Gestión de la seguridad de la información

Logros importantes de 2019	Retos más destacados para 2020
Definición y despliegue del Plan de Seguridad Estratégica Global para la Ciberseguridad y la Seguridad Física.	Puesta en marcha de la Oficina de Seguridad Global y el servicio de inteligencia y vigilancia jurídica en todos los países integrados en 2019 (España, Francia, Italia, Holanda, Suiza y Reino Unido).
Establecimiento de un modelo de gobernanza de seguridad de la información.	Análisis y aplicación de una solución técnica de gestión de riesgos que permita la gestión automatizada de riesgos de seguridad global.
Certificación ISO 27001 en todos los países.	Implantación de un modelo de seguimiento de incidencias de seguridad en todos los países integrados en 2019.
	Implantación de una solución CASB para permitir la aplicación de políticas y el gobierno de aplicaciones en la nube.

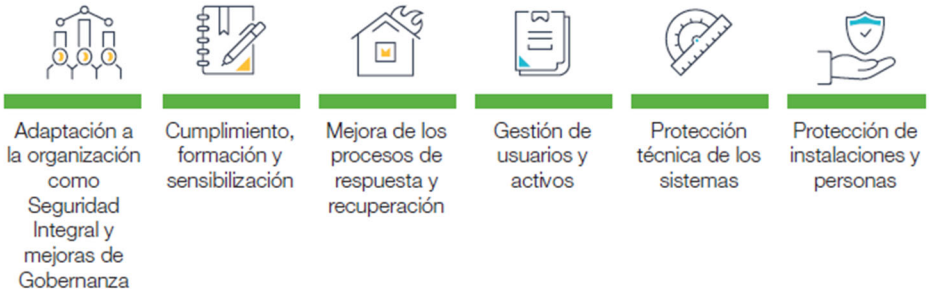
El sector de las telecomunicaciones debe protegerse de una amplia variedad de diferentes tipos de amenazas para prestar un servicio estable y de alta calidad a sus clientes. Por esta razón, Cellnex ha puesto especial énfasis en el área de la seguridad, ya sea física o informática, con una gran cantidad de actividades destinadas a evitar y mitigar cualquier posible amenaza que pueda afectar su servicio.

Por lo tanto, este año hemos elaborado un Plan Estratégico de Seguridad Global para Ciberseguridad y Seguridad Física que permite prever incidencias de alto impacto, según los marcos de referencia. El Plan se aplica a todas las empresas que conforman el grupo Cellnex y abarca todos los aspectos de la seguridad corporativa, independientemente del tipo de amenaza, ya sea física, informática o híbrida. En lo relativo a este plan, se han llevado a cabo las siguientes acciones:

- Evaluación Integral de Seguridad.
- Definición de un mapa de riesgos.
- Desarrollo de un plan de acción global.
- Aprobación de un presupuesto para tres años.

En primer lugar, analizamos la seguridad de la empresa en función de los marcos habituales (NIST Cybersecurity e ISO 27001) centrándonos en IT, OT y física, y cinco bloques de alto nivel, que abarcan distintas actividades de seguridad (identificar, proteger, detectar, responder y recuperar). Cada control ha sido evaluado considerando el nivel de madurez de las unidades de negocio, clasificados en cuatro categorías (No implementado, Parcialmente implementado, Extensamente implementado y Totalmente implementado).

Por otro lado, se ha definido un plan de acción global a tres años con el objetivo de mejorar el nivel de seguridad de Cellnex de acuerdo con el Comité de Riesgos. Este Plan ha definido 6 líneas estratégicas y 36 iniciativas, la mayoría de las cuales son acciones de la Corporación o de España, pero también hay proyectos en otros países. Para ello se ha establecido un umbral de madurez objetivo basado en la evaluación comparativa.



El Plan Estratégico de Seguridad Global para Ciberseguridad y Seguridad Física se ha formalizado en la Política de Seguridad de la Información, aplicable a todas las empresas que componen el grupo Cellnex, en línea con la norma ISO 27001.
Esta política fija una serie de pautas y líneas de acción para la Seguridad de la Información que regirán cómo deberá Cellnex administrar y proteger su información y servicios, así como su comunicación a partes interesadas y su despliegue en todas las empresas y áreas funcionales del Grupo.

El modelo de gobernanza de seguridad de la información también se ha definido y está estructurado de la siguiente manera:

- A nivel de grupo:
  - Director de Seguridad Global
  - Centro de Control de Seguridad
  - Oficina de Seguridad
- A nivel de país:
  - Ciberseguridad local (seguridad lógica)
  - Responsable de la seguridad física
  - Interfaz de usuario local

Fruto de estas acciones, en 2019 no hubo fugas de datos, robo ni pérdida en Cellnex, ni se recibieron quejas en relación con la seguridad de la información o la protección de datos.

En septiembre se obtuvo la certificación ISO 27001 para todos los países y todas las empresas. Esta normalización garantiza la aplicación del modelo industrial y la homogeneización de procesos a nivel global en un grupo tan diverso como es Cellnex, en el que se integran diferentes países y permite la mejora continua. Esta certificación también nos da acceso a ciertos mercados y clientes que la exigen para poder trabajar con ellos.

Para obtener la certificación ISO 27001, en 2019 se auditó la Corporación, España, Suiza e Italia. En 2020 se auditarán los Holanda y Francia, así como España y la Corporación, que siempre se auditarán debido a su volumen e importancia en el grupo Cellnex.

El progreso realizado en 2019 conlleva aumentar el nivel de madurez y reducir el nivel de riesgo asociado con la gestión de la información.

En cuanto a los datos personales gestionados por la compañía, el 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos (RGPD), por lo que fueron necesarias varias modificaciones dentro del Grupo para su correcta adaptación. Uno de los principales cambios marcados por el RGPD fue la obligatoriedad de nombrar a un Encargado de Protección de Datos (EPO). En Cellnex estas tareas las realizará el director de Asuntos Jurídicos de la compañía, que informará periódicamente al Comité de Ética y Cumplimiento sobre el estado de la aplicación y el cumplimiento del RGPD en las empresas del Grupo. Gracias a la correcta aplicación de la antigua normativa europea y al sistema maduro y robusto con el que ya contaba la compañía, dicha adaptación ha sido rápida y efectiva.

Además, este año el despliegue de algunos proyectos ha empezado a garantizar la protección de la información y a evitar la fuga de lo que se considera más sensible, como por ejemplo:

- Implantación de AIP (Azure Information Protection): pensado para proteger la información, independientemente de si está alojada en Cellnex, la nube o ubicaciones de terceros.
- MDM de reemplazo (Mobile Device Management): permite la gestión avanzada de dispositivos móviles, asegurando que solo los dispositivos autorizados puedan acceder a la información corporativa.
- Regularización de usuarios administradores: permite acceder a la información con los permisos adecuados para su tratamiento.
- Implantación de CASB (Cloud Access Security Broker): permite gobernar el acceso a la información ubicada en nubes públicas.