con certificaciones que nos ponen a la vanguardia en temas de gestión de la infraestructura, la conectividad y las telecomunicaciones, incluyendo ISP 9001, ISO 14001, LEED, EPDs/HPDs, RoHS COC, entre otras.

Nosotros también nos comprometemos con la gobernanza de la información y la calidad de nuestras soluciones. Por esto contamos con un sistema de garantías y certificaciones que están cubiertas bajo el sistema **Certification Plus System Warranty** que nos permite asegurar que nuestros aliados son expertos y pueden desplegar infraestructura de tecnología de manera confiable y segura.

Colombia, por su parte ha desarrollado estrategias para la protección de la información de sus ciudadanos, de sus fronteras y sus fuerzas militares.

Sin embargo, aún falta un detalle determinante para mejorar la estrategia de seguridad partiendo desde la misma infraestructura de TI y teniendo en cuenta los nuevos escenarios descritos previamente, algo que James Ferraioli, de Morgan Stanley, explica al expresar que:

> las empresas de defensa y aeroespaciales están integrando cada vez más la ciberseguridad en sus productos, ya que los riesgos geopolíticos elevados difuminan las líneas entre la ciberseguridad y la defensa nacional. Esto podría fortalecer la oportunidad de inversión secular entre las empresas involucradas en ciberseguridad, como los contratistas de defensa tradicionales.