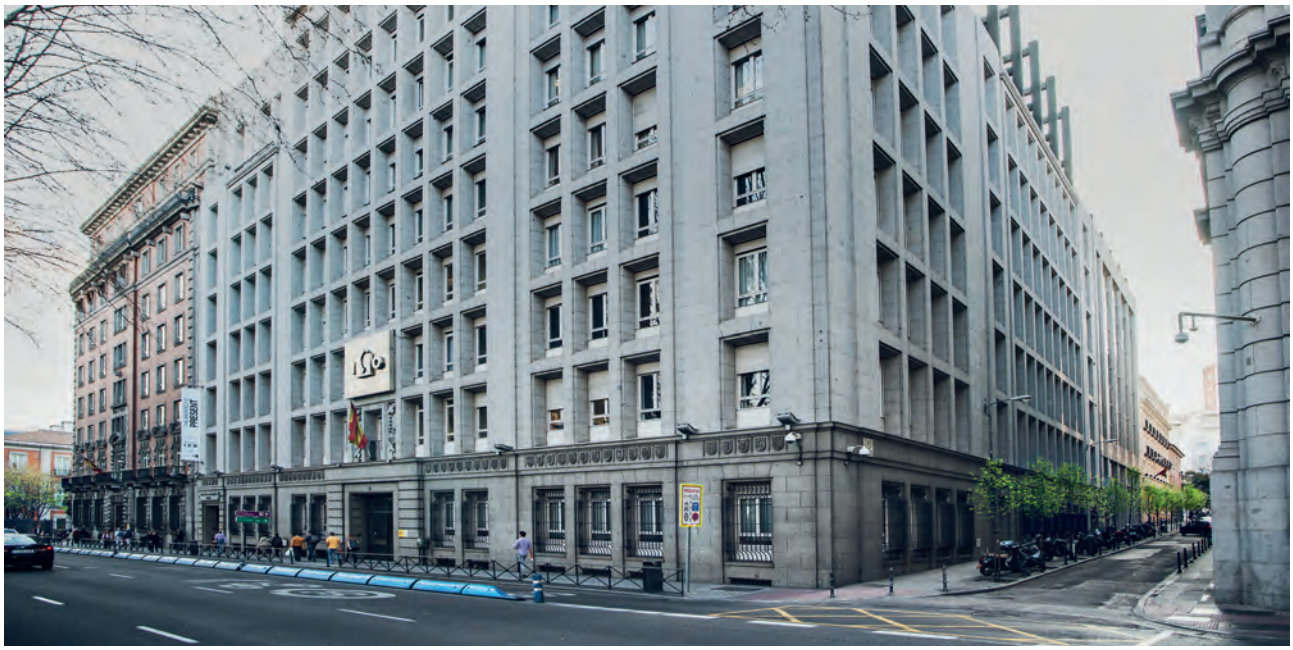
ICO

Premio: CPD más innovador



El Instituto de Crédito Oficial (ICO) es un banco público con forma jurídica de entidad pública empresarial, que apuesta por la continuidad de negocio y su renovación tecnológica de la mano de Fibernet. Su función principal es la promoción de actividades económicas que contribuyan al crecimiento, al desarrollo del país y a la mejora de la distribución de la riqueza nacional. Por tales motivos, durante los próximos años, Fibernet continuará con la prestación de los servicios del centro de respaldo de los sistemas de información y su evolución. Los sistemas en el CAR (Centro Alternativo de Respaldo) están soportados por una serie de servidores, almacenamiento y comunicaciones con enlaces de fibra óptica entre centros. Su objetivo es dotar a esta organización de un centro de respaldo que le permita seguir prestando sus servicios informáticos principales, en el caso de que se produjese alguna contingencia que impidiese la normal prestación de los mismos desde sus instalaciones en el Paseo del Prado, nº 4 de Madrid. Además, las plataformas instaladas en dicho centro podrán ser utilizadas como ampliación de sus entornos.

En un futuro se abarcarán proyectos más complejos y seguros para el cliente como crecimiento esnatural y evolutivo de sus sistemas que garanticen la integridad y permanencia de datos ante eventuales desastres, y la repartición de aplicaciones críticas que aseguren la continuidad del negocio sea cual sea la situación de conflicto que se pudiera plantear. El CAR de ICO debe estar operativo para los servicios declarados por la gestión como críticos en un tiempo mínimo en caso de desastre en el centro primario. Este centro físicamente alejado del principal mantiene una arquitectura tecnológica espejo, pero con un dimensionado en recursos hardware y software proporcional al porcentaje de servicios a respaldar y al acuerdo de nivel de servicio establecido.

"El CAR del ICO está sometido a las mismas evoluciones de su arquitectura que las de su centro principal"

Replicación en caliente

Uno de los cambios más importantes en esta nueva etapa que Fibernet tiene por delante es la prestación de los servicios de enlace entre centros sustentada en una replicación en "caliente" mediante fibra, de los datos y aplicaciones del ICO. Para ello se montará una solución basada en tecnología de transmisión DWDM (Dense Wavelength Division), ajustándose en cada caso a la rejilla y parámetros ópticos recomendados en las

normas ITU-T G.694.1 y en la ITU-T G.694.2. Esto dotará de alta disponibilidad al sistema, contando con caminos diversificados y equipamiento independiente para cada uno de ellos con canales GbEthernet y migración a 10GbEthernet y el F.Channel 2G con migración a F.Channel 8G, y manteniendo las mismas características de canales de transporte nativo y encriptado y con módulos de monitorización en tiempo real de calidad.

Cifrado de canal

Una parte fundamental en el cumplimiento de las nuevas normativas europeas es el cifrado de canal que introduce innovaciones orientadas a las nuevas reglamentaciones como que no requiere de memorias / blades extras en switch / router / FW para mantener rendimiento con cifrado; sus principales características son:

- Encriptación extremo a extremo de la línea de fibra.
- Comunicación transparente.
- Algoritmo criptográfico AES (Advanced Encryption Standard) funcionando con claves de 256 bits.
- Cambio automático con claves frecuentes mediante algoritmo de intercambio de claves Diffie-Hellman.
- Autenticación segura extremo a extremo impidiendo suplantación o ataques "man in the middle".
- Gestión por parte del cliente con clave principal.

"ICO, adelantándose más de un año a la GDPR, instaló la seguridad en la transmisión de los datos con sistemas y tecnología de Fibernet"

Otra característica de esta nueva fase es la LAN extendida que permitirá también la utilización del centro de respaldo como ampliación del CPD actual, con el fin de que el ICO pueda utilizar los recursos allí alojados cuando se requiera.

Asegurar la información

En este proyecto, el objetivo principal es adecuar los niveles de seguridad en el transporte de la información. El riesgo en dicho transporte es la pérdida de la información y conlleva una serie de requisitos técnicos a los cuales las empresas deben adaptarse en los próximos meses según nuevas normativas europeas. Básicamente y atendiendo a la tecnología del tratamiento de la información, su naturaleza, alcance, contexto, así como probabilidad y gravedad de los derechos del mal uso o robo de estos contenidos, obliga a medidas técnicas y organizativas que Fibernet ya dispone en el mercado con tecnologías apropiadas.

Así, un nivel de seguridad adecuado al riesgo debe de atender a una serie de recomendaciones:

- El cifrado de los datos a tratar.
- Capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- Capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida y segura en caso de incidente físico o técnico.
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento (léase explotación o transporte de los datos). Un claro ejemplo de la aplicación de todas estas normas de seguridad y tratamiento es la tecnología de Fibernet en el trasporte de la información desde el CPD principal del Instituto de Crédito Oficial y el centro de prestación del servicio de BRS (Business Recovery Site) de Fibernet, este enlace está constituido por una doble ruta en fibra oscura la cual es iluminada y tratada por el proveedor.

Para esta tarea se prestan una serie de servicios cuyo alcance es:

- 1 canal Ethernet 10 Gbps con diversificación de ruta y protección (1+1)
- 1 canal FC (Fiber Channel) 8 Gbps con diversificación de ruta y protección (1+1). Este sistema está configurado en modo alta disponibilidad y con equipamiento independiente en cada uno de los nodos. Van cifrados extremo a extremo, siendo la comunicación transparente para los equipos del ICO.

Otro sistema de seguridad en esta arquitectura es el añadido de módulos de monitorización en tiempo real de la calidad e intrusión en la fibra.

La solución se fundamenta en la implementación de una infraestructura DWDM mediante multiplexores DWDM DUSAC 350 en configuración de HA (Alta Disponibilidad) con redundancia de equipamiento por nodo de 2 canales ópticos cifrados nativos y caminos diversificados. Los transponders soportan servicios mediante tarjetas FTX (Interfaz Multiprotocolo altamente flexible) así como un módulo de monitorización en tiempo real (OSW-3) (Conmutador Óptico para protección de ruta).

La configuración se realizó en modo TWIN (Idénticos sistemas) implementado mediante un splitter pasivo que ofrece protección de canal ante uno de los fallos / eventos siguientes:

- Corte en fibra de planta externa.
- Fallo de hardware.
- Fallo de alimentación en alguna de las infraestructuras.

Con esta funcionalidad el servicio al ICO y la garantía de los datos no se ven afectados. ●