4.6. Gestió de la tecnologia i de la informació

“La tecnologia i la digitalització són eines estratègiques en l’eficiència i en el valor d’un negoci, en les experiències de més valor dels grups d’interés i en la preparació d’informació estratègica per a la presa de decisions.”

Una de les categories que s’integren dins del sistema de gestió dels grups d’interés de Caixa Popular és la dels “aliats socis”, en què se situa l’empresa participada RSI (Rural Serveis Informàtics). Per a enfortir el valor de gestió dels sistemes d’informació de l’entitat i de la visió estratègica de generar i capitalitzar aliances, utilitza els serveis informàtics comuns d’aquesta empresa.

RSI és responsable de les activitats de desenvolupament o millora de les aplicacions clau del negoci, de la ubicació de dades, de la seguretat informàtica d'aquestes, de les pàgines web, etc., i estableix protocols per a utilitzar-les de manera diferenciada per totes les empreses del Grup.

RSI posseeix certificacions i fa auditories independents que avalen l'excel·lent gestió de la seguretat i la ciberseguretat:

- ISO 27001 Sistema de gestió de la seguretat informàtica.
- ISO 38500 Governança de la tecnologia de la informació.
- ISO 22301 Sistema de gestió per a la continuïtat del negoci.
- ISO 22320 Sistema de gestió per a la resposta davant d'emergències.
- CMMi (CVS) Cicle de vida de programari (nivell 3).
- LEET Security amb el nivell màxim AAA+ l'any 2019.
- Certificats específics de seguretat:
- Certificació PCI/DSS: certificat de l'estàndard de seguretat de dades en targetes.
- Certificació CSP de Swift: certificació de seguretat per a pagaments per Swift.
- Auditories d'assegurament del marc de control intern europees:
- ISAE 3402 Tipus 2: Per a l'eficàcia operativa de marc de control intern en la gestió dels processos generals de TI.
- SOC 2 Tipus 2: Per a l'eficàcia operativa de marc de control intern en la gestió dels processos de seguretat i ciberseguretat de TI.

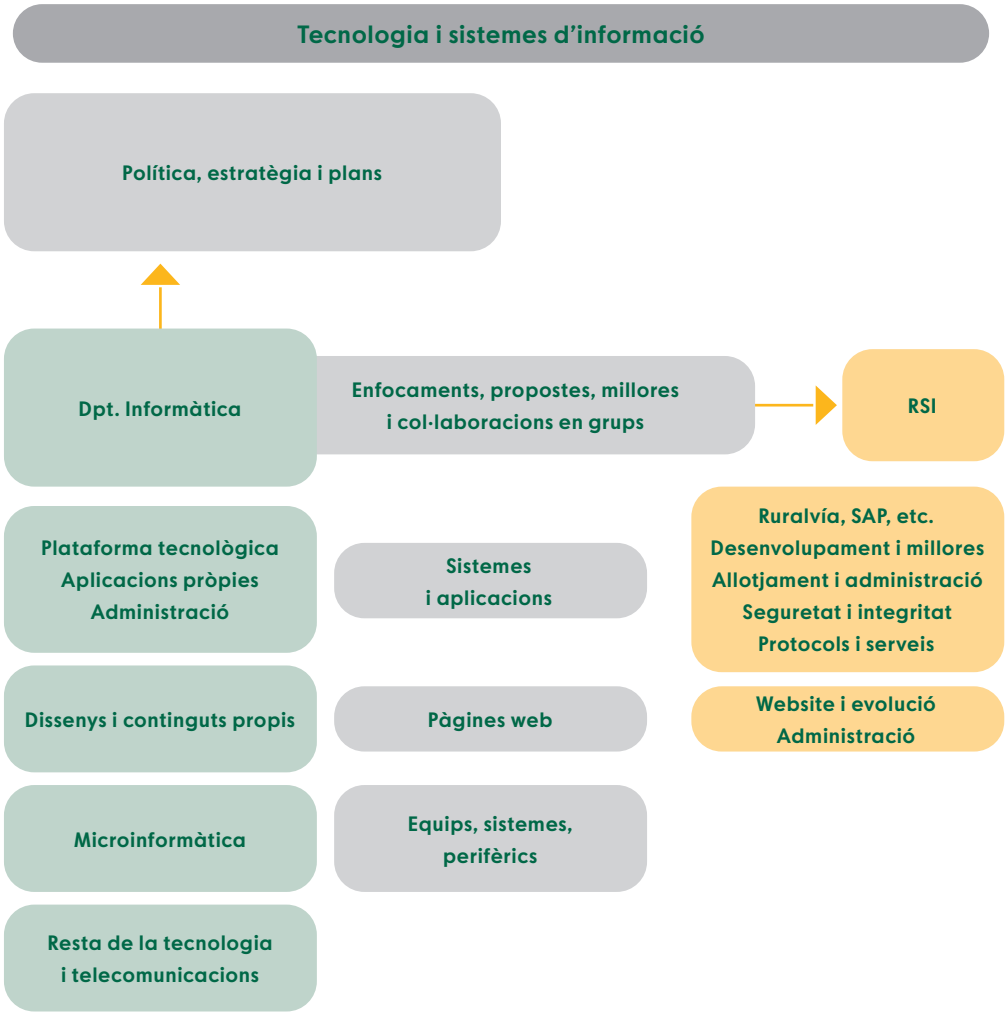
De manera complementària, també té altres certificacions de gran valor per a incrementar la confiança i el valor de la gestió:

- UNE 19601 Sistema de gestió de *compliance* o compliment normatiu penal.
- ISO 37001 Sistema de gestió antisuborn.

L'Àrea d'Informàtica de Caixa Popular és responsable de la planificació de projectes i actuacions relatives als sistemes i als mitjans informàtics de l'organització, la definició de la plataforma informàtica, la seguretat de processos i sistemes, la gestió i l'operativitat d'equips informàtics (servidors, ordinadors...), xarxes, dispositius de suport (impressores, etc.), programari, solucions de telecomunicació, telefonia, la microinformàtica i desenvolupaments locals, i la gestió de la resta de la tecnologia del negoci, amb la investigació i les proves associades.

Model de tecnologia i de sistemes d'informació i telecomunicació

El model de tecnologia i de sistemes té una responsabilitat compartida entre RSI i el departament de sistemes que participa en tots els grups de treball d'RSI (especialment el d'informàtica i el d'organització) per a aportar millores, innovacions i influir en les decisions tècniques i en la definició i la priorització de projectes.



Aplicacions (principals i locals), nous desenvolupaments i millores

Les aplicacions principals utilitzades per les empreses del Grup són la de "Banca en línia (Ruralvía)", la de "Gestió de persones (SAP)" i les de "Gestió del negoci (IRIS NTF)", que resideixen en RSI i són responsabilitat completament seua.

Actualment hi ha dos grans macroprojectes pluriennals de valor en la gestió de les tecnologies de la informació:

- La protecció contra el crim cibernètic (sabotatges, pirateria, caixers i targetes, i robatoris d'identitat).
- El projecte d'estratègia digital "Impulsa't" amb la renovació d'actius digitals, nous canals d'interacció, noves propostes de valor, potenciació de la cultura digital, intel·ligència empresarial (*business intelligence*) i el màrqueting digital

L'any 2019 els avanços principals van ser:

- L'evolució NTF, incloent-hi eines d'administració per a l'usuari final i millores GED-gestió electrònica de documents.
- L'enfortiment de la seguretat lògica (model i pla).
- La millora dels entorns de prova.
- El desenvolupament d'una eina de traçabilitat de les errades de migració.
- La implantació d'un mètode de mesurament de la qualitat en telefonades al centre d'atenció telefònica.
- La reducció del temps d'espera al client a 30 segons.

Projectes rellevants:

- Nova banca digital amb una app millorada i de més funcionalitats.
- Google Pay, servei de pagament mòbil per a clients amb dispositius Android.
- Nova web comercial del Grup Caixa Rural.
- PSD2 *compliance* i estratègic: compliment de la nova normativa de serveis de pagaments digitals PSD2.
- Factoring Iris: aplicació per a integrar aquest producte en el terminal financer.
- Assistents de veu (*chatbots*): dissenyar i implantar un nou canal automatitzat d'atenció a clients i empleats.
- Mur de clients: implantar l'eina de mercat "Mur digital" que done cobertura a la figura que es va creant en les entitats de "Gestors digitals".
- Procés guiat d'assegurances: simplificació de l'operativa en oficines i d'usuaris.
- Ús de marques de protecció de dades en aplicacions: integració en les aplicacions de les noves marques de consentiment derivades de l'entrada en vigor de l'RGPD.
- Nou model de ràting de pimes.
- Adaptacions Llei de crèdit immobiliari: desenvolupaments per a complir la LCI.

Ciberseguretat

Les diferents línies d'actuació en matèria de ciberseguretat es poden estructurar en tres etapes: la prevenció del risc, la detecció ràpida i la resposta precisa davant de qualsevol ciberincident. Les principals línies d'actuació l'any 2019 van ser:

Processos de gestió preventiva

Aquests processos comprenen el reforç del servei de vigilància digital i antifrau, les proves de procediments i protocols de seguretat, la realització d'auditories internes i externes, l'ús d'eines específiques de monitoratge del trànsit i de les xarxes, la millora dels processos d'anàlisis i definició de causes arrels d'activitats sospitoses, la gestió i el monitoratge dels tallafocs i dels centres d'operacions de seguretat, els grups de treball d'alt rendiment per a la gestió integral dels serveis i el pla director per a la gestió preventiva de riscos de la transformació digital.

Processos de detecció i resposta immediata

Aquests processos comprenen el monitoratge continu dels sistemes d'alerta davant d'incidents, els processos d'anàlisis de patrons d'esdeveniments de seguretat, la utilització d'eines de prevenció de la fugida d'informació, la creació de comités específics per a analitzar i gestionar activitats sospitoses o ciberincidents, la millora de processos de la traçabilitat d'activitats d'anàlisis de ciberseguretat i la millora dels processos de gestió d'incidents.

Processos d'anàlisi de tancament de ciberincidents

Aquests processos comprenen la millora dels processos de gestió d'incidents, la millora dels processos d'emmagatzematge d'evidències, sistemes de traçabilitat i la definició de marcs de gestió de la cadena de custòdia.

Disseny i desenvolupament de solucions

Aquesta activitat comprén la utilització de vies de codificació segura, l'anàlisi del codi que genera el desenvolupador abans de penjar-lo al repositori en les eines del cicle de vida, les proves addicionals sobre les aplicacions en la promoció entre entorns mitjançant l'ús d'eines del tipus DAST i SAST, i l'anàlisi addicional de codi fet per part de tercers.

Ús i explotació de serveis

Aquesta funcionalitat comprén la implementació de processos periòdics d'anàlisis del codi estàtic per part de tercers, la implementació de marcs d'anàlisis de vulnerabilitats i la millora del marc de gestió de la seguretat perimetral amb el redisseny de les activitats que inclouen les proves de penetració per part de tercers.

Durant l'any 2019 la consolidació i l'enfortiment de la ciberseguretat es van basar en:

- Definir un marc nou per a la gestió integral d'amenaces de seguretat.
- Reforçar el marc de controls en matèria de seguretat.
- Elaborar un pla de transformació digital en matèria de ciberseguretat.
- Reforçar les polítiques de bon govern i enfocament de la ciberseguretat durant tot el cicle de vida dels serveis.
- Enfortir l'activitat de la segona línia de defensa i compliment, aplicant-hi la gestió integral del marc de ciberseguretat, conjuminant les exigències reguladores, legals, normatives, i també els marcs internacionals de millors pràctiques des del disseny i creant models sostenibles.
- Millorar el marc de formació i conscienciació en matèria de ciberseguretat.

Resultats de la gestió durant l'exercici 2019

Durant l'exercici 2019 el compliment dels acords de nivell de servei relatius a la disponibilitat d'aplicacions i sistemes van ser raonables. Es destaca la millora en el compliment de l'ANS en el centre d'informació i en l'atenció als usuaris.

A continuació, es presenten els resultats obtinguts de la gestió de la qualitat en la tecnologia i els sistemes d'informació:

GESTIÓ DE LA TECNOLOGIA I INFORMACIÓ			
VARIABLE	**ANY 2019**	**ANY 2018**	**VARIACIÓ**
Compliment ANS plataforma bancària	99,85 %	99,90 %	-0,05 %
Compliment ANS mitjans de pagament	99,96 %	100,00 %	-0,04 %
Compliment ANS centre d'informació	99,04 %	93,00 %	+6,04 %
Compliment ANS intercanvi	100,00 %	100,00 %	0 %
Compliment ANS banca a distància	99,89 %	99,90 %	-0,01 %
Compliment ANS atenció a usuaris	96,90 %	96,20 %	+0,70 %
Valors mitjans	**99,71 %**	**98,17 %**	

El compliment dels acords de nivell de servei relatius a l'atenció prestada, tant a caixes com a clients finals en els dos exercicis, són molt semblants i hi destaca la millora en la resolució d'incidències.

ATENCIÓ A CLIENTS I INCIDÈNCIES			
VARIABLE	**ANY 2019**	**ANY 2018**	**VARIACIÓ**
Atenció a telefonades de clients finals	100 %	100,0 %	0 %
Atenció de telefonades al CAU–Centre d'Atenció a Usuaris	100 %	100,00 %	0 %
Resolució d'incidències	87,62 %	84,91 %	+2,71 %
Temps d'espera telefonades clients finals	100 %	100,0 %	0 %
Valors mitjans	**96,90 %**	**96,23 %**	

Nou posicionament estratègic per al període 2020-2022

Per al període 2020-2022 es plantegen els desenvolupaments i les millores següents, en relació amb els riscos tecnològics interns, externs i les polítiques d'externalització de serveis:

- El principi de proporcionalitat.
- La governança i l'estratègia.
- El marc de gestió de riscos.
- La seguretat de la informació.
- La gestió de les operacions de les tecnologies de la informació i de les telecomunicacions.
- La gestió de projectes i de canvis.
- La continuïtat de negoci.
- La gestió de la relació amb els usuaris dels serveis de pagament.