Definició, creació i implantació de CSIRT_FGC a Ferrocarrils de la Generalitat de Catalunya

Nom de l'estudiant: Noé Jiménez Maturano

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les comunicacions (MISTIC)
Seguretat en xarxes i sistemes
Seguretat en serveis i aplicacions
Àrea: PFM ad-hoc
Consultor: Jordi Guijarro Olivares
Professor/a responsable de l'assignatura: Antoni González Círia
Centre: Universitat Oberta de Catalunya
Data d'entrega: 4 de juny de 2018

FITXA DEL TREBALL FINAL

Títol del treball:	*Definició, creació i implantació de CSIRT_FGC a Ferrocarrils de la Generalitat de Catalunya*
Nom de l'autor:	*Noé Jiménez Maturano*
Nom del consultor/a:	*Jordi Guijarro Olivares*
Nom del PRA:	*Antoni González Círia*
Data de lliurament:	*06/2018*
Titulació o programa:	*Màster Universitari en Seguretat de les Tecnologies de la Informació i de les comunicacions (MISTIC)* *Seguretat en xarxes i sistemes* *Seguretat en serveis i aplicacions*
Àrea del Treball Final:	*TFM ad-hoc*
Idioma del treball:	*Català*
Paraules clau	*CSIRT, FGC, Resposta incidents seguretat*

Resum del Treball:

Aquest TFM, neix amb la finalitat de crear un equip de resposta a incidents de seguretat a Ferrocarrils de la Generalitat de Catalunya.

FGC, com moltes altres empreses té un especial interès en la protecció de les seves dades e informació empresarial. És per aquest motiu que sorgeix la necessitat de l'estudi, l'anàlisi i la creació d'un CSIRT que vetlli per la seguretat de la informació i doni resposta, eficaç i eficient, a qualsevol incident de seguretat, permetent una contingència i recuperació ràpides.

Per dur a terme aquest objectiu, s'ha realitzat un estudi sobre els CSIRT i el seu estat de l'art, així com s'ha realitzat un anàlisi que justifiqués els motius i beneficis de la creació d'aquest equip a FGC.

Fet l'anàlisi i selecció de les eines adients, s'ha analitzat, estructurat, definit i creat tota la estructura més adient per l'equip de resposta envers a FGC. S'ha de tenir en compte que els serveis que ofereix un equip estan íntimament lligats al grup de clients a qui donarà servei i aquest han d'estar ben planificats i justificats, per que l'equip tingui èxit.

Fen balanç del desenvolupament d'aquest projecte, podem dir, que l'objectiu ha estat assolit, ja per part del cap de TI sota el qual hi ha la previsió que

arrenqui el CSIRT_FGC, en tot moment ha tingut tota la documentació i informació necessàries per poder prendre la decisió de crear l'equip. I per altra banda, un cop definida i creada l'organització de l'equip, la interacció amb els clients i els serveis que ha d'oferir, ha mostrar la seva conformitat.

Finalment, a l'entrega d'aquest TFM esta pendent l'arrencada de l'equip.

Abstract:

This TFM, was created with the purpose of creating a security response team in Ferrocarrils de la Generalitat de Catalunya.

FGC, like many other companies, has a special interest in protecting their data and business information. It is for this reason that the need arises for the study, analysis and creation of a CSIRT that safeguards for the security of the information, and gives an efficient response to any security incident and allows a fast contingency and recovery.

To carry out this objective, a study on the CSIRT and its state of the art has been done, as well as an analysis that justified the reasons and benefits of the creation of this team in FGC.

Made the analysis and selection of the appropriate tools, the most appropriate structure for the response team towards FGC has been analysed, structured, defined and created. It should be taken into account that the services offered by a team are intimately linked to the group of clients to whom it will provide service and this must be well planned and justified, so that the team is successful.

This is a great achievement in the development of this project, we can say, that the objective has been achieved, already by the IT chief under which there is the forecast to start the CSIRT_FGC, has at all times had all the necessary documentation and information to be able to make the decision to create the team. On the other hand, once the organization of the team has been defined and created, the interaction with the clients and the services that it has to offer, has shown its conformity.

Finally, to the delivery of this TFM is pending the startup of the team.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

Avui en dia totes son moltes les empreses que son molt conscients de la importància de mantenir segures les seves dades de negoci. És per això que la majoria adopta mesures de gestió de riscos en ciberseguretat. Per norma aquesta gestió de riscos es basa en avaluacions anuals o auditories del programa de seguretat establert.

El problema es troba en que moltes empreses que compleixen el seu programa de seguretat es troben amb incidents de seguretat greus (fuga d'informació, atacs a sistemes crítics, etc.), això es degut a que les empreses son dinàmiques i en canvi constant i les auditories representen un estat dels sistemes concret.

Moltes vegades, en l'anàlisi de les causes d'incidents es quan es troben indicis que apunten a respostes no efectives per part de les organitzacions. Es va complir amb l'auditoria, però les coses han canviat i ningú ha estat conscient del canvi ni del risc que comportava.

Amb tot això, veiem que les empreses que basen la seva gestió del risc en complir auditories de seguretat, comencen la seva resposta davant d'incidents massa tard, quan un incident greu ja s'ha produït. Això evidencia que les mesures que s'han definit per protegir els actius de l'empresa no estan funcionant.

Per aquest motiu, en aquest projecte es vol crear un CSIRT, que realitzi activitats adients per protegir els actius crítics definits d'acord amb els objectius de gestió de risc de seguretat cibernètic.

El que es vol aconseguir es que hi hagi una prevenció continua i actuació davant d'incidents de seguretat en tot moment. Que es tingui la capacitat de prevenció i reacció davant d'aquest incidents i no ens haguem de limitar a analitzar el que ha succeït i posar remei (quan ja s'han perdut dades, han caigut sistemes, etc.)

1.2 Objectius del Treball

A continuació, s'enumeren els objectius que es volen assolir en la realització d'aquest TFM:

1. Anàlisi i documentació de CSIRT. Estudi i estat de l'art dels CSIRTS actuals.

2. Creació d'un equip, CSIRT_FGC que ofereixi serveis a l'edifici d'oficines de FGC.

3. Coordinació i proposta de posada en funcionament de l'equip amb un mínim d'activitats ofertes.

1.3 Enfocament i mètode seguit

Per resoldre la part teòrica sobre els CSIRT i la cerca de guies sobre les que es basarà la creació del CSIRT_FGC, es farà servir una metodologia de revisió bibliogràfica. Es procedirà a una investigació documental, que ens proporcionarà una visió complerta del tema tractat i ens facilitarà la selecció de les guies que es faran servir.

Pel que fa a l'estudi i la definició dels serveis importants que ens definiran el catàleg de serveis sobre el que ens basarem, es seguirà una metodologia d'entrevistes i enquestes que ens permetrà aconseguir el catàleg de serveis a protegir en l'edifici d'oficines.

Per justificar la definició de serveis que oferirà el nou CSIRT, es confeccionarà un anàlisi DAFO, que ens permetrà avaluar des debilitats, amenaces, fortaleses i oportunitats de la implantació d'aquest CSIRT i els seus serveis. Amb aquest anàlisi, podrem decidir raonada i justificadament, quins seran els serveis indispensables a oferir segons les necessitats del grup a qui donarà servei.

Per tal de fer oficial la creació del nou equip de resposta d'incidents, es definirà el document RFC-2350, en el que es detallarà tot el detalls i funcionalitats que oferirà el nou CSIRT. En aquest document s'identifica el tipus de CSIRT, el perquè de la seva creació, a qui presta servei, els serveis oferts, temps en activitat, enfoc futur, etc. A més en aquest document es defineix en que es caracteritzarà, es definirà la seva missió, visió i valors.

Finalment, seguint una metodologia de entrevistes i reunions, s'avaluarà el moment idoni per la posada en marxa del CSIRT_FGC amb els responsables de tecnologia.

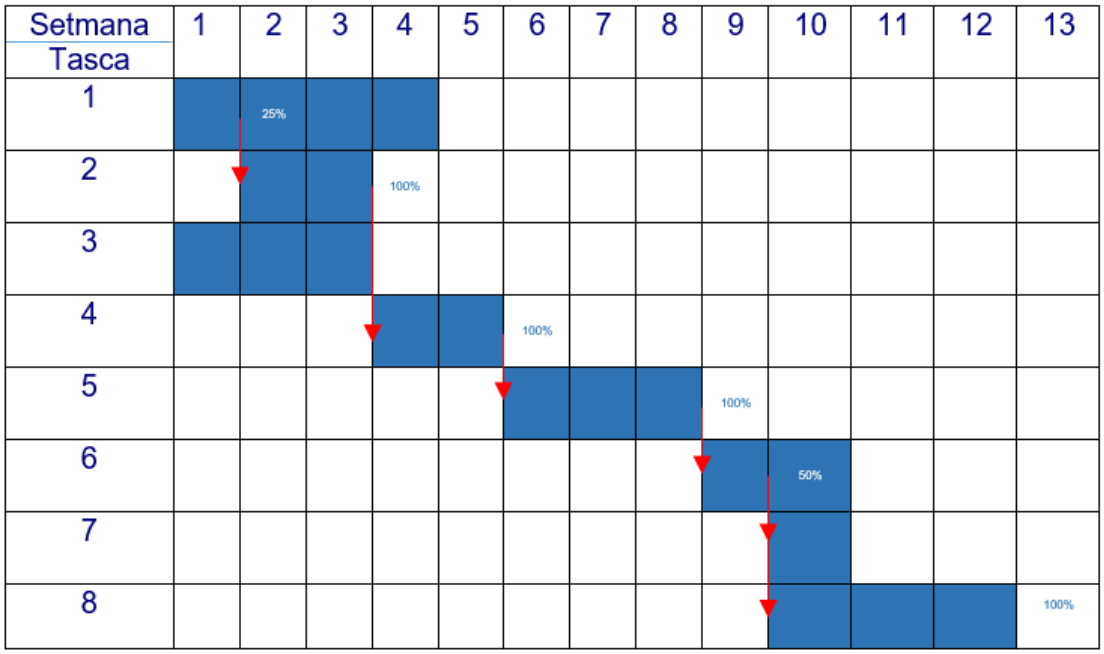
1.4 Planificació del Treball

Les tasques a realitzar en el TFM són les que es defineixen a continuació. Aquestes donen la idea a grans trets del que s'ha d'anar realitzant per assolir els objectius:

1. Cerca d'informació i documentació CSIRT.
2. Estudi i selecció de guies per elaborar CSIRT (ENISA, i d'altres).
3. Identificar necessitats, riscos i problemàtiques pròpies de l'entorn empresarial d'oficines.
4. Realitzar estudi i confeccionar anàlisi DAFO per definir i justificar serveis que oferirà CSIRT.
5. Definir i elaborar el document RFC-2350 d'un nou equip de resposta d'incidents de seguretat que donarà servei a les oficines corporatives de FGC.
6. Definir serveis mínim que s'oferiran inicialment.
7. Posada en marxa de l'equip.

Entrant més en detall, la planificació temporal detallada d'aquestes tasques amb les seves dependències serà la següent:

1. Investigació, cerca d'informació i documentació (CSIRT, ENISA i altres).
2. Estudi i selecció de guia més adient per crear CSIRT.
3. Obtenir catàleg de serveis a protegir en el pla de risc.
4. Realitzar DAFO.
5. Definir, crear i justificar serveis recomanats.
6. Definir i redactar la RFC-2350 pel nou CSIRT_FGC.
7. Decidir serveis mínims per posada en marxa.
8. Posada en servei i arrancada del nou CSIRT_FGC.



Il·lustració 1: Planificació del TFM

1.5 Breu revisió de l'estat de l'art

Actualment a FGC, pel que fa a la seguretat de la informació es regeix per la normativa ISO 27001. A banda de diferents auditories de seguretat que es duen a terme en les entitats públiques, FGC esta en compliment de l'ENS.

Tot i que es compleixen els requeriments i recomanacions de les auditories passades i el seguiment de la ISO 27001, actualment no es compta amb un equip de resposta a incidents de seguretat que pugui preveure o evitar possibles incidents de seguretat que sorgeixin intrínsecament al dinamisme de l'empresa.

El dinamisme i l'interès per les tecnologies de avantguarda per part de FGC per millorar i oferir un servei d'excel·lència, fa que es pugin donar casos on podem tenir incidents de seguretat, que no han estat contemplats en auditories, tal i com hem explicat anteriorment.

Aquesta situació, propicia la proposta de creació d'un CSIRT_FGC, objecte d'aquest TFM i que tindrà com a principal missió vetllar i intentar preveure possibles incidents de seguretat que es poden donar en els impassos temporals entre les auditories que es duen a terme.

2. Anàlisi

Actualment, el nombre d'incidents de seguretat reportats per les empreses, cada cop és més elevat. Cada cop hi ha un número més elevat d'atac, més sofisticats i perillosos.

Segons l'INCIBE (Institut Nacional de Ciberseguretat de Espanya), al 2017 es van reportar més de 120.000 incidents de seguretat i segons els seus anàlisis es una dada que va en augment en els últims anys. Des de l'any 2014 la tendència ha estat la següent:

- ·Any 2014: 18.000 incidents registrats.
- ·Any 2015: 50.000 incidents registrats.
- ·Any 2016: 115.000 incidents registrats.
- ·Any 2017: 120.000 incidents registrats.

Segons Karspersky Lab, en el seu conegut informe de seguretat del 2017, es van detectar més de 15.714.700 objectes maliciosos únics (scripts, espolits, arxius executables, etc.) i 199.455.606 URLs úniques. Segons Karspersky Lab, les seves solucions van detectar i neutralitzar 1.188.728.338 atacs maliciosos llançats des de recursos a la xarxa localitzats en 206 països en tot el mon.

Com podem veure, la tendència dels ciberatacs esta en alça. A més hem de tenir en compte la tendència a la mobilització en les empreses actuals. En la majoria d'empreses hi ha previst o en marxa un pla de digitalització, que implicarà dotar al seu personal de més equips informàtic que contindran dades personals i/o empresarials i que seran susceptibles de ser atacats.

Tenint sobre la taula totes aquestes variables, podem intuir fàcilment la necessitat de protegir i vetllar per la seguretat tant dels usuaris, com els recursos i sistemes d'informació de les empreses. És per aquest motiu que la majoria d'organitzacions intenten complir amb les normatives de ciberseguretat, passar les auditories pertinent i millorar tots els seus sistemes.

A vegades, l'estricte compliment de la normativa i el compromís de solucionar errors o problemes detectats en auditories periòdiques, no és suficient. No ens garanteix de cap manera donar una bona resposta a incidents de seguretat donats. La formació del personal qualificat, definició d'objectius i tasques periòdiques a dur a terme, definició de pla de riscos, conscienciació, informació i formació als usuaris, etc., son tasques que fan que el tractament dels incidents de seguretat sigui més eficient i fins i tot es pugui reduir el seu nombre.

El dia a dia dels departaments de TI, tot i tenir definits bons plans d'acció i de resposta a ciberincidents, fa que moltes bones practiques, accions preventives i el reciclat i actualització dels coneixements sobre seguretat (els canvis en el món de la ciberseguretat són molt ràpids), no es dugui a terme i com a conseqüència ens trobem amb personal o àrees de l'empresa que no tenen la capacitat, formació i a vegades els recursos per coordinar, contenir i restablir-se d'atacs greus de la seguretat.

La situació real de moltes empreses és que estan en compliment de la legalitat, tenen definits plans de contenció i d'actuació, definits plans de riscos, etc., passen periòdicament les auditories (intentant millorar o corregir errors detectats), però no hi ha cap acció més fins a la següent auditoria. Aquí podem trobar enormes riscos de seguretat, ja que entre el pas d'auditories, es poden actualitzar equips, aparèixer noves vulnerabilitat (Zero Day) i infinitats de canvis més que poden suposar un greu forat de

seguretat i no s'és conscient fins que tenim un incident de seguretat (si es que s'adonen) o es torna a passar una auditoria i es detecta.

Per aquest motiu sorgeix el plantejament d'aquest projecte, d'implantació un CSIRT. Tenint en compte que avui en dia totes les àrees de l'empresa estan connectades, informatitzades i comparteixen fins i tot algunes àrees de negoci, és evident que el tema de la seguretat es imprescindible. La seguretat avui en dia en una empresa ha de ser transversal i atènyer a totes les àrees. Per aquest motiu es més que adient la creació d'un equip de resposta a incidents de seguretat que vetlli per la seguretat de tots els aspectes relacionats amb les TI.

La creació d'un CSIRT en una empresa, dona un plus en el tractament de la seguretat de la informació en totes les àrees de l'empresa. Centralitza tota la gestió de la seguretat en un equip de professionals amb coneixements elevats sobre aquest tema que seran capaços de realitzar tasques proactives, preventives i de gestió que ens permetran gestionar de manera ràpida i eficaç qualsevol incident de seguretat i fins i tot en alguns cassos preveure-ho i evitar-ho.

3. Motivació

La motivació per realitzar aquest projecte de definició i creació d'un equip de resposta a indecents de seguretat en FGC, ve donada per interès de dotar d'un nivell d'excel·lència a la gestió de la seguretat informàtica a l'empresa.

El que es vol aconseguir és conscienciar al personal de la importància de la seguretat informàtica en els temps que corren. Centralitzar i donar a l'empresa un punt de referencia pel tractament de qualsevol incident o consulta sobre la seguretat informàtica. I sobretot, el que es vol, és crear un equip de professionals qualificats en seguretat amb les capacitats per dur a terme tasques tant preventives, com proactives, com de gestió de qualitat, en tot el que fa referencia a la seguretat informàtica.

Tal i com s'ha comentat, hi ha una tendència a la mobilització informàtica de tot el personal en totes les empreses. En FGC, també hi és, hi ha un pla de mobilitat que el que vol aconseguir és que tot el personal de l'empresa tingui la possibilitat de treballar, així com accedir als recursos que ofereix l'empresa des de qualsevol lloc (amb diversitat de dispositius). Això, implica diversitat de dispositius, noves aplicacions, diferents sistemes operatius, diferents casos d'ús segons els usuaris, etc., en definitiva tot un repte per a la seguretat de la informació. És per això que és planteja en aquest TFM la creació d'un CSIRT_FGC amb l'objectiu de prevenir, detectar, respondre i recuperar qualsevol incident relacionat amb la seguretat informàtica, així com ser el referent per a tota l'empresa i ser el coordinador de tota acció relacionada amb la seguretat informàtica a FGC i amb l'exterior.

4. Investigació i estudis de CSIRT

Les estadístiques actuals d'atacs contra sistemes d'informació, son cada dia més amplies. Els atacs a sistemes d'informació son cada dia més nombrosos, variats i a més cada cop més perillosos i nocius.

Tot i les accions i mesures que es prenen per prevenir aquests atacs en funció dels resultats dels anàlisis de riscos, auditories, etc., que contribueixen a reduir el nombre de ciberincidents, no tot es pot prevenir. Hem de ser conscients com a responsables de seguretat que incidents tindrem, és per això que es fa necessari tenir una capacitat de resposta a aquests incidents adequada i eficaç.

Bàsicament la capacitat de resposta davant de ciberincidents ens ha de permetre, detectar ràpidament atacs i amenaces, minimitzar pèrdues i/o destrucció d'actius tecnològics o d'informació, mitigar l'explotació de punts febles de les infraestructures tecnològiques, així com recuperar els serveis i la normalitat en el menor temps possible.

Gestionar adequadament els ciberincidents, constitueix un conjunt d'activitats complexes que requereixen una planificació molt detallada i una assignació adequada de recursos necessaris. En molts cassos, és necessària una estreta col·laboració entre diferents àrees i departaments empresarials això com amb proveïdors externs (de software, hardware, de plataformes al núvol, etc.).

Tenir una adequada capacitat de resposta davant de ciberincidents, dona grans beneficis a les empreses. Permet abordar la gestió dels incidents de seguretat de manera sistemàtica, és a dir seguint una metodologia, cosa que facilita la realització i pressa de decisions més adequades. Les fases a tenir en compte en la gestió dels ciberincidents son:

1. Preparació: Formació d'equip de resposta i selecció d'eines i recursos necessaris. També s'identifica i despleguen mesures de seguretat en funció d'un previ anàlisi de riscos.
2. Detecció, anàlisis i notificació: Anàlisi i detecció de possibles bretxes de seguretat en els sistemes d'informació. Desencadenament de processos de notificació.
3. Contenció, eradicació i recuperació: Fase on en primera instancia s'intenta mitigar l'impacte produït. Un cop contingut, es procedirà a eliminar la causa de l'incident i finalment es recuperaran els sistemes afectats. Aquesta fase s'ha de realitzar cíclicament fins a estar segurs que l'incident esta controlat.
4. Activitats post-ciberincident: Generació d'informes (origen, impacte, cost, mesures a prendre per evitar futurs atacs, etc.), per tal d'avaluar i justificar les actuacions i resultats davant del ciberincident.

Finalment, hem de comentar que hi ha diferents normatives de seguretat (ENS, ISO27001, etc.), que estableixen els requisits mínims que ha de contemplar tota política de seguretat de tota organització. Entre d'altres, ha d'especificar amb claredat la posició de l'equip de resposta davant incidents (ERI), les seves competències i . autoritat dintre de l'estructura empresarial i definir els rols i responsabilitats.

4.1 Introducció als CSIRT

Un CSIRT, és un equip d'experts en seguretat de les TI que tenen com a principal tasca respondre davant els incidents de seguretat informàtica. Els CSIRT, presten els serveis necessaris per ocupar-se i solucionar aquest incidents i ajudar a les organitzacions a qui presten servei a recuperar-se després de patir-ne un. A més, per minimitzar els riscos i minimitzar el nombre de respostes necessàries, molts CSIRT treballen de manera proactiva oferint serveis preventius i educatius als seus clients.

El terme CSIRT és el que es fa servir a Europa, “Computer Security Incident Response Team”, mentre que als EUA fan servir CERT o CERT/CC, “CERT Coordination Center” Existeixen altres sigles per a referir-se a aquests tipus d’equips:

- CERT o CERT/CC: Computer Emergency Response Team / Coordination Center
- CSIRT: Computer Security Incident Response Team
- IRT: Incident Response Team
- CIRT: Computer Incident Response Team
- SERT: Security Emergency Response Team

El primer equip d’aquestes característiques es va crear al 1988, arrel de l’incident que va provocar el cuc “Morris”. Aquest era un virus del tipus cuc, creat per Robert Tappan Morris i que s’estima que va infectar un 10% dels sistemes informàtics connectats a ARPANET (predecessor d’Internet). Aquest, feia servir una vulnerabilitat del sistema operatiu Unix per reproduir-se fins aconseguir bloquejar les màquines. Aquest succés va fer que saltés una alarma i que la gent fos conscient que era necessària una cooperació i coordinació entre administradors de sistemes i gestors de TI per afrontar i defensar-se d’aquests tipus d’incidents, ja que el temps de resposta era vital, per detectar, contenir, eradicar i recuperar l’incident.

És a posteriori d’aquest incident de seguretat, que la DARPA (Defence Advanced Research Projects Agency) poses en marxa el primer CSIRT, CERT Coordination Center (CERT/CC), cap al 1988 i ubicat en la Universitat de Camegie Mellon, en Pittsburg (Pensilvania).

Poc tems després, cap al 1992, el model es va exportar a Europa de mans de SURFnet (proveïdor acadèmic holandes), que va posar en marxa el primer CSIRT d’Europa, el SURFnet-CERT. Al 1993, va arrencar el BSI-CERT alemany, fins a l’actualitat que hi ha mes de 100 registrats a la guia de “Inventari d’activitats de CERT a Europa” de ENISA.

Amb el temps, els CERT van ampliar les seves capacitats oferint serveis de seguretat complert a banda de ser equips reactius únicament. Els serveis que van anar afegint incloïen, serveis proactius (alertes, avisos de seguretat, formació, etc.), serveis preventius (creació d’eines de seguretat, sistemes d’alerta, seguretat proactiva, etc.) i serveis de gestió de la seguretat. Aquest ampliació de serveis que ofereixen els converteix en prestadors de serveis de seguretat complerts que s’ocupen de tota la gestió d’incidents de seguretat en tot el seu espectre. Amb aquesta ampliació de serveis aquests equips es passen a anomenar CSIRT (Computer Security Incident Response Team) que defineix millor el seu camp d’actuació.

4.2 Àmbits d’actuació dels CSIRT

A tot el món, existeixen centenars de CSIRT, que tot i tenir com a objectiu general i principal la resposta als incidents de seguretat informàtica i la seva recuperació, tenen diferencies significatives en quant a la seva missió, el seu abast i a quina comunitat donen servei (grup de clients atesos pel CSIRT). Catalogar-los segons el grup de clients (o comunitat) a qui donen serveis és una pràctica general. A continuació veurem una mostra dels principals tipus de CSIRT que podem trobar actius en la actualitat:

·CSIRT acadèmics: donen servei a comunitats acadèmiques, universitats, facultats, escoles, etc. El seu tamany i instal·lacions, respon al de la comunitat i unifiquen esforços i investigacions amb altres CSIRT acadèmics.

·CSIRT comercials: són CSIRT que donen servei a diverses empreses que volen tenir externalitat aquests serveis. S’estableixen SLA amb les empreses per definir el nivell de servei, temps de resposta, etc. segons les necessitats de cada client.

·CSIRT d’infraestructures crítiques: aquest són els CSIRT que protegeixen els actius d’informació critica i les infraestructures d’una nació. Com que les institucions que

depenen d'aquests CSIRT poden ser de territoris (comunitats, regions, etc.) diferents, han d'establir protocols d'interacció amb altres equips.

·CSIRT governamentals: són els que donen servei a les institucions dels estats amb la finalitat de que les infraestructures de TI del govern i els serveis que donen als ciutadans tinguin nivells de seguretat adequats.

·CSIRT nacionals: són els CSIRT definits a donar servei a un país i es l'encarregat de coordinar a nivell nacional les respostes a incidents i el punt de contacte i referencia nacional i internacional.

·CSIRT interns: són els que presten serveis a les organitzacions a les que pertanyen.

·CSIRT militar: donen servei a les institucions militars d'un país. Les seves activitats es limiten a la defensa o a les capacitats cibernètiques ofensives d'una nació. Han de tenir coneixement específics de les TIC d'ús militar (armament, sistemes de radars, etc.).

·CSIRT de proveïdors: presten serveis relacionats a productes específics d'un fabricant, desenvolupador o proveïdor de servei. Aquest CSIRT tenen com a propòsit mitigar l'impacte de les vulnerabilitats o problemes de seguretat relacionats amb els seus productes.

·CSIRT de PIME: són CSIRT que donen resposta a incidents de seguretat molt individuals. Responen a les necessitat de petites entitats, empreses i usuaris.

4.3 Per què un CSIRT

Poder tenir un equip dedicat a la seguretat de les TI en una organització, ajuda significativament a mitigar i evitar en elevat percentatge els incidents greus de seguretat i ajuda a protegir el patrimoni, el negoci i la reputació d'aquestes organitzacions.

Altres avantatges significatives que podem ressaltar de tenir un CSIRT propi són:

·Disposar de coordinació centralitzada i un punt de contacte per a tota l'organització per qualsevol qüestió relacionada amb la seguretat de les TI.

·Reaccionar ràpidament als incidents relacionats amb la seguretat de TI, i tractar-los de manera especialitzada i centralitzada.

·Disposar a dintre de l'organització els coneixements tècnics per ajudar i assistir en la recuperació ràpida d'algun incident de seguretat.

·Tractament de qüestions legals i poder realitzar anàlisis forenses i disposar de proves en cas de litigis.

·Analitzar i avaluar l'estat i els progressos que s'aconsegueixen en l'àmbit de la seguretat.

·Fomentar bones practiques i cooperació en la seguretat de les TI en tots els membres a qui es dona servei (l'organització).

4.4 Beneficis de la gestió d'incidents amb CSIRT

Com ja s'ha comentat, la centralització de les activitats relacionades amb la seguretat de la informació és actualment una pràctica molt comuna. És una bona pràctica, ens permet complir amb la normativa vigent i dona la capacitat d'afrontar els incidents i riscos de seguretat que van sorgint de manera sistemàtica, eficaç i eficient.

Avui en dia, com ja hem comentat, afrontar les amenaces es molt important tenir un gran coneixement organitzatiu, normatiu i tècnic, a més de estar actualitzat i al dia de totes les qüestions sobre seguretat que van sorgint. Avui e dia, l'operativa i el manteniment de la gestió d'incidents de seguretat, requereix un esforç cada dia més elevat i que fa que aconseguir-ho amb equips dispersos o no especialitzats sigui una tasca molt complicada. D'aquí la centralització dels CSIRT.

Tenint en compte la normativa vigent (ENS – RD 3/2010) es requereix que els incidents de seguretat així com la seva resolució i tractament s'han de registrar i analitzar per la continua millora de la seguretat en el sistema a més s'ha de disposar d'un procés integral definit per afrontar incidents que impactin en la seguretat dels sistemes. Tot això, requereix d'un sistema de gestió i resposta a incidents, per aquest motiu centralitzar els recursos i processos per donar resposta total a incidents de seguretat (CSIRT) té nombroses avantatges. Principalment el que aconseguim es millorar els temps de resposta i recuperació en la gestió i resolució d'incidents de seguretat. Un CSIRT ho fa possible mitjançant:

·La centralització de la coordinació d'accions de contenció i resposta en tota l'organització, actuant com a referent i punt únic de contacte.

·L'increment de capacitat de coordinació amb altres CSIRT que poden compartir coneixements i experiències per ajudar a la prevenció o resolució d'incidents, que d'altra manera no es tindria accés.

·L'establiment del CSIRT com a centre d'excel·lència per donar el coneixement i suport per tal de que qualsevol membre de l'organització es pugui recuperar ràpidament dels incidents de seguretat soferts.

Respecte als beneficis que ofereix la gestió centralitzada dels incidents de seguretat que proporciona la implantació d'un CSIRT, en destaquem:

·Estalvi de costos: Per una banda concentrem i reduïm tot el coneixement altament especialitzat a un sol centre a partir del qual es difondrà a tota l'organització (estalvia costos en formació del personal no especialitzat). Per altra banda serà el CSIRT el que durà a terme a terme tots els serveis de gestió de seguretat (estalviant costos) o centralitzarà la contractació de tercers per dur-les a terme però amb uns nivells d'exigència a l'alçada.

·Millora de la qualitat de la gestió de la seguretat: Tenir un CSIRT altament especialitzat i dedicat a la gestió d'incidents ens permetrà millorar substancialment les actuacions davant incidents, actuant de manera més ràpida i eficient.

·Millora dels coneixements de seguretat: Part de les funcions que ofereix un CSIRT, son avisos, cursos i formacions del personal a qui presten el seus serveis. Això per una banda millora notablement els coneixements de seguretat dels empleats i a conseqüència es millora el nivell de seguretat a tota l'organització.

·Avaluar progressos en seguretat: Arrel del programes de formació, enquestes i KPIs de control de l'àmbit de seguretat, el CSIRT pot avaluar informes i realitzar seguiment de les millores i progressos que l'organització esta assolint en temes de seguretat.

·Millora en funcions legals i jurídiques: Un CSIRT, pot atorgar valor per la gestió i coordinació de qüestions normatives que s'han de complir i qüestions jurídiques que poden derivar d'incidents de seguretat. A més en cas d'anàlisis forenses i recaptació i protecció d'evidències en serien els més adients.

·Cooperació en millorar la seguretat: Exercint de punt central i referent, sensibilitzant i comunicant-se amb els membres de l'organització (formacions,

mailings, consultories, etc.), es fomenta la col·laboració, cooperació i la conscienciació d'aquest en la seguretat de les TIC.

4.4 Serveis que pot oferir un CSIRT

Com ja s'ha comentat en apartats anteriors, els CSIRT actuals ofereixen nombrosos serveis, son proveïdors de serveis integrals de seguretat. Dintre dels serveis que poden oferir hi ha una amplia gama, però fins l'actualitat no hi ha cap que el pugui prestar tots. Cada CSIRT, en funció de la seva missió, objectius i comunitat a la que donarà servei en fa una selecció. L'elecció del conjunt de serveis adequada constitueix una decisió crucial en la creació i el funcionament del CSIRT.

Els serveis que pot oferir un CSIRT es pot englobar dintre de tres categories:

·Serveis reactius: Serveis orientats al tractament de l'incident de seguretat sofert i la mitigació dels danys resultants. Aquests serveis son el component central de la tasca del CSIRT.

·Serveis proactius: Son serveis orientats a la prevenció d'incidents de seguretat mitjançant la sensibilització i la formació. El bon rendiments d'aquests serveis reduirà directament el nombre d'incidents en el futur.

·Serveis de gestió de la qualitat de la seguretat: Aquest serveis complementen i milloren els serveis de gestió d'incidents que ja es porten a terme en l'organització per part d'altres àrees (TI, Formació, Consultoria, etc.). Amb aquest serveis, el CSIRT aporta valor, fruit del seu coneixement especialitzat i experiència en seguretat ajudant a millorar la seguretat general de l'organització identificant riscos, amenaces o debilitat en els sistemes. Aquests serveis d'anàlisi, consultoria i formació, ens permet donar un plus a la gestió de la seguretat de l'organització i prevenir incidents futurs.

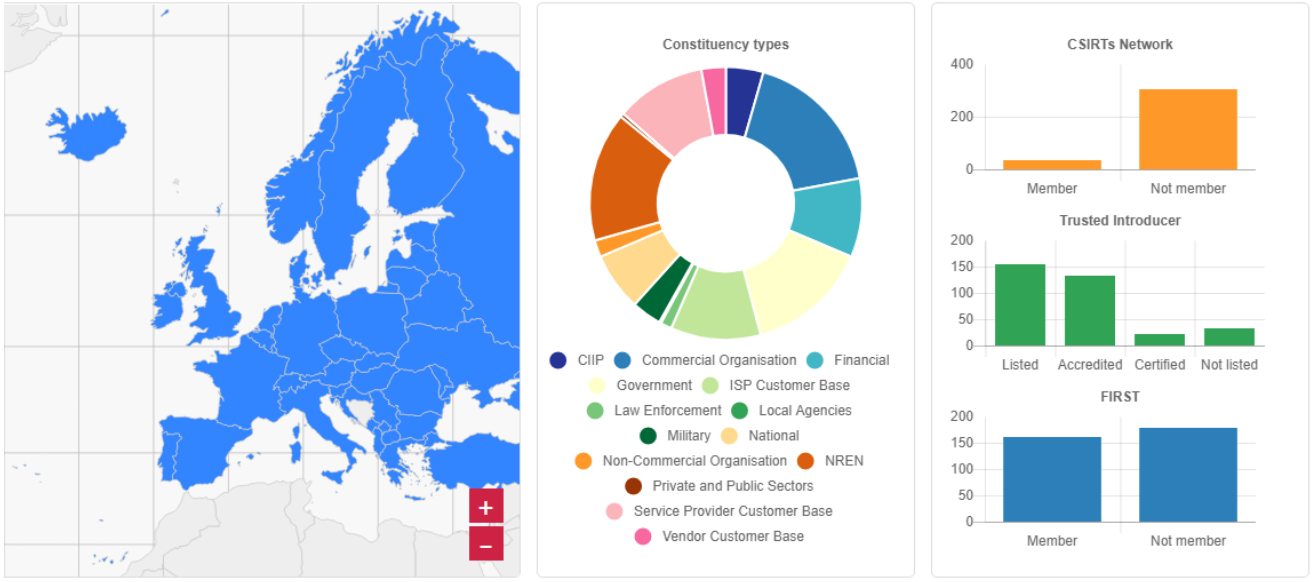
La llista de serveis més comuns dels CSIRT segons CERT/CC son:

Il·lustració 2: Llistat de serveis CSIRT

L'elecció dels serveis adients és molt important. La majoria de CSIRT, comencen amb un catàleg de serveis bàsics distribució d'alertes i advertències, comunicats i tractament d'incidències) i els van ampliant.

4.4 Estat de l'art dels CSIRT

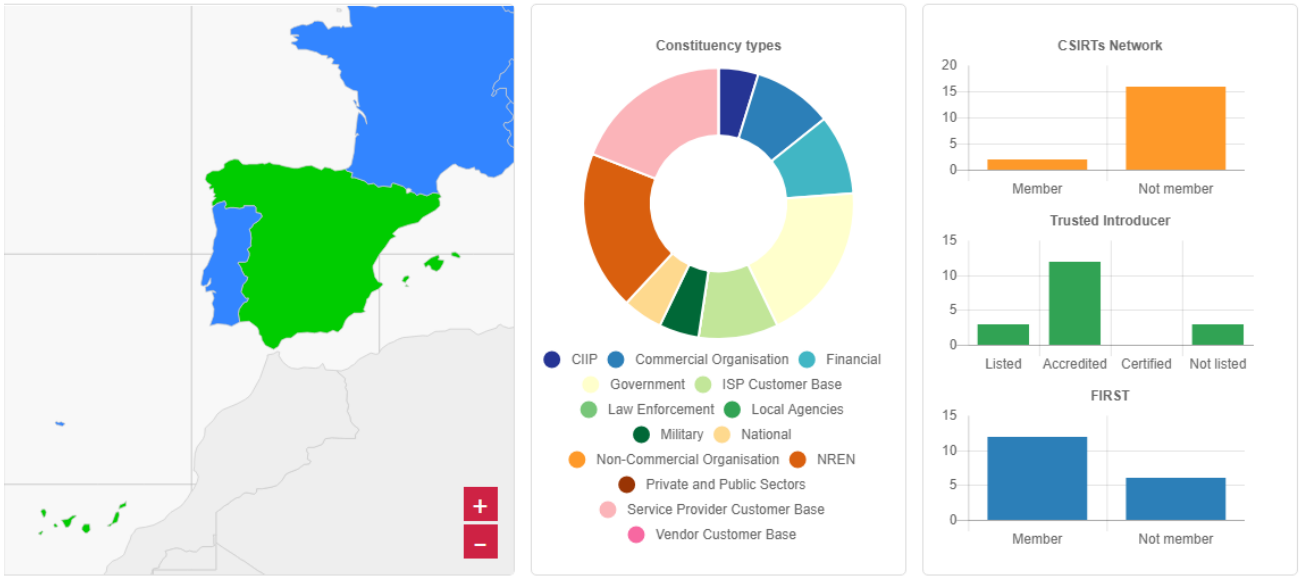
Actualment, segons l'inventari de CSIRT que manté l'agencia europea per la seguretat de les xarxes i la informació, ENISA, a tota Europa ens trobem aproximadament uns 342 CSIRT creats amb les següents característiques:



Il·lustració 3: Estat de l'art dels CSIRT d'Europa (ENISA)

Podem veure els tipus de CSIRT que predominen (comercials i governamentals entre altres), a més podem observar que la majoria estan connectats, que la majoria son membres d'alguna agrupació de CSIRT (CSIRTs Network, Trusted Introducer o FIRST).

Si entrem en detall de l'estat de l'art a Espanya, trobem la següent situació:



Il·lustració 4: Estat de l'art dels CSIRT a Espanya (ENISA)

Veiem que la majoria són membres de l'agrupació FIRST i TI, però només dos de CSIRTs Network. Veiem també que la majoria de CSIRT espanyols son governamentals (4), de proveïdors (3) i acadèmics (4). A continuació podem veure el llistat i la seva informació bàsica que ens permet fer-nos a la idea de l'estat de l'art en quant a nombre de CSIRT que hi ha actualment en territori espanyol.

Country	Team name	Constituency	CSIRTs Network	Trusted Introducer	FIRST	Contact
Spain	All teams	All types	Any status	Any status	Any status	
Spain	CCN-CERT	Government	Member	Accredited	Member	ccn-cert.cni.es
Spain	CERTSI	CIIP, National	Member	Accredited	Member	certsi.es
Spain	CESICAT-CERT	Government	Not member	Accredited	Member	cesicat.cat/cert/
Spain	esCERT-UPC	NREN	Not member	Accredited	Member	escert.upc.edu
Spain	RedIRIS	NREN	Not member	Accredited	Member	rediris.es/cert/
Spain	S21sec CERT	Service Provider Customer Base	Not member	Accredited	Member	cert.s21sec.com
Spain	TEFCSIRT	Commercial Organisation, ISP Customer Base	Not member	Accredited	Member	Public website not available
Spain	ENTELGY-CSIRT	Commercial Organisation, Service Provider Customer Base	Not member	Accredited	Member	entelgy.com
Spain	S2 Grupo CERT	Service Provider Customer Base	Not member	Accredited	Member	s2grupo.es
Spain	ESP DEF CERT	Military	Not member	Accredited	Not member	Public website not available
Spain	CSIRTCV	Government	Not member	Accredited	Not member	csirtcv.es/
Spain	CSUC-CSIRT	NREN	Not member	Accredited	Not member	cesca.cat/en/c...
Spain	MAPFRE-CCG-CERT	Financial	Not member	Listed	Member	mapfre.com
Spain	AndaluciaCERT	Government	Not member	Listed	Not member	juntadeandaluc...
Spain	CERT-UC3M	NREN	Not member	Listed	Not member	Public website not available
Spain	BBVA CERT	Financial	Not member	Not listed	Member	bbva.com
Spain	PROSEGUR CERT	ISP Customer Base	Not member	Not listed	Member	prosegur.com/...
Spain	CyberSOC-CERT	Service Provider Customer Base	Not member	Not listed	Not member	cybersoc.deloit...

Showing 1 to 18 of 18 entries (filtered from 342 total entries)

Il·lustració 5: Detall dels CSIRT a Espanya (ENISA)

Actualment a Espanya s'ha creat un grup, CSIRT.es (principis de 2018), sota el que s'han integrat els principals equips de resposta a incidents de seguretat del país amb l'objectiu de donar resposta coordinada i efectiva davant de possibles ciberatacs globals. Sota el paraigües de CSIRT.es s'integren tant organismes públics com privats que disposin d'aquests tipus d'equips.

A dia d'avui, formen part del CSIRT.es els següents equips:

- Andalucía CERT
- Caixabank CSIRT
- CCN-CERT
- CERTSI
- CertUC3M
- CESICAT-CERT
- CNPIC
- CSIRT.gal
- CSIRT-CV
- CSIRT GLOBAL TELEFONICA
- CSUC-CSIRT
- esCERT-UPC
- ESP DEF CERT
- eSOC Ingenia
- EULEN-CCSI-CERT
- everis CERT
- Guardia Civil
- InnoTec, Entelgy-CSIRT
- MAPFRE-CCG-CERT
- MNEMO-CERT
- NestleSOC
- Policía Nacional
- PROSEGUR CERT
- RedIRIS
- RENFE CERT
- S2 Grupo CERT
- S21sec CERT
- UCIBER - Mossos d'Esquadra

Il·lustració 6: Equips espanyols agrupats en CSIRT.es

Mundialment, podem obtenir tots els CSIRT/CERT més significatius de les organitzacions més conegudes com TI i FIRST. A continuació, s'ha fet un recopilatori dels més significatius per països per poder-nos fer una idea:

North American

United States - Computer Emergency Readiness Team
United States - Industrial Control System - Cyber Emergency Response Team
CERT Coordination Center at Carnegie Melon University
Canada - Computer Emergency Response Team
Canadian Cyber Incident Response Center (CCIRC)
Mexico - Equipo de Respuesta a Incidentes de Seguridad Informática - UNAM-CERT

Europe

Austria - National Computer Emergency Response Team of Austria
Belgium - Belgian National Computer Emergency Response Team
Denmark - Danish Computer Emergency Response Team
Estonia - CERT
Finland - CERT - Finnish Communications Regulatory Commission
France - Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques
Germany - Computer Emergency Response Team für Bundesbehörden
Hungary - CERT
Lithuania - Lithuanian National Computer Emergency Response Team
Luxembourg - Computer Security Incident Response Team
Luxembourg - Computer Incident Response Centre Luxembourg
Netherlands - Computer Emergency Response Team for the Dutch Government
Norway - Norwegian Computer Emergency Response Team
Poland - Computer Emergency Response Team Polska
Portugal - CERT
Slovenia - Slovenian Computer Emergency Response Team
Spain - Cryptology National Center - Computer Security Incident Response Team
Spain - INTECO IT Incident Response Center
Spain - Spanish National Research Network Computer Emergency Response Team
Sweden - Swedish IT Incident Centre
Switzerland - Swiss Education and Research Network Computer Emergency Response Team
Turkey - Computer Emergency Response Team
Ukraine - Computer Emergency Response Team
United Kingdom - GovCertUK
United Kingdom - Centre for the Protection of National Infrastructure (CPNI)

Pacific

AusCERT - based at University of Queensland
CERT Australia - part of Australian Federal Attorney-General's Department
New Zealand - National Cyber Security Center

South America

Argentina - Computer Emergency Response Team of the Argentine Public Administration
Brazil - Brazilian National Computer Emergency Response Team
Brazil - Computer Security and Incident Response Team - Brazilian Federal Government
Chile - Chilean Computer Emergency Response Team
Columbia - Columbia Computer Emergency Response Team
Uruguay - CERTuy

Middle East

Oman - National Computer Emergency Readiness Team
Qatar - Supreme Council for Information and Communications Technology, ictQATAR
Saudi Arabia - Computer Emergency Response Team
United Arab Emirates - Computer Emergency Response Team

Africa

Kenya -Kenyan National Computer Security Incident Response Team
Mauritius -Mauritian National Computer Security Incident Response Centre
South Africa - South African Computer Security Incident Response Team
Tunisia - Computer Emergency Response Team

Asia

Brunei - Computer Emergency Response Team
Cambodia - National Cambodia Computer Emergency Response Team
China - CNCERT
Hong Kong - Computer Emergency Response Coordination Centre
India - Indian Computer Emergency Response Team
Japan - Computer Emergency Response Team Coordination Center
Japan - National Information Security Center
Malaysia - Malaysian Computer Emergency Response Team
Myanmar - Computer Emergency Response Team
Philippines - Computer Emergency Response Team
Singapore - Computer Emergency Response Team
South Korea - CERT Coordination Center Korea
Sri Lanka - Computer Emergency Response Team
Taiwan - Taiwan National Computer Emergency Response Team
Thailand - Thai Computer Emergency Response Team
Vietnam - Viet Nam CERT

Il·lustració 7: CSIRT més importants mundialment

4.5 Guies per a la creació d'un CSIRT

En la cerca i l'anàlisi de la informació trobada respecte a la creació d'equips de resposta a incidents de seguretat, he trobat molts manuals, recomanacions, exemples pràctics de creació de tipus concrets de CSIRT, etc.

La conclusió és que hi ha nombrosa informació de com crear, gestionar i madurar aquests equips de resposta, però la majoria de la informació trobada sempre fa referencia a certes guies o manuals a seguir. Aquestes guies trobades recurrentment son:

"Creating and Managing Computer Incidents Response Teams" – Del CERT/CC.
"A steps-by-step approach on how to set up a CSIRT" – De ENISA.
"Guia de creació d'un CERT/CSIRT" – Del CCN.

En aquestes tres guies, tenim tots els aspectes importants a tenir en compte en la creació d'un equip de resposta a incidents de seguretat i com operar-lo de la manera més adient.

En la elaboració d'aquest TFM, es faran servir les tres guies per assolir l'objectiu final de fer una proposta de creació i implantació d'un CSIRT a FGC. En tots els punts es farà un anàlisis de les tres guies per tenir en compte els diferents punts de vista (si hi son) i a partir d'aquí es triarà la millor opció. Com a full de ruta, es seguirà l'índex i proposta de la guia ENISA, que és la recomanació de l'agencia europea.

5. Recomanacions per a la creació del CSIRT

5.1 ENISA

En aquesta guia, es descriu el procés de creació d'un equip de resposta a incidents de seguretat informàtica des de tota perspectiva, la gestió empresarial, gestió de processos i el punt de vista tècnic del procés de creació.

A continuació mostrarem l'índex del document que farem servir de guia:

Il·lustració 8: Índex de la guia ENISA

5.2 ENS

Aquesta guia, forma part del desenvolupament del RD 3/2010 del ENS, segons es fa referencia a l'article 37 sobre la prestació de serveis de resposta a incidents a les administracions publiques, i específicament en el punt 2 del programa desenvolupat pel CCN per que es puguin desenvolupar les capacitats de resposta a incidents de seguretat.

Aquesta guia, té com a objectiu ser un instruments eficaç per facilitar la visió global (tecnològiques i no tecnològiques) que comporten la posada en servei d'aquests equips de resposta pel que fa al seu disseny, desenvolupament i posterior posada en funcionament.

En aquest document al que fem referencia, es desenvolupa l'estratègia general, experiència i àmbits d'actuació dels CERT nacionals, així com les normatives, bones pràctiques i legislació aplicable, la formació i informació necessària això com les eines que es poden fer servir.

A continuació mostrarem l'índex amb el contingut que farem servir:

Il·lustració 9: Índex de la guia de l'ENS

5.3 CERT/CC

El CERT Coordination Center (CERT/CC) va ser el primer equip de resposta a incidents de seguretat que es va crear. Va ser creat al novembre de 1988 per l'agencia de defensa DARPA (Defense Advanced Research Projects Agency) a conseqüència del atac del cuc Morris que es va propagar per Internet i va afectar a molts equips.

A posteriori van aparèixer més equips de resposta als Estats Units i Europa. Tots van seguir en un inici les passes i recomanacions del CERT/CC. El CERT/CC va crear una guia per propiciar i facilitar la creació de nous equips de resposta.

Aquesta guia és la "Creating and Managing Computer Security Incident Response Teams", és un referent en la creació i posada en servei d'aquest tipus d'equips. En aquest projecte, tal i com hem comentat la seguirem i consultarem consensuant coneixements amb les altres guies trobades i proposades.

L'índex amb el contingut del document que farem servir és el següent:

Il·lustració 10: Índex de la guia de CERT/CC

6. Catàleg de serveis

6.1 Àrees implicades

El CSIRT que es vol crear, donarà servei a la part corporativa d'oficines. Aquí, s'engloben tots els serveis corporatius de l'empresa i en seran actors importants totes les àrees implicades en donar i mantenir aquests serveis.

Les àrees implicades a les que el CSIRT haurà de donar servei són les següents:

·Departament d'atenció a l'usuari (Atenció Informàtica): Aquest departament és l'encarregar de resoldre les incidències de primer nivell i el tracte directe amb l'usuari. Són responsables de tots els equips d'usuari corporatius (PC's, portàtils, impressores, tabletes, etc.), així com els responsables de les instal·lacions de software i versions d'aquest.

·Departament de sistemes (Tecnologia Informàtica): Aquest departament és l'encarregat de resoldre les incidències de segon nivell (derivades del nivell 1). Són responsables de tots els servidors que mantenen els serveis corporatius, tan de la instal·lació, manteniment i actualitzacions.

·Departament de desenvolupament d'aplicacions: Aquest departament és responsable del desenvolupament a mida d'aplicatius i el manteniment del software creat. Aquest departament esta dividit en tres branques:
Aplicacions de personal (Sistemes de Personal i Producció)
Aplicacions de manteniment (Sistemes de logística i manteniment)
Aplicacions economicofinanceres (Sistemes Economicofinancers)

Com podem veure, aquestes son les principals àrees que hauran d'estar en contacte directe amb el nou CSIRT. Aquest haurà de donar servei a totes elles en el grau adient i exercir de coordinador i referent en qualsevol incident de seguretat informàtic. Les tasques proactives, reactives i de gestió de la qualitat de la seguretat que el CSIRT dugui a terme, seran aplicades sobre aquestes àrees.

Algunes tasques de conscienciació i formació es duran a terme directament sobre l'usuari final, per tal d'aconseguir un aire de cooperació i conscienciació respecte a la seguretat entre tot el personal de l'empresa.

6.2 Actius i serveis importants

El CSIRT creat, tindrà la missió de protegir els actius i serveis importants per a l'empresa de qualsevol incident de seguretat, així com realitzar tasques proactives per mantenir en un bon nivell de seguretat als equips i evitar en la mesura possible alguns dels incidents.

El parc hardware a protegir és bastant divers:

·PC's i portàtils:
Sistemes operatius W7 en endavant
Programari ofimàtic
Programari corporatiu

·Servidors:
Sistemes operatius WS2008 en endavant
Sistemes operatius Linux SUSE
Aplicatius per donar serveis (Correu corporatiu, CRM, Portal del Personal, aplicacions web, etc.)

·Tabletes i mòbils:
Android i Apple
Aplicacions publiques dels markets
Aplicacions fetes a mida

Com podem veure es disposa d'una amplia gama de hardware i versions de sistemes operatius, firmware i actualitzacions de programari. Aquesta diversitat ofereix un ampli ventall de possibles vulnerabilitats que hauran de ser estudiades, catalogades i avisades per ser solucionades.

Pel que fa als serveis crítics, FGC ha elaborat i definit un catàleg de serveis amb un pla de contingència, el qual es farà arribar al nou equip de resposta d'incidents de seguretat per tal d'avaluar-lo i analitzar-lo per poder-lo fer servir i definir i modelar segons convingui els serveis que oferirà el nou CSIRT.

7. DAFO

El DAFO, és una metodologia d'estudi de la situació d'una empresa o projecte, en la qual s'analitzen les seves característiques internes (Fortaleses i Debilitats) i les externes (Oportunitats i Amenaces). D'aquesta manera podem considerar tots els factors que poden ajudar a la implantació del CSIRT i les seves problemàtiques, cosa que ens permetrà prendre decisions sobre la seva creació i podrem donar una justificació a la decisió que s'ha de prendre de definir els serveis mínims amb que arrencarà l'equip entre d'altres.
Amb el DAFO següent, ens farem una idea de la situació real en que ens trobem de cara a dur a terme la creació de l'equip de resposta y ens permetrà prendre decisions i justificar-les de cara a establir una estratègia de futur.

En les Fortaleses, es descriuen els recursos i habilitats que té l'empresa per porta a terme la realització de la creació i implantació del CSIRT.

A les Debilitats, es destaques quins factors interns, de l'empresa, poden fer perillar la implantació i èxit del projecte de creació i implantació del CSIRT.

Pel que fa a les Oportunitats, aquí en destaquem de cara a l'exterior de la empresa que es pot aconseguir i quines avantatges o resultats positius obtindríem de l'èxit de la implantació del nostre projecte de creació del CSIRT.

Finalment, sobre les amenaces es descriuen els factors que poden fer que el projecte finalment fracassi. Son aquelles que si s'identifiquen i es tracten de manera adient es poden reconduir a oportunitats, sinó poden fer fracassar tot el projecte.

A continuació es mostra el DAFO:

Fortaleses	Debilitats
·FGC és molt conscient de la importància de la seguretat de la informació ·Pot facilitar el compliment de les normatives i auditories necessàries per a les empreses públiques. FGC ja les compleix. ·S'està duent a terme un Pla de Mobilitat a l'empresa que facilitarà als empleats poder treballar en qualsevol lloc. Això implica controlar possibles incidents de la seguretat de la informació empresarial a la que s'accedirà. ·Usuaris familiaritzats amb les tecnologies i conscienciats en la importància de la seguretat (tot i no tenir amplis coneixements) ·Molt bons resultats i qualificacions en els resultats de les auditories de seguretat que FGC esta obligada a passar. Un equip de resposta a incidents de seguretat intern millora la percepció de la seguretat a nivell empresarial. ·Interès, col·laboració i predisposició per part de la direcció en la creació del CSIRT i la gestió d'incidents de seguretat.	·Poc coneixement sobre seguretat del personal de FGC. ·Manca de formació especifica en seguretat de tot l'equip a crear. ·Disponibilitat insuficient de personal en l'equip per assolir les totes tasques de seguretat. ·Resistència al canvi o a l'aplicació de nous processos de seguretat en els procediments habituals d'algunes àrees o usuaris. ·Reorganitzar i restablir polítiques d'ús d'equips i serveis per millorar seguretat. ·Gran nombre de dispositius i molta varietat per poder tenir un control exhaustiu a priori. ·Dificultats per mantenir SO i SW a nivells d'actualitzacions segurs.

·Coneixement del possible impacte econòmic i d'imatge que podria suposar no gestionar adequadament un incident de seguretat greu. ·Tan els treballadors i directius com des de l'exterior es té una imatge de que FGC sempre busca la millora i excel·lència, cosa que es busca igualment en temes de seguretat de la informació.	
Oportunitats	**Amenaces**
·Coordinació enfront incidents de seguretat. ·Protocols de detecció, contingència i resolució d'incidents. ·Resposta, resolució i recuperació ràpida, davant incidents de seguretat. ·Millorar la resiliència en general davant d'incidents. ·Formar i educar sobre seguretat de la informació a tota l'empresa. Cosa que permetrà reduir notablement el nombre d'incidents de seguretat. ·Crear eines que ajudin a millorar la seguretat en els diferents entorns, àrees i departaments de FGC ·Ser un referent com a empresa publica en quant a la seguretat de la informació. ·Tenir un pla de seguretat per a tota l'empresa i poder garantir la seva aplicació i bon funcionament ·Assolir l'excel·lència en quant a seguretat de la informació, amb aplicacions continues de bones pràctiques i comportaments de seguretat en tots el àmbit de l'empresa. Millora la imatge de l'empresa i l'entorn TIC.	·El baix coneixement sobre seguretat, pot provocar una negativa per part dels usuaris. ·Reticència al canvi i l'aplicació de nous processos i protocols de seguretat per part d'algunes àrees o usuaris. ·Disposar de personal insuficient, poc qualificat o poc format. ·Crear-se moltes expectatives en les activitats a desenvolupar, en comptes de realitzar una bona planificació. ·No fer cas a recomanacions, avisos o comunicats.

Anàlisi Intern:

En aquest anàlisi, es tenen en compte les *Fortaleses* i *Debilitats* que s'han identificat que té l'empresa envers el projecte de creació del CSIRT. Com hem vist al quadre, per una banda s'ha identificat en que es destaca i que pot facilitar la creació del CSIRT, mentre que per l'altra s'han identificat motius i situacions de l'empresa que poden donar problemes a l'hora de dur a bon terme el projecte y que s'haurien de millorar.

Com podem veure, es té el l'interès per part de la direcció de donar suport al projecte, ja que s'és molt conscient de la importància de la seguretat de la informació i del que podria comportar una gestió d'incidents de seguretat desafortunada. En base a l'experiència de l'empresa en el compliment de les normatives i les revisions d'auditories periòdiques que s'han de passar, hi ha una bona base de coneixements per posar en marxa un CSIRT que coordini i millori en l'àmbit general, la seguretat de les dades i més concretament, doni resposta als incidents de seguretat.

Altre punt important a destacar és la predisposició de l'empresa a apostar per la implantació de tecnologia (Pla de Mobilitat) en tots els àmbits i la predisposició dels usuaris a fer-la servir i millorar els procediments i feines del dia a dia.

Per contraposició a les fortaleses que té l'empresa envers al projecte de creació del CSIRT, ens trobem com a mancances, que tot i l'interès general per la tecnologia, tenim poca formació i coneixements sobre la seguretat per part dels treballadors. Això pot oferir certa resistència al bon evolutiu del projecte ja que implicarà canvis en el dia a dia i els procediments de les àrees implicades i els usuaris. També s'ha de destacar que no hi ha definits procediments i polítiques de seguretat especifiques aplicades a cada àrea o usuari segons convingui i que s'haurà de definir i consensuar.

Un altre punt important destacat és la limitació de recursos de personal per assumir tota la carrega de noves feines que s'hauran de dur a terme, cosa que es pot veure afectada per l'ampli parc de dispositius i el manteniment de versions de SO i aplicatius. Finalment s'ha de tenir en compte que un de les principals debilitats que podem trobar en aquest projecte podria ser que la formació tècnica en seguretat de tots els integrants de l'equip no fos suficient, tot i que gran part d'aquest si que estaria a l'alçada en coneixements.

Anàlisi Extern:

En aquest sentit, no estem parlant d'un àmbit completament extern a l'empresa, ja que el projecte es totalment intern. Però el que s'analitza aquí, serà quines *Oportunitats* i *Amenaces* podem trobar de cara a la implantació del CSIRT i la visió que les àrees i els usuaris de l'empresa en tindran i que poden fer que fracassi el projecte o que s'aconsegueixin les oportunitats presentades i sigui un èxit.

Les oportunitats que es presenten, són clarament part dels beneficis i serveis que pot aportar la creació de l'equip. El que es planteja com a oportunitat és millorar la detecció, la gestió, les actuacions i la recuperació davant d'incidents de seguretat. Per altra banda es planteja com a una oportunitat mantenir al personal de l'empresa informat i al dia sobre la seguretat de la informació tenint com a objectiu millorar la seguretat general de l'empresa i porta-la a nivells d'excel·lència. També es presenta com a oportunitat poder desenvolupar eines a mida que millorin els processos interns i tasques dels usuaris, a nivell de seguretat.

Per contra d'aquestes oportunitats, existeixen certes amenaces que poden fer que no avanci el projecte d'implantació del CSIRT o que el dificulti molt, per això s'han de tenir molt en compte i intentar identificar-les e intentar reconvertir-les en opcions o oportunitats pel projecte. Principalment com amenaça identifiquem que el baix coneixement de la seguretat de les dades i les implicacions que pot tenir per part dels usuaris, pugui desenvolupar en una negativa a assolir els canvis necessaris i adients, com poden ser nous procediments i protocols, i això provoqui un problema. La manca de recursos humans en la formació de l'equip i la justa preparació o coneixements en la seguretat de les dades, pot comportar que no s'assoleixin tots els objectius o no amb la planificació adequada. També s'ha identificat com un possible problema o amenaça, la creació d'unes expectatives massa altes o no alineades amb el projecte pot fer que hi hagi una sensació de descontent i fracàs, que por complicar el bon avenç de la instauració del CSIRT i el seu normal funcionament.

Finalment, no seguir les recomanacions, avisos, informes, etc., que marquen el funcionament i l'evolució envers la seguretat de l'empresa donats pel CSIRT, pot comportar que les tasques i serveis definit per aquest, no es puguin dur a terme i no siguin suficients per evitar o respondre els incidents de seguretat, amb el conseqüent fracàs pel projecte.

Fet aquest anàlisi, hem vist els punts forts i virtuts per la implantació del nou CSIRT i els inconvenients i punts crítics que poden trobar. Aquets anàlisi ens dona una visió de la situació del projecte i ens permetrà prendre decisions i definir els serveis que CSIRT_FGC oferirà perquè els usuaris assoleixin i adaptin el seu dia a dia i s'aliïn amb la seguretat de la informació.

8. Organització del CSIRT

Definir l'estructura organitzativa adequada d'un CSIRT, depèn directament de l'estructura de l'organització a la qual depèn i al grup de clients atesos. També és molt important a tenir en compte els recursos de que disposarà l'equip per planificar i definir aquesta estructura organitzativa.

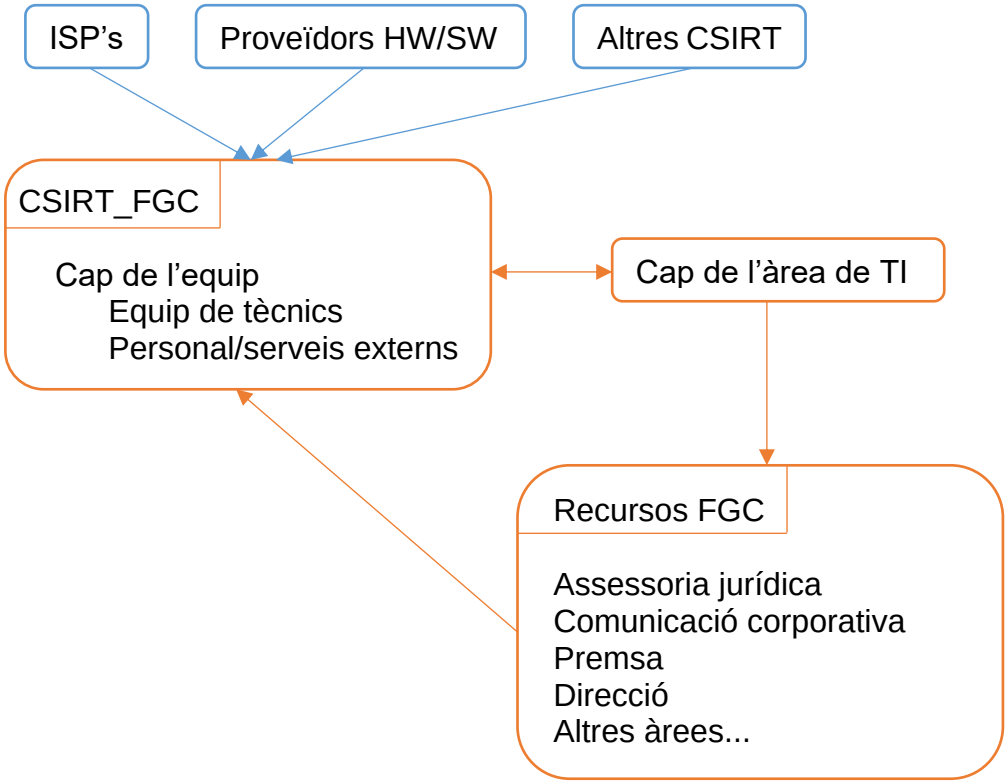
És important tenir en compte si es disposa d'assessorament legal per no tenir cap problema afegit durant la implantació.

En el cas d'aquest TFM, el CSIRT que es vol crear és a dintre d'una organització existent (FGC) i es vol crear a dintre del departament de TI ja existent i que fa actualment les tasques de seguretat. El plantejament de l'equip que es vol crear dependrà directament del Cap de l'àrea de TI i es definirà un Cap de l'equip que serà responsable de les activitats de l'equip i que tindrà un equip de tècnics assignats i possibilitat de contractar suport extern.

Aquest model permet adaptar-se a les situacions excepcionals que puguin sorgir ja que l'equip té un mínim de personal assignat, però pot créixer en moments donats contractant suport extern sempre sota la seva supervisió directa.

Aquest model, s'adapta perfectament al funcionament de FGC i en possibilita en un futur estendre aquests serveis a les seus de remotes de muntanya que formen part de l'empresa. La idea seria muntar equips satèl·lits que depenguin directament del CSIRT_FGC i del seus recursos, però que tinguin certa autonomia per oferir els serveis concrets i limitats necessaris en les seus remotes de l'empresa.

L'esquema organitzatiu que es faria servir en aquest cas seria el següent:



Il·lustració 11: Organització del CSIRT_FGC

Un cop definit el model organitzatiu que seguirà el nou CSIRT, farem una proposta dels serveis que haurà de donar. Tot i que en un inici es donaran els serveis considerats mínims i justificat segons una matriu DAFO per tal d'iniciar el funcionament amb unes mínimes garanties d'èxit.

Aquests serveis, en funció de les necessitats reals del grup a qui es donarà servei haurien de ser:

- Serveis reactius:
  - Avisos i alertes de seguretat
  - Anàlisi d'incidents
  - Tractament d'incidents
  - Resposta a incidents
  - Coordinació de resposta a incidents
- Serveis proactius:
  - Comunicats
  - Monitorització, detecció i prevenció d'intrusions
  - Desenvolupament d'eines de seguretat
- Serveis de gestió de la qualitat de la seguretat:
  - Conscienciació i sensibilització
  - Educació/Formació

D'altra banda, organitzativament, és important establir els canals de comunicació que el CSIRT_FGC farà servir per comunicar-se i que tenen com a objectiu facilitar el tractament d'incidents de seguretat (alta d'incidents, rebre informes d'incidents, coordinar-se amb altres CSIRT, donar suport, comunicar-se amb el seu grup atès, etc.). A més es publicarà també al seu lloc web i llistes de correu, tots els avisos e informació sobre seguretat.

Els canals de comunicació inicialment definits seran:

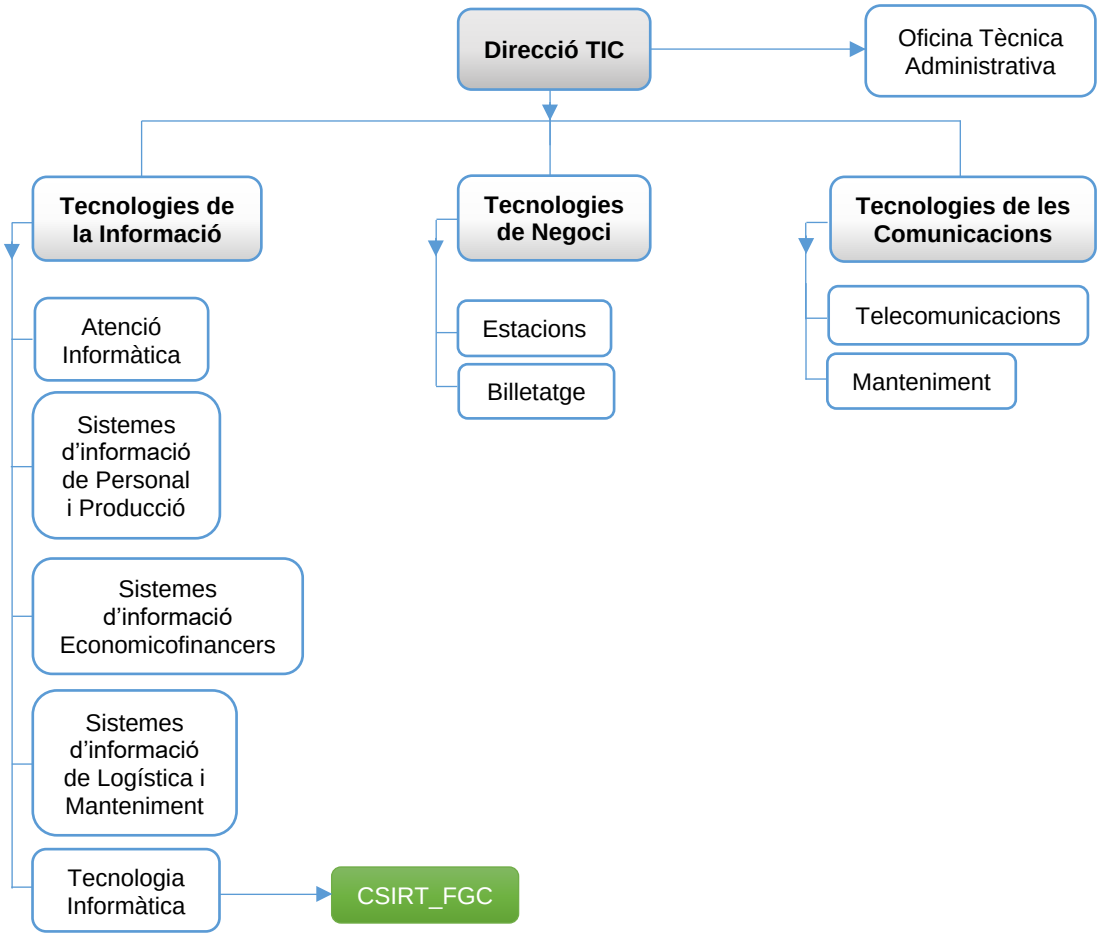
- Lloc web
- Lloc web privat (membres, administrador i personal autoritzat)
- Llistes de correu
- Correu personalitzat
- Telèfon
- Informes periòdics
- Eina de ticketing

8.1 Impacte sobre l'estructura actual

El CSIRT que es vol crear en un inici donarà servei a l'àrea TIC de Informàtica Corporativa, que engloba els serveis corporatius de l'empresa (Correu, ERP, Aplicacions, Atenció a l'usuari, Web Corporativa, Portal del Personal, etc.). Aquesta àrea, dona servei als treballadors dels edificis corporatius així com a les seus remotes.

Hem de tenir en compte que FGC té com a àrea de negoci principal els trens, però disposa d'estacions d'esquí (La Molina, Vallter, Portainé i Espot) a més d'activitats turístiques i hotels entre d'altres. Tot el seu àmbit de negoci esta estès en un ampli territori cosa que comporta en alguns casos centralitzar certs serveis i descentralitzar d'altres. En el cas dels serveis corporatius la majoria estan administrats de manera central des de l'àrea d' Informàtica Corporativa.

L'esquema gràfic del departament TIC amb el nou CSIRT és el següent:



Il·lustració 12: Organigrama TIC amb CSIRT_FGC

Tal i com podem observar en la figura anterior el nou CSIRT es crearà sota l'àrea de Tecnologia Informàtica (Administració de Sistemes) i donarà servei a la resta d'àrees que pertanyen a Informàtica Corporativa. A nivell organitzatiu l'impacte serà petit ja que l'equip es crea depenent d'una subàrea a dintre de l'àrea TIC, però funcional i operativament l'impacte és elevat. El fet de que el CSIRT doni servei a les subàrees corporatives, implica que la majoria d'incidents que repercuteixen en els treballadors d'oficines de l'empresa estaran sota la supervisió, l'assessorament i la coordinació del nou CSIRT. Tots els sistemes corporatius (servidors, webs, hosting, etc.), aplicacions corporatives, equips mòbils (portàtils, tabletes i telèfons), equips de sobre taula, software comercial, etc. quedarà sota la supervisió i l'assessorament del nou CSIRT, que entre altres funcions, vetllarà pel seu bon funcionament, actualitzacions, revisions de versió, etc.

Com podem veure, l'impacte sobre la gestió d'incidents de seguretat, la protecció i conscienciació sobre la seguretat que pot aportar el nou CSIRT_FGC és molt gran.

Un cop establert el CSIRT_FGC, amb un parell d'anys de funcionament i rodatge, que permetin el creixement de l'equip, que s'hagi assolit un cert grau de formació de tot l'equip, hi hagi una maduresa i experiència notable en la gestió d'incidents de seguretat, etc., es plantejaria un canvi organitzatiu que permetés un escalat estructural de CSIRT que li dones transversalitat i pogués oferir serveis a les demes àrees de l'empresa.

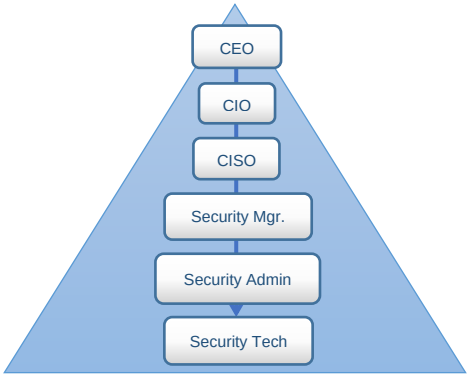
Assolit aquest grau de maduresa del CSIRT, la idea seria conformar un "Àrea de Seguretat de la Informació" que estaria al mateix nivell funcional que la resta d'àrees TIC i amb independència total, cosa que així aconseguiríem independència total entre la funcionalitat i la seguretat de tots els sistemes d'informació de l'empresa. D'aquesta manera tots els sistemes d'informació de FGC estarien gestionat i protegits per un àrea i equip especialitzats i amb total independència. És en aquest moment en que la nova àrea creada pren una visió transversal a totes les àrees de l'empresa i juntament amb el nou equip CSIRT_FGC podria assumir la gestió de la seguretat i incidents de tot FGC.

Aquesta estructura que es planteja com a evolutiu a curt termini de la implantació del CSIRT, comportaria un impacte sobre l'estructura organitzativa que hi ha actualment a FGC. La creació d'aquesta nova àrea ens permetria la creació de la figura de CISO, i permetria la independència total de les tasques del CIO respecte a la seguretat de la informació. D'aquesta manera es podrà desvincular la funcionalitat de la seguretat i estarà alineada la missió de l'empresa amb la tecnologia de la informació i la seguretat de les dades.

- *CISO* (Chief Information Security Officer): és el director de la seguretat de la informació, té la missió d'alinear la seguretat de la informació amb els objectius de negoci de l'organització.

- *CIO* (Chief Information Officer): és el director de tecnologies de la informació, té la missió d'encarregar-se de que les estratègies de l'organització estiguin alineades amb la tecnologia de la informació per assolir el objectius planificats.

L'estructura organitzativa final que s'aconseguirà serà la següent:



Il·lustració 13: Organigrama empresarial a assolir amb CSIRT_FGC

8.2 Interacció amb l'equip

En aquest apartat es definiran i es detallaran els diferents canals de comunicació oficials que les àrees implicades i usuaris de l'empresa hauran de fer servir per reportar incidents de seguretat, consultes, etc. i comunicar-se amb el CSIRT_FGC.

Els diferents departaments de l'empresa, així com els usuaris que poden interactuar amb el CSIRT_FGC, ambdós, ho faran seguint els mateixos canals i procediments que s'establiran a continuació. S'ha de tenir en compte, que segons la circumstancia, El CSIRT_FGC pot redefinir o autoritzar temporalment altres canals segons convingui.

Per interactuar amb CSIRT_FGC, s'han definit dos tipus de canals que permeten la interacció i obtenció d'informació serveis de diverses maneres i estableixen una política d'ús per obtenir els diferents serveis que s'oferiran.

CANALS PASIUS (no requereixen resposta directe als usuaris):

·**Llista de distribució**: A partir d'una llista de distribució amb tots els usuaris de l'empresa (en un inici els usuaris d'oficines i serveis corporatius), el CSIRT_FGC farà arribar als usuaris per una banda:

Informes mensuals periòdics: es generarà un informe cada mes amb l'estat de la seguretat, reports d'incidents, comunicats i informació interesant, etc.

Comunicats puntuals: també es farà servir aquesta llista per avisar o infirmar sobre incidents puntuals o donar informació preventiva i formativa als usuaris quan es cregui adient.

·**Portal del Personal**: Aquest portal, és una eina corporativa interna en la que cada àrea te el seu espai. El CSIRT_FGC, disposarà de dos espais, un de públic en que es crearà un blog amb informació interessant sobre seguretat, informació sobre incidents de seguretat, consells i bones pràctiques de seguretat, etc. Qualsevol usuari de l'empresa podrà consultar aquesta informació i estar al dia de tota la informació de seguretat proporcionada.

Per altra banda, es disposarà també d'un entorn privat (només per administradors i personal vinculat a l'equip) en el que es publicarà tota la informació tècnica d'incidents, documentació tècnica, cursos, etc. Aquest serà l'espai on els components del CSIRT_FGC podran gestionar i compartir amb tot l'equip tota la informació més sensible.

CANALS ACTIUS (requereixen resposta en curt període de temps cap a l'usuari):

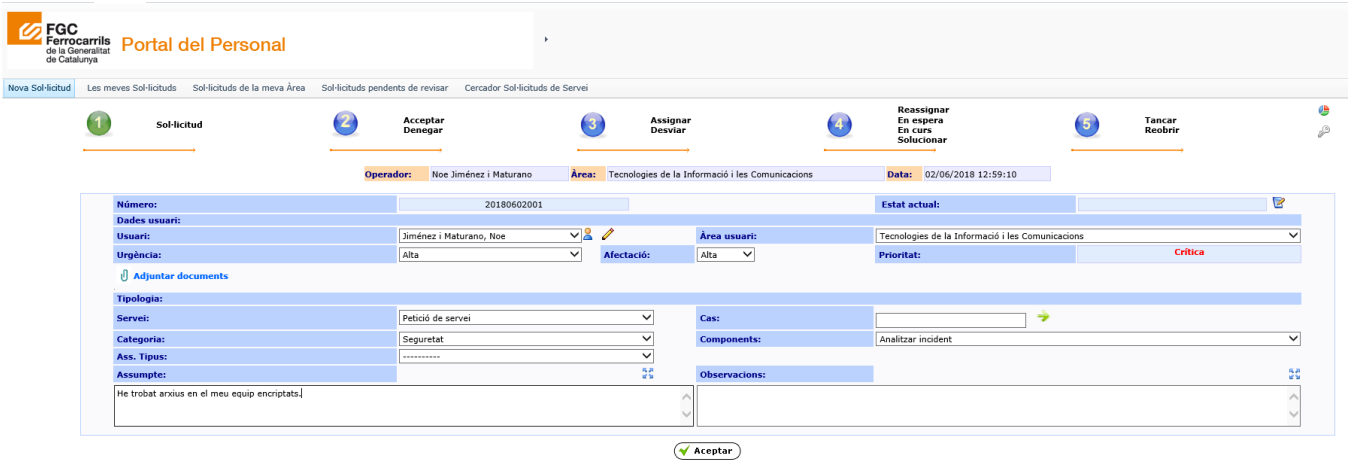
·**Eina de ticketing**: FGC té una eina interna de peticions i sol·licituds de servei que tots els usuaris poden fer servir per interactuar amb les diferents àrees de l'empresa. CSIRT_FGC, es donarà d'alta a aquesta eina i la defineix com el mitjà oficia per reportat incidents de seguretat, consultes o qualsevol interacció que es vulgui tenir amb l'equip.

Aquesta eina permet a l'usuari establir la prioritat en funció de la *Urgència* i l'*Afectació* (tot i que serà gestionada i modificada en cas necessari segons els criteris de CSIRT_FGC). A més permet la recollida recopilació d'informació bàsica i documents necessaris per tenir tota la informació necessària perquè el CSIRT pugui començar a tractar l'incident.

Amb aquesta eina s'estableixen diferent workflows de comunicació entre usuari-CSIRT, primer perquè en obrir incidència s'envia un mail al CSIRT i en tractar-la i resoldre-la es comunica a l'usuari. En segon lloc, s'estableix un punt (la incidència creada) on es recull tota la informació sobre l'incident i els procediments que s'estan duent a terme per a la seva resolució, que en tot moment pot consultar l'usuari.

Tots els usuaris poden accedir al Portal del Personal i consultar l'estat, modificacions, documentació o informació que s'està desenvolupant durant el procés de resolució de l'incident o tractament de la petició, tal com hem explicat.

A continuació mostrarem un exemple de la creació mitjançant l'eina de ticketing d'una petició o incident de seguretat:

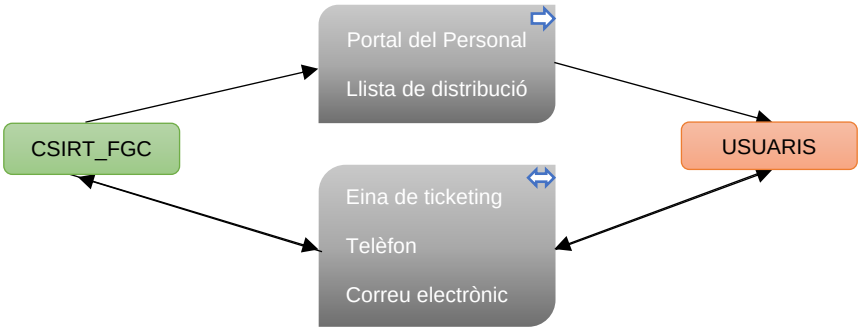


Il·lustració 14: Eina de ticketing del CSIRT_FGC

·**Telèfon**: L'equip disposarà d'un telèfon propi en el que es podrà establir contacte directe. Aquest telèfon es pot fer servir dintre del horari de servei definit, per informar només sobre incidents de seguretat. La persona que reporta per telèfon un incident haurà de crear la corresponent petició en l'eina de ticketing.

·**Correu electrònic**: L'equip disposa d'una adreça de correu (que és una llista de distribució cap a tots els membres de l'equip) on es pot establir contacte per fer consultes, peticions, reportar incidents, etc. De totes maneres no és el mitjà definit amb més urgència tot i que es donarà resposta. Igualment, si es reporta un incident per correu s'haurà d'haver complimentat correctament l'alta del tiquet corresponent en l'eina de ticketing.

Esquemàticament podem veure dos maneres d'interaccionar amb el CSIRT_FGC, la primera és obtenint informació per part de l'usuari a través del blog al portal o la llista de distribució on es poden mantenir al dia i estar alineats amb la seguretat. En segon lloc, com podem veure es pot interactuar amb el CSIRT_FGC informant i esperant resposta d'aquest, per tal de resoldre, informar o conscienciar sobre incidents de seguretat.



Il·lustració 15: Esquema de la interacció USUARIS - CSIRT_FGC

8.3 Serveis oferts

Durant aquest PFM, s'ha analitzat i comentat quins serien els serveis desitjats que es voldria que el CSIRT_FGC oferís. Tal i com també s'ha comentat, és important definir un catàleg de serveis d'acord amb la necessitat del grup d'usuaris a qui es donarà servei. Després d'haver analitzat els pros i contres i el grup a qui s'oferiran serveis mitjançant el anàlisi DAFO, en aquest apartat definirem i explicarem quins son els serveis inicials mínims amb que es posarà en marxa el CSIRT_FGC.

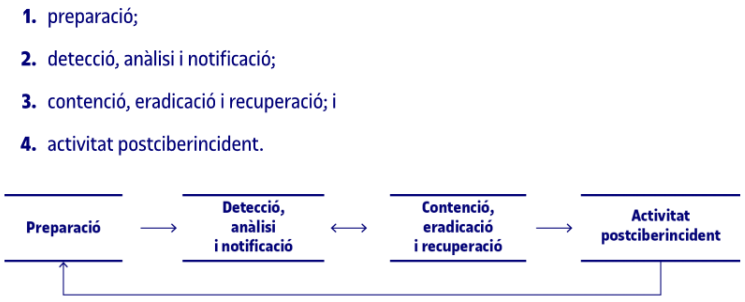
Es molt normal que els equips de resposta facin la seva posada en marxa oferint uns mínims serveis i que a mida que es va afermant el seu funcionament, es va prenen maduresa i experiència en el tractament d'incidents de seguretat, es plantegin la posada en marxa de nous serveis que complementin i millorin les tasques del CSIRT.

En aquest sentit, la definició de serveis mínims inicialment que oferirà el CSIRT_FGC és la següent:

- Serveis reactius:
  - Avisos i alertes de seguretat
  - Anàlisi d'incidents
  - Tractament d'incidents
  - Resposta a incidents
  - Coordinació de resposta a incidents
- Serveis proactius:
  - Comunicats
  - Monitorització, detecció i prevenció d'intrusions
- Serveis de gestió de la qualitat de la seguretat:
  - Conscienciació i sensibilització

Com podem observar, els serveis reactius són els propis de la resposta a incidents de seguretat que ha d'oferir un CSIRT. Aquests serveis oferts, ens permeten assolir la gestió de ciberincidents en totes les seves fases i a més permet que el CSIRT_FGC exerceixi de punt central en quant a seguretat i oferint la gestió centralitzada i la coordinació de la resposta a incidents de seguretat a tota l'empresa.

L'esquema de la gestió de ciberincidents que s'assoleix amb els serveis reactius que ofereix el CSIRT_FGC és la següent:



Il·lustració 16: Esquema de Gestió de Ciberincidents
Font: Apunts UOC/CCN-CERT

Tenint en compte l'anàlisi DAFO, hem vist que hi ha un especial interès i predisposició per part de l'empresa i els treballadors en la gestió de la seguretat i els incidents que puguin sorgir al seu voltant. La gestió de seguretat, les normatives i les auditories que es passen actualment avalen un interès per millorar i centralitzar tots els incidents de seguretat, així com poder ser capaços de detectar-los, analitzar-los, contenir-los i recuperar-los. Per altra banda, hem vist que hi ha l'oportunitat de millorar la coordinació dels incidents de seguretat a nivell de tota l'empresa així com millorar els procediments i polítiques que tenen a veure amb la seguretat i afecten als processos de negoci de totes les àrees. Aquests motius han fet que en l'inici del CSIRT_FGC, aquests serveis que

hem comentat fossin indispensables, ja que tota l'empresa es veurà beneficiada d'aquests serveis ja que com en l'arrencada el CSIRT donarà serveis a la part d'oficines corporativa, és una afectació molt gran en quant a volum d'usuaris.

És important destacar el servei *d'Avisos i alertes de seguretat*, que tot i formar part del procés de la gestió i actuació davant d'incidents de seguretat, tindrà la funció d'alertar al usuaris sobre qualsevol possible bug de seguretat, una configuració dolenta dels equips, etc. que els afecti, tot i que no s'hagi produït encara un incident de seguretat. El CSIRT, en base a les configuracions, equips, software i hardware inventariat a l'empresa alertarà del possibles problemes de seguretat que puguin haver per tal de posar solució de seguretat.

Com hem vist també s'ofereixen serveis proactius, en aquest sentit s'ofereix el servei de realitzar comunicats de manera periòdica, informant, alertant i donant a conèixer l'estat de seguretat en que ens trobem. És molt important oferir aquests serveis, ja que poden prevenir nombrosos incidents de seguretat. Molts dels incidents que sorgeixen en referencia a la seguretat son deguts a desinformació o mala configuració per part dels usuaris perquè ni tan sols eren conscients de que ho estaven fent malament.

Per altra banda, el CSIRT_FGC, aprofitant els mecanismes de monitorització existents en àrees de l'empresa (Tecnologies de la Informació i Tecnologies de les Comunicacions, entre altres), oferirà el serveis de monitorització i anàlisi dels sistemes i la xarxa per intentar establir patrons i detectar usos anòmals per tal de prevenir intrusions i incidents de seguretat.

Fent referencia al DAFO, amb aquest serveis intentem pal·liar les debilitats i amenaces que s'identificaven del fet que el personal no tenia prou coneixement sobre seguretat. Mantenint informat sobre diversos temes de seguretat i temes d'interès pels usuaris i les seves àrees en quan a maneres d'actuar i prevenir possibles incidents de seguretat aconseguim reconduir aquests aspectes negatius identificats al DAFO. Per aquest motiu aquests serveis son imprescindibles en l'inici del CSIRT_FGC. Pel que fa a la monitorització crec que és un servei molt important per tal de poder estar al dia de l'estat i ús de les infraestructures a les que dona servei el CSIRT i a més ens afavoreix el control i la identificació i creació de mesures preventives.

Finalment, comentar que el CSIRT_FGC oferirà també serveis de gestió de la qualitat de la seguretat, concretament oferirà serveis de conscienciació i sensibilització envers la seguretat de la informació. Amb aquest servei, es pretén iniciar campanyes d'informació, ensenyar casos reals, posar exemples reals del que pot succeir en un incident de seguretat, ensenyar possibles vectors d'atac i atacs controlats, etc., per tal de sensibilitzar i conscienciar al usuaris del CSIRT de la importància de la seguretat, tant pel propi usuari, com per a l'empresa. S'iniciaran campanyes, xerrades i grups de treball amb temàtiques diverses per a tot el personal interessat i s'intentarà premiar i incentivar l'interès i la participació.

Amb aquest servei s'intentarà donar a conèixer el món de la seguretat informàtica a tots els usuaris de l'empresa. Sense ser un programa de formació tècnica i exhaustiva, s'intentarà donar a conèixer certs aspectes tècnics importants i sobretot ensenyar best practices als usuaris per tal que es garanteixi a la llarga un bon ús dels recursos empresarials des de l'àmbit de la seguretat.

Tenint en compte l'anàlisi DAFO, amb oferint de manera inicial aquest servei en la implantació del CSIRT, focalitzem i canalitzem de manera adient la reticència que ens podem trobar a la implantació de canvis per la seguretat deguts al desconeixement i poca formació del personal al que el CSIRT donarà serveis.

Aquest serveis comentats, son els mínims i imprescindibles amb els que el CSIRT_FGC es posarà en marxa. Amb aquests, s'ofereixen els serveis imprescindibles per garantir una bona gestió dels incidents de seguretat i a més es forma i es prepara als usuaris als que donem servei per assumir i entendre els canvis que s'han de dur a terme per assolir nivells de seguretat de la informació en tots els processos de negoci de l'empresa.

Aquests serveis definits inicialment facilitaran la implantació i arrencada del CSIRT i garantiran que un cop aquest equip vagi madurant es puguin implantar serveis més avançats i complexes sobre la seguretat en l'empresa assumint que els usuaris hauran madurat en quant a coneixements i actitud envers la seguretat informàtica gràcies als serveis inicials implantats.

9. RFC-2350

En aquest apartat definirem la RFC que detalla el CSIRT en tots els àmbits i en defineix els serveis que ofereix. L'idioma en que s'escriurà tot i ser un CSIRT intern que prestarà servei de manera local a dintre de l'estat espanyol, serà en anglès. Això es decideix fer així per facilitar el contacte i la interacció amb altres CSIRT de l'àmbit nacional, europeu o mundial si escaigués.

Pel que fa a les comunicacions i a la difusió de dades, tot i que es definirà a la RFC, destacar que es farà de la manera segura fent servir signatura digital i dades encriptades fent servir GPG (derivat lliure de PGP).

RFC-2350

1. About this document

1.1. Date of last Update

This is version 1.0, not published yet.

1.2. Distribution list for notifications

Currently CSIRT_FGC does not use any distribution lists to notify about changes in this document.

1.3. Locations where this document may be found

The current version of this document can always be found at http://csirt.fgc.cat.

1.4 Authenticating this Document

This document has been signed with the CSIRT_FGC GPG key. The signature is also on our web site, under: http://csirt.fgc.cat/claus/.

1.5 Document Identification

Title: "RFC 2350 CSIRT_FGC "
Version: 1.0
Document Date: June 2018
Expiration: This document is valid until superseded by a later version

2. Contact information

2.1. Name of the team

CSIRT_FGC: Equip de resposta a incidents de FGC.

2.2. Address

CSIRT_FGC: Equip de resposta a incidents de FGC.
C/ Vergós, 44
08017 Barcelona

2.3. Time zone

Central European Time (GMT+0100, Brussels, Copenhagen, Madrid, Paris)

2.4. Telephone number

+34 934817272

2.5. Facsimile number

None available.

2.6. Electronic mail address

All incidents reports should be sent to csirt_fgc@fgc.cat

2.7. Other telecommunication

None available.

2.8. Public keys and encryption information

GPG is used for functional exchanges between CSIRT_FGC and its Partners
CSIRT_FGC has:

KeyID is 0x5EAAFA81
Fingerprint is: AEE7 7D8E 172B FA9C AF77 B17A A2F2 23EB 5EDA FA81
The public key and its signatures can be found at:
GPG Public Keyservers
CSIRT_FGC's web site: http://csirt.fgc.cat/claus/gpg-publiques

2.9. Team members

The CSIRT_FGC team leader is Noé Jiménez. The team is made up of IT security experts and system administrators.

2.10. Other information

Any other information about CSIRT_FGC, can be found at http://csirt.fgc.cat.

2.11. Points of customer contact

The preferred method to external contact CSIRT_FGC team is to send an e-mail to the address csitr_fgc@fgc.cat which is monitored by a duty officer during hours of operation. We encourage our constituency to use GPG encryption when sending any sensitive information

The preferred method to internal contact CSIRT_FGC team is by corporative incident tool (Available on Enterprise Personnel Portal).

Urgent cases can be reported by phone on +34 934817272

Days/Hours of Operation: 07:30 to 15:00 Monday to Friday. Out of office hours' operation in case of emergency.

3. Charter

3.1. Mission statement

Mission CSIRT_FGC aims to prevent, detect, respond and recover the security incidents that affect Ferrocarrils de la Generalitat de Catalunya, as well as the coordination of incidents all empresarial areas and with others CSIRT if its necessari. It is also important for CSIRT_FGC, that proactive measures are in constant development, involving timely warning of possible problems, technical advice and the development of security tools.

3.2. Constituency

CSIRT_FGC offers full service to all departments related with corporative services of FGC.

3.3. Sponsorship and/or Affiliation

CSIRT_FGC is sponsored by the IT Director and by the Corporate Computing Responsible.

3.4. Authority

CSIRT_FGC operates under the auspices of, and with authority delegated by the IT Director and by the Corporate Computing Responsible. Has the authority to take the measures it deems appropriate to properly handle a computer security related incident in all departments from FGC.

4. Policies

4.1. Types of incidents and level of support

CSIRT_FGC is authorized to address all types of computer security incidents which occur, or threaten to occur, in the FGC network.

CSIRT_FGC may act upon request of one of FGC' workers, or may act if a member is in risc, or threatens to be, involved in a computer security incident.

The level of support given by CSIRT_FGC to all incidents are NORMAL. May vary if is explicitly labelled URGENT, CRITICAL. May vary after a first analysis too by CSIRT_FGC. Incidents will be prioritized according to their apparent severity and extent.

End users are expected to contact the CSIRT_FGC by the incidents tool for assistance. In exceptional case can be by direct phone or by presence.

4.2. Co-operation, interaction and disclosure of information

CSIRT_FGC exchanges all necessary information with other CSIRTs as well as with affected parties' administrators. Personal data are protected by LOPD and is no exchanged unless explicitly authorized. All sensible data are encrypted if they must be transmitted over unsecured environment as stated in 4.3 of this document.

4.3. Communication and authentication

CSIRT_FGC protects sensitive information in accordance with relevant regulations and policies within the Spanish and EU.

Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes

Telephones will be considered sufficiently secure to be used even unencrypted, in view of the type of information threated.

Smartphones apps for communications will not be considered secure and could not be used to communicate with CSIRT_FGC.

All communication security (encryption and authentication) is achieved by GPG.

5. Services

5.1. Incident response

CSIRT_FGC will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incidents management:

5.1.1. Incident triage

CSIRT_FGC offers the incident analysis. It consists in investigating whether indeed an incident occurred. If the incident has occurred, determining the extent of the incident, catalogue its criticized and prepare the incident coordination.

5.1.2. Incident coordination

This service has the objective of coordinating the response to security incidents at the FGC installations with all the IT administrators in all areas, other emergency response IT teams, telecommunications operators, ISPs and other public bodies and private (police, investigators, courts) as appropriate.

The services offered:

- ·Determining the initial cause of the incident (vulnerability exploited).
- ·Prepare a possible action plan
- ·Coordinating with other sites which may be involved.
- ·Coordinating with appropriate law enforcement officials, if necessary.
- ·Making reports and situation analysis (local or to others CSIRT).
- ·Composing announcements and alerts, to users, if applicable.

5.1.3. Incident resolution

This service has the objective of dealing and respond to the security incident to solve it and return to normal situation as soon as possible.

The services offered:

- ·Helping to remove the vulnerability.
- ·Helping to secure the system from the effects of the incident.
- ·Collecting evidence of the incident. Collecting statistics concerning incidents processed, and notifying the community as necessary to assist it in protecting against known attacks.
- ·Informing al campus members about the incident, the solutions taken and how to prevent new related situations.

5.2. Proactive services

This services tries to raise security awareness and to prevent incidents in the future.

The services offered:

- ·Announcements: CSIRT_FGC, aims at providing information (e.g. on threat landscape, published vulnerabilities, new attack tools or artefacts, security/protection measures, etc.) needed to protect systems and networks.
- ·Alerts and warning: This service aims at disseminating information on cyberattacks or disruptions, security vulnerabilities, intrusion alerts, computer viruses, and providing recommendations to tackling and avoid the new security incidents.

5.3. Security and quality management services

CSIRT_FGC has longer-term goals, seeks to improve the security approach of campus users by raising awareness and sensitization to prevent serious security incidents in the future. CSIRT_FGC conducts awareness campaigns on informatics security and good practices periodically for all users. It also organizes talks and basic courses to raise awareness about the importance of information security.

6. Incident reporting forms

FGC has an internal IT incident tool. CSIRT_FGC encourages anyone reporting an incident using this tool. You can find the FGC Staff Portal.

7. Disclaimers

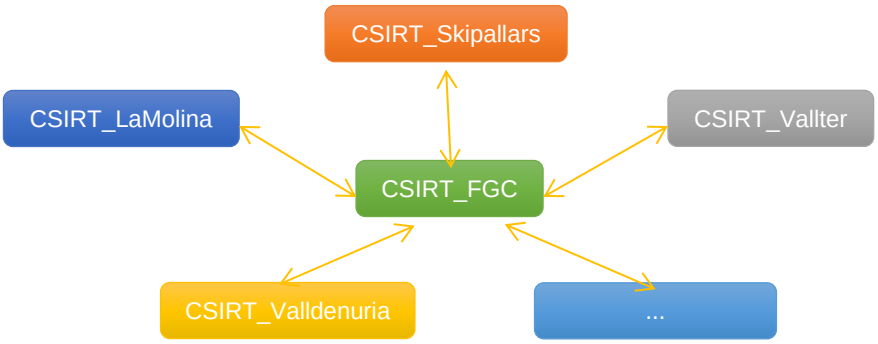
None

10. Línies de futur

En aquest apartat, explicarem la projecció de futur del projecte, que donarà continuïtat i millorarà la funcionalitat i el servei que dona el CSIRT_FGC. De la mateixa manera, la maduresa que anirà assolint l'equip amb el temps de funcionament, tard o d'hora reclamarà una reestructuració o redefinició organitzativa i funcional, que s'haurà de definir i que és el definim com a línies de futur.

En primer lloc, tal i com s'ha definit al llarg del TFM, el CSIRT_FGC arrencarà sota l'àrea de *Tecnologies de la Informació* amb uns serveis adients a la part del serveis corporatius de FGC. Un cop l'equip, passats uns anys, vagi assolint experiència i maduresa en el tractament dels incidents de seguretat, la idea serà fer un escalat organitzatiu i situar-lo al mateix nivell que l'àrea de *Tecnologies de la Informació, Tecnologies de Negoci i Tecnologies de les Comunicacions*, creant l' Àrea de Seguretat, penjant directament de la Direcció TIC. Amb això guanyarà transversalitat a totes les àrees i podrà donar servei a totes elles, cosa que comportarà redefinir el catàleg de serveis per tal de millorar el servei donat a tot els clients del CSIRT.
Aquest escalat, comportarà un gran canvi organitzatiu, ja que apareixerà ben definida la figura del CISO, amb independència total de la seguretat respecte a la funcionalitat, i es podran establir polítiques de seguretat a tots els sistemes d' informació de l'empresa.

En segon lloc, potser en paral·lel o abans de l'escalat. El CSIRT_FGC podria modificar la seva estructura de funcionament i crear CSIRT satèl·lits per donar servei de gestió d'incidents de seguretat a la part de serveis corporatius de les seus remotes. Es crearien CSIRT que donarien serveis local, però connectats i sota la supervisió del CSIRT_FGC. Això comportaria un creixement estructural considerable del CSIRT_FGC així com uns requeriments de recursos humans i econòmics. És per això, que en funció de l'evolució que faci en els primers anys i la situació empresarial es podria donar abans aquest pas que el de l'escalat i creació de la nova Àrea de seguretat.



Il·lustració 17:Estructura satèl·lit per seus remotes amb CSIRT_FGC

Per últim, com a línia de futur, un cop establert i madur el CSIRT_FGC, escalat organitzativament i consolidat com un àrea independent TIC, amb tota l'empresa com a usuaris i amb els serveis consolidats; Potser seria un bon moment per que deixés de ser un CSIRT intern i s'obrís a ser un CSIRT nacional amb comunicacions i relacions a nivell nacional i internacional. Això comportaria un remodelat de l'estructura i certs canvis que donat el moment es podrien assumir per arribar a ser un referent en la seguretat i donar una imatge d'excel·lència sobre el tractament de la seguretat de la informació de FGC.

11. Conclusions

Si fem una cerca ràpida per internet sobre incidents de seguretat, veurem que la tendència dels últims anys és a créixer i a ser cada cop més complexos i perillosos. Avui en dia, totes les empreses són conscients de la importància de les seves dades i la seva informació. Basant-nos en això podem dir que la majoria de les empreses actualment estan interessades en la seguretat informàtica i en la gestió dels incidents de seguretat que poden sofrir. Una bona gestió dels incidents de seguretat els pot evitar molts problemes, tant econòmics, d'imatge de la companyia, legals, etc.

Aquest projecte neix d'aquest interès per millorar la seguretat de la informació i la gestió dels incidents de seguretat que podent sofrir les empreses avui en dia, concretament l'empresa en la que treballo, Ferrocarrils de la Generalitat de Catalunya (FGC). El que es vol oferir amb aquest TFM, és la possibilitat de conèixer amb detall els Equips de Resposta a Incidents de Seguretat (CSIRT) en tots els seus àmbits, formar un equip que encaixi en el perfil i doni els serveis adients pel grup d'usuaris al que donarà servei a FGC i finalment deixar l'equip preparat per la seva posada en marxa.

Un dels primers objectius era obtenir un ampli anàlisi i documentació sobre els CSIRT. Tot i l'interès empresarial que hi pot haver darrera de la gestió d'incidents de seguretat i els seus beneficis, poden sorgir dubtes a l'hora de crear un nou equip o àrea de seguretat i destinar recursos (humans i econòmics) en una empresa si no es coneixen tots els detalls i estan molt clars. A FGC, com a la majoria de les empreses, tot l'òrgan directiu havia de ser conscient i tenir tots els detalls de que és un CSIRT, que ens aporta, com ha de funcionar, quin és l'estat de l'art al seu respecte, etc. Per això, en la primera part del TFM s'ha fet un ampli estudi i anàlisi que detalla des de la creació d'aquests equips a l'estat actual, passant per l'anàlisi dels beneficis que pot aportar a l'organització. El que es pretenia era aconseguir una amplia referència sobre aquests equips que resolgués tota mena de dubte que es pogués plantejar a més de definir les bases sobre les que es crearia el nou CSIRT_FGC. En aquest sentit, s'han aconseguit els objectius ja que per part del cap de TI, ha quedat entès i clar tot el referent a la creació del nou CSIRT.

Un cop assolit l'objectiu de donar coneixements amplis sobre els CSIRT i obtenir el vist i plau per la seva creació, en aquest TFM es planteja aquest segon objectiu de crear i definir un equip que compleixi les expectatives de FGC. Fruit de la investigació, es van analitzar diverses guies oficials de creació i es va decidir seguir-ne tres, les més significatives, però adaptant i millorant en els aspectes que es pogués per adaptar-nos a les expectatives de l'empresa. Partint d'aquí, s'ha fet un anàlisi de FGC i s'ha decidit quin serà l'scope inicial del CSIRT, quines seran les àrees afectades i els serveis i actius a tenir en compte i protegir. Fet això i abans de començar a estructurar definitivament l'equip i definir-lo, s'ha analitzar el grup de clients a qui es donarà servei (FGC) mitjançant un DAFO que ens ha permès enfocar la creació de l'equip i definir de manera justificada quins seran els serveis mínims amb els que arrencarà. Aquest objectiu també ha estat assolit satisfactòriament ja que el cap de TI al qual en un inici serà adscrit l'equip, ha esta d'acord en tota la definició de l'equipo, estructura i definició de serveis que s'ha donat.

Finalment, comentar que s'ha complert la idea i objectiu general d'aquest TFM, ja que s'ha aconseguit crear, deixar llest i preparat l'equip de resposta a incidents, CSIRT_FGC, amb un catàleg de serveis mínims inicials que vetllaran i milloraran la seguretat de les dades en la part corporativa de FGC i que donaran resposta a tots els incidents de

seguretat que es plantegin. Queda pendent per part de FGC de donar el tret de sortida a l'equip i començar a funcionar.

Tot i que no és objectiu d'aquest projecte, m'agradaria concloure amb un breu comentari sobre les línies de futur del CSIRT_FGC que s'han plantejat, ja que donaran continuïtat al projecte i dotaran d'excel·lència el tractament de la seguretat a FGC (assolint totes les àrees i seus remotes de l'empresa) i potser en un futur esdevenint-se un referent en la seguretat i arribar a ser CSIRT Nacional.

12. Glossari

CC – Coordination Center.
CEO – Chief Executive Officer.
CERT – Computer Emergency Response Team.
CIO – Chief Information Officer.
CISO – Chief Information Security Officer.
CSIRT – Computer Security Incident Response Team.
CIRT – Computer Incident Response Team.
CSIRT_FGC – CSIRT creat per FGC.
CSIRT_Skipallars – CSIRT satèl·lit per la seu a Skipallars.
CSIRT_LaMolina – CSIRT satèl·lit per la seu a La Molina.
CSIRT_Valldenuria – CSIRT satèl·lit per la seu a Valldenuria.
CSIRT_Vallter – CSIRT satèl·lit per la seu a Vallter.
DAFO – Debilitat/Amenaces/Fortaleses/Oportunitats.
ENISA – European Union Agency for Network and Information Security.
ENS – Esquema Nacional de Seguretat.
FGC – Ferrocarrils de la Generalitat de Catalunya.
GPG – GnuPG, free version PGP.
IRT – Incident Response Team.
ISO-27001 – Normativa internacional que descriu com gestionar la seguretat de la informació en una empresa.
KPI – Key Performance Indicator.
SERT – Security Emergency Response Team.

13. Bibliografia

Documents:

·Apunts UOC, assignatura *Seminaris en empresa (Cassos A).*

·Guia "Cómo crear un CSIRT paso a paso", de ENISA.

·Guia de seguretat (CCN-STIC-810), "*Guía de creación de un CERT/CSIRT",* de CCN-CERT.

·Guia "*Creating and Managing Computer Security Incident Response Teams (CSIRTs)",* de CERT/CC.

Altra informació al web:

·ENISA - https://www.enisa.europa.eu/

·CCN-CERT - https://www.ccn-cert.cni.es/

·CERT/CC – http://www.cert.org

·CSIRT.es - https://www.csirt.es/index.php/es/

·FISRT - https://www.scadahacker.com/resources/cert.html

·TI (Trusted Introducer) - https://www.trusted-introducer.org/