En Movistar, el proceso de Seguridad de la Información asegura que los demás procesos puedan operar sin interrupciones, pérdidas de datos o filtraciones de información. Este proceso se basa en proteger la integridad y confidencialidad de los datos a través de mecanismos de control como la verificación de credenciales, la clasificación de archivos y el cifrado automático de la información cada vez que se carga o modifica algo dentro del sistema.

Una de las principales debilidades actuales es la existencia de vulnerabilidades que no siempre son detectadas a tiempo, lo que puede provocar fallas graves en otras áreas. Por ejemplo, si un archivo con información sobre un equipo en reparación se pierde o se corrompe, el sistema no puede rastrear su ubicación o estado, generando demoras o incluso causando la perdida de dispositivos. Esto muestra cómo una falla en este proceso puede desencadenar problemas en otros sectores, afectando la eficiencia y la comunicación entre procesos internos.

El equipo responsable de llevar adelante estas tareas está compuesto por personal de Seguridad Informática, Sistemas, administradores de red y especialistas en cumplimiento normativo.

El procedimiento muchas veces se desencadena automáticamente al detectar un comportamiento sospechoso en el sistema o cuando se realiza una carga de información. Además, cada cierto tiempo se programan análisis preventivos de amenazas, sin necesidad de que haya un incidente previo. La documentación utilizada para estas tareas incluye logs del sistema, reportes de incidentes, manuales de seguridad, informes de auditorías y registros de acceso, entre otros.

Aunque todo el proceso es completamente virtual y se ejecuta en plataformas digitales, puede ser gestionado tanto desde oficinas centrales como de forma remota, ya que gran parte de las herramientas que utiliza el equipo están en la nube. Esta flexibilidad permite mantener una vigilancia constante sobre la infraestructura digital de la empresa, independientemente de la ubicación del equipo encargado.

En definitiva, la situación ideal sería contar con un sistema proactivo, que no solo reaccione ante amenazas, sino que las anticipe y neutralice antes de que afecten al resto de los procesos. La meta es tener una infraestructura sólida y confiable que permita que todos los demás procesos productivos se desarrollen de forma segura, contribuyendo al cumplimiento de los objetivos de la empresa.