4.6. Gestión de la tecnología y de la información

“La tecnología y la digitalización son herramientas estratégicas en la eficiencia y el valor de un negocio, en las experiencias de mayor valor de los grupos de interés y en la preparación de información estratégica para la toma de decisiones.”

Una de las categorías que se integran dentro del sistema de gestión de grupos de interés de Caixa Popular es “aliados socios”, donde se encuentra la empresa participada RSI (Rural Servicios Informáticos). Para fortalecer el valor de gestión de sus sistemas de información y de su visión estratégica de generar y capitalizar alianzas, utiliza los servicios informáticos comunes de esta empresa.

RSI es responsable de las actividades de desarrollo o mejora de las aplicaciones clave del negocio, de la ubicación de datos, de la seguridad informática de las mismas, de las páginas web, etc., y establece protocolos para la utilización diferenciada por todas las empresas del Grupo.

RSI posee certificaciones y realiza auditorías independientes que avalan la excelente gestión de la seguridad y ciberseguridad:

- ISO 27001 Sistema de gestión de la seguridad informática.
- ISO 38500 Gobernanza de la tecnología de la información.
- ISO 22301 Sistema de gestión para la continuidad del negocio.
- ISO 22320 Sistema de gestión para la respuesta ante emergencias.
- CMMi (CVS) Ciclo de vida de software (nivel 3).
- LEET Security con el nivel máximo AAA+ en 2019.
- Certificados específicos de seguridad:
- Certificación PCI/DSS: certificado del estándar de seguridad de datos en tarjetas.
- Certificación CSP de Swift: certificación de seguridad para pagos por Swift.
- Auditorías de aseguramiento del marco de control interno europeas:
- ISAE 3402 Tipo 2: Para la eficacia operativa de marco de control interno en la gestión de los procesos generales de TI.
- SOC 2 Tipo 2: Para la eficacia operativa de marco de control interno en la gestión de los procesos de seguridad y ciberseguridad de TI.

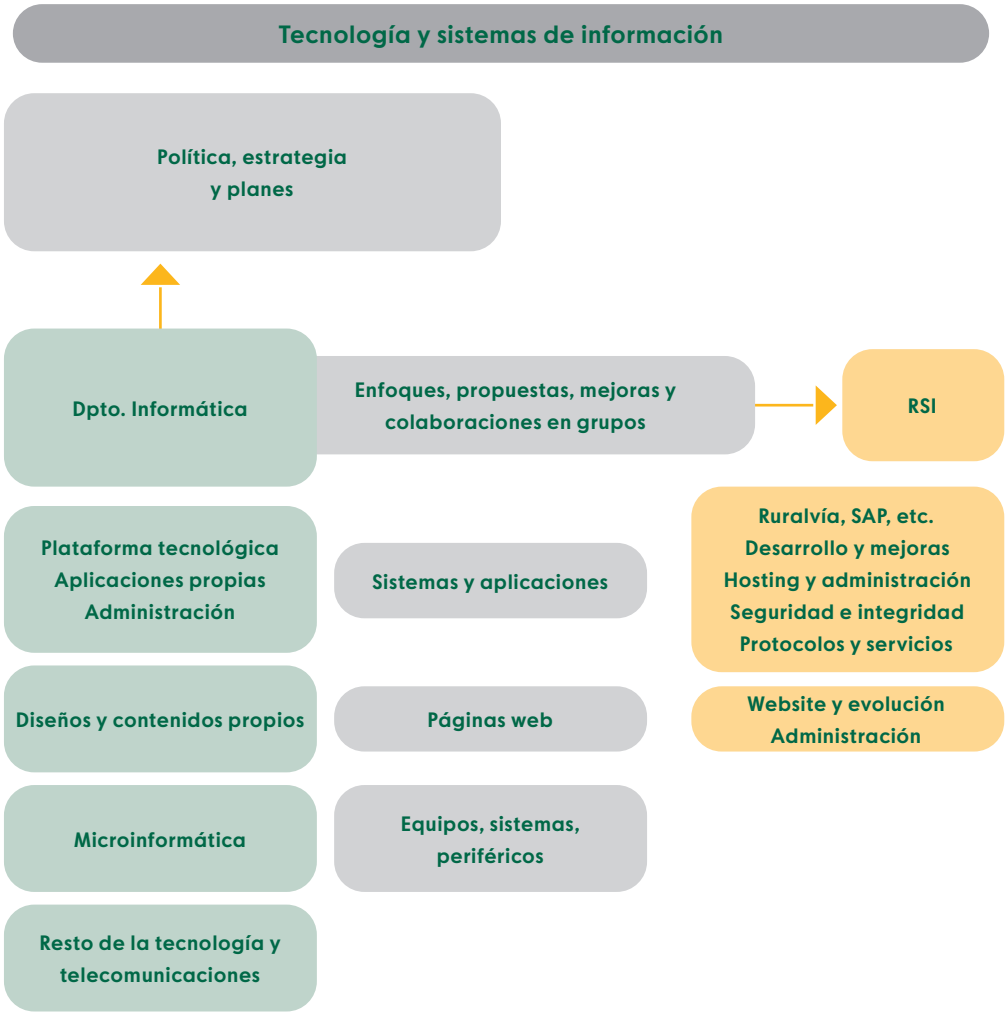
De forma complementaria, también posee otras certificaciones de gran valor para incrementar la confianza y el valor de su gestión:

- UNE 19601 Sistema de gestión de *compliance* penal.
- ISO 37001 Sistema de gestión antisoborno.

El Área de Informática de Caixa Popular es responsable de la planificación de proyectos y actuaciones relativas a los sistemas y medios informáticos de la organización, la definición de la plataforma informática, la seguridad de procesos y sistemas, la gestión y operatividad de equipos informáticos (servidores, ordenadores...), redes, dispositivos de apoyo (impresoras, etc.), *software*, soluciones de telecomunicación, telefonía, la microinformática y desarrollos locales, y la gestión del resto de la tecnología del negocio, con la investigación y pruebas asociadas.

Modelo de tecnología y de sistemas de información y telecomunicación

El modelo de tecnología y sistemas tiene una responsabilidad compartida entre RSI y el departamento de sistemas que participa en todos los grupos de trabajo de RSI (especialmente el de informática y el de organización) para aportar mejoras, innovaciones e influir en las decisiones técnicas y en la definición y priorización de proyectos.



Aplicaciones (principales y locales), nuevos desarrollos y mejoras

Las principales aplicaciones utilizadas por las empresas del Grupo son la de "Banca online (Ruralvía)", la de "Gestión de personas (SAP)" y las de "Gestión del negocio (IRIS NTF)", que residen en RSI y son de su completa responsabilidad.

Actualmente hay dos grandes macroproyectos plurianuales de valor en la gestión de las tecnologías de la información:

- La protección contra el crimen cibernético (sabotajes, piratería, cajeros y tarjetas, y robos de identidad).
- El proyecto de estrategia digital "Impúlsate" con la renovación de activos digitales, nuevos canales de interacción, nuevas propuestas de valor, potenciación de la cultura digital, *business intelligence* y el *marketing* digital.

En 2019 los principales avances fueron:

- La evolución NTF, incluyendo herramientas de administración para el usuario final y mejoras GED-gestión electrónica de documentos.
- El fortalecimiento de la seguridad lógica (modelo y plan).
- La mejora de los entornos de prueba.
- El desarrollo de una herramienta de trazabilidad de los errores de migración.
- La implantación de un método de medición de la calidad en llamadas al *call center*.
- La reducción del tiempo de espera al cliente a 30 segundos.

Proyectos relevantes:

- Nueva banca digital con una app mejorada y de mayores funcionalidades.
- Google Pay, servicio de pago móvil para clientes con dispositivos Android.
- Nueva web comercial del Grupo Caja Rural.
- PSD2 *compliance* y estratégico: cumplimiento de la nueva normativa de servicios de pagos digitales PSD2.
- Factoring Iris: aplicación para integrar este producto en el terminal financiero.
- Chatbots: diseñar e implantar un nuevo canal automatizado de atención a clientes y empleados.
- Muro de clientes: implantar la herramienta de mercado "Muro digital" que dé cobertura a la figura que se está creando en las entidades de "Gestores digitales".
- Proceso guiado de seguros: simplificación de la operativa en oficinas y de usuarios.
- Uso de marcas de protección de datos en apps: integración en las aplicaciones de las nuevas marcas de consentimiento derivadas de la entrada en vigor del RGPD.
- Nuevo modelo de rating de PYMES.
- Adaptaciones Ley de crédito inmobiliario: desarrollos para el cumplimiento de la ley (LCCI).

Ciberseguridad

Las diferentes líneas de actuación en materia de ciberseguridad se pueden estructurar en tres etapas: la prevención del riesgo, la rápida detección y la respuesta precisa ante cualquier ciberincidente. Las principales líneas de actuación en 2019 fueron:

Procesos de gestión preventiva

Estos procesos comprenden el refuerzo del servicio de vigilancia digital y antifraude, las pruebas de procedimientos y protocolos de seguridad, la realización de auditorías internas y externas, el uso de herramientas específicas de monitorización del tráfico y de las redes, la mejora de los procesos de análisis y definición de causas raíces de actividades sospechosas, la gestión y monitorización de los cortafuegos y de los centros de operativas de seguridad, los grupos de trabajo de alto rendimiento para la gestión integral de los servicios y el plan director para la gestión preventiva de riesgos de la transformación digital.

Procesos de detección y respuesta inmediata

Estos procesos comprenden la monitorización continua de los sistemas de alerta ante incidentes, los procesos de análisis de patrones de eventos de seguridad, la utilización de herramientas de prevención de la fuga de información, la creación de comités específicos para el análisis y gestión de actividades sospechosas o ciberincidentes, la mejora de procesos de la trazabilidad de actividades de análisis de ciberseguridad y la mejora de los procesos de gestión de incidentes.

Procesos de análisis y de cierre de ciberincidentes

Estos procesos comprenden la mejora de los procesos de gestión de incidentes, la mejora de los procesos de almacenamiento de evidencias, sistemas de trazabilidad y definición de marcos de gestión de la cadena de custodia.

Diseño y desarrollo de soluciones

Esta actividad comprende la utilización de vías de codificación segura, el análisis del código que genera el desarrollador antes de su subida al repositorio en las herramientas del ciclo de vida, las pruebas adicionales sobre las aplicaciones en la promoción entre entornos mediante el uso de herramientas tipo DAST y SAST, y el análisis adicional de código realizado por parte de terceros.

Uso y explotación de servicios

Esta funcionalidad comprende la implementación de procesos periódicos de análisis del código estático por parte de terceros, la implementación de marcos de análisis de vulnerabilidades y la mejora del marco de gestión de la seguridad perimetral con el rediseño de las actividades que incluyen las pruebas de penetración por parte de terceros.

Durante 2019 la consolidación y el fortalecimiento de la ciberseguridad se basaron en:

- Definir un nuevo marco para la gestión integral de amenazas de seguridad.
- Reforzar el marco de controles en materia de seguridad.
- Elaborar un plan de transformación digital en materia de ciberseguridad.
- Reforzar las políticas de buen gobierno y enfoque de la ciberseguridad durante todo el ciclo de vida de los servicios.
- Fortalecimiento de la actividad de la segunda línea de defensa y cumplimiento, aplicando la gestión integral del marco de ciberseguridad, aunando las exigencias regulatorias, legales, normativas, así como los marcos internacionales de mejores prácticas desde el diseño y creando modelos sostenibles.
- Mejora del marco de formación y concienciación en materia de ciberseguridad.

Resultados de la gestión durante el ejercicio 2019

Durante el ejercicio 2019 el cumplimiento de los acuerdos de nivel de servicio relativos a la disponibilidad de aplicaciones y sistemas fueron razonables. Se destaca la mejora en el cumplimiento del ANS en el centro de información y en la atención a los usuarios.

A continuación, se presentan los resultados obtenidos de la gestión de la calidad en la tecnología y sistemas de información:

GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN			
VARIABLE	AÑO 2019	AÑO 2018	VARIACIÓN
Cumplimiento ANS plataforma bancaria	99,85 %	99,90 %	-0,05 %
Cumplimiento ANS medios de pago	99,96 %	100,00 %	-0,04 %
Cumplimiento ANS centro de información	99,04 %	93,00 %	+6,04 %
Cumplimiento ANS intercambio	100,00 %	100,00 %	0 %
Cumplimiento ANS banca a distancia	99,89 %	99,90 %	-0,01 %
Cumplimiento ANS atención a usuarios	96,90 %	96,20 %	+0,70 %
Valores medios	**99,71 %**	**98,17 %**	

El cumplimiento de los acuerdos de nivel de servicio relativos a la atención prestada, tanto a cajas como a clientes finales en los dos ejercicios, son muy similares, destacando la mejora en la resolución de incidencias.

ATENCIÓN A CLIENTES E INCIDENCIAS			
VARIABLE	AÑO 2019	AÑO 2018	VARIACIÓN
Atención a llamadas de clientes finales	100 %	100,0 %	0 %
Atención de llamadas al CAU–Centro de Atención a Usuarios	100 %	100,00 %	0 %
Resolución de incidencias	87,62 %	84,91 %	+2,71 %
Tiempo de espera llamadas clientes finales	100 %	100,0 %	0 %
Valores medios	**96,90 %**	**96,23 %**	

Nuevo posicionamiento estratégico para el periodo 2020-2022

Para el periodo 2020-2022 se plantean los siguientes desarrollos y mejoras, en relación con los riesgos tecnológicos internos, externos y las políticas de externalización de servicios:

- El principio de proporcionalidad.
- La gobernanza y estrategia.
- El marco de gestión de riesgos.
- La seguridad de la información.
- La gestión de las operaciones de las tecnologías de la información y de las telecomunicaciones.
- La gestión de proyectos y de cambios.
- La continuidad de negocio.
- La gestión de la relación con los usuarios de los servicios de pago.