Plec de prescripcions tècniques per la contractació dels serveis de manteniment correctiu, monitorització, gestió i administració de la Ciberseguretat de l'Organisme de Gestió Tributària de la Diputació de Barcelona.

Contingut

1. OBJECTE.

És objecte del present plec fixar les condicions tècniques a les quals s'ajustarà la contractació consistent en:

- La subscripció i el suport tècnic de les llicències dels tallafocs.
- La subscripció i el suport tècnic de les llicències dels antivirus pels escriptoris virtuals i ordinadors.
- El servei de manteniment correctiu dels commutadors dels centres de processaments de dades (CPD) i dels tallafocs.
- El servei de monitorització, gestió i administració dels commutadors de xarxa i equips de seguretat perimetral.
- La implantació de serveis addicionals de ciberseguretat.

2. SITUACIÓ ACTUAL.

Pel que fa a l'equipament de ciberseguretat, l'ORGT disposa de tallafocs en alta disponibilitat, un Sistema de Gestió d'esdeveniments (SIEM de l'anglès Security Information and Event Management) i antivirus en tots els escriptoris virtuals (VD de l'anglès Virtual Desktop) i en les estacions de treball (PC).

El tallafocs és un clúster de dos nodes, que treballen en mode actiu-passiu, del model *PA3020*, del fabricant Palo Alto Networks i fa les següents tasques:

- Filtratge de les comunicacions de sortida cap a internet.
- Filtratge de les comunicacions d'entrada que accedeixen als diferents serveis de l'ORGT.
- Filtratge d'adreces (URL-Filtering) depenent de la categoria a la que pertanyen.
- Detecció de virus en la navegació, fins i tot en les comunicacions encriptades.
- Permetre l'accés a la infraestructura de l'ORGT mitjançant túnels VPN-SSL.
- Permetre l'accés a la infraestructura de l'ORGT mitjançant túnels IPSEC.
- Autenticació mitjançant certificat digital (DNIe o TCAT) per accedir al tallafocs o a algun dels túnels VPN-SSL.
- Verificació que els ordinadors, que es connecten a la infraestructura de l'ORGT a través de túnel VPN-SSL, estan actualitzats i es troben correctament protegits mitjançant un antivirus.

L'ORGT disposa de 625 escriptoris virtuals protegits mitjançant l'antivirus *McAfee Move AV for Virtual Desktops*. Aquest antivirus utilitza 8 servidors virtuals per a realitzar la protecció dels escriptoris virtuals.

En la Direcció de Serveis d'Informàtica de l'ORGT hi ha estacions de treball, tipus PC, protegits per l'antivirus *McAfee Endpoint Protection Suite*.

L'ORGT per dur a terme els serveis que ofereix als ajuntament disposa de dos centres de processament de dades, ubicats en la província de Barcelona. Pel que fa a la Xarxa Local (LAN de l'anglès Local Area Network), ambdós CPD disposen del següent equipament:

- 2 commutadors *Cisco Nexus 5548* de 48 ports.
- 1 extensió de ports tipus FEX, *Cisco Nexus 2224T* de 24 ports.

Aquests commutadors realitzen tasques de commutació i d'encaminament estàtic a nivell 3.

El vigent servei de monitorització, gestió i administració dels commutadors de xarxa i equips de seguretat perimetral, es recolza en un Sistema de Gestió d'Esdeveniments (SIEM de l'anglès Security Information and Event Management), propietat de l'operador del servei, que recopila esdeveniments del tallafocs i fa una recerca de patrons d'atac cibernètic. El SIEM és un dispositiu virtual *Allien Vault all-in-one* que permet una consolidació de 400 EPS (Esdeveniments per segon).

3. SUBSCRIPCIÓ I SUPORT TÈCNIC DE LLICÈNCIES

3.1. Llicències pels tallafocs.

Per aconseguir que els tallafocs realitzin les funcionalitats necessàries, cal subscriure les següents llicències:

- *Threat Prevention*, que habilita les funcionalitats d'antivirus, antispyware i protecció de vulnerabilitats, amb actualitzacions diàries de les signatures del codi maliciós.
- *Wildfire*, que aporta funcionalitats avançades de detecció de codi maliciós amb actualitzacions cada 5 minuts de les signatures.
- *PAN-DB URL-Filtering*, que habilita la possibilitat de crear polítiques de seguretat que permetin o bloquegin l'accés segons la categoria dinàmica de l'adreça URL.
- *Global Protect*, que habilita la verificació de les mesures de seguretat que tenen implantades els ordinadors que es connecten a la infraestructura de l'ORGT a través de túnels VPN-SSL.

Aquestes 4 llicències cal aportar-les per cadascun dels 2 nodes del tallafocs i aniran acompanyades d'un servei de suport tècnic que resolgui les incidències que es puguin produir en la gestió i utilització de les llicències.

3.2. Llicències pels antivirus.

A fi de protegir de programari maliciós els llocs de treball dels empleats de l'ORGT, caldrà subscriure les següents llicències:

- 625 llicències de *McAfee Move AV for Virtual Desktops*,
- 40 llicències de *McAfee Endpoint Protection Suite*,

Aquestes llicències aniran acompanyades d'un servei de suport tècnic que resolgui les incidències que es puguin procuir en la gestió i utilització de les llicències.

4. SERVEI DE MANTENIMENT CORRECTIU DELS COMMUTADORS DEL CENTRE DE PROCESSAMENT DE DADES(CPD) I DELS TALLAFOCS.

El servei de manteniment correctiu té per objectiu esmenar i reparar les incidències o avaries que sorgeixen en els equips físics i en corregir els problemes derivats del funcionament incorrecte dels programes associats a l'equipament. Realitzarà les següents accions:

- Registrar les incidències i peticions,
- Seguiment de les incidències i peticions,
- Diagnòstic i primer intent de resolució de la incidència,
- En el cas d'avaries hardware, el contractista enviarà un tècnic de camp per substituir les peces avariades per les subministrades pel fabricant del maquinari.
- Configurar el nou maquinari.

El contractista haurà de disposar de les certificacions de suport (clàusula 1.10 PCAP) per part del fabricant de l'equipament, i això li permetrà:

- Accedir a les actualitzacions de programari dels equips,
- Accedir a la base de dades de coneixement,
- Disposar d'equips de recanvi.
- Obrir casos (per incidències i per peticions) amb el fabricant del maquinari.

L'equipament a mantenir és l'especificat a la clàusula 7 d'aquest plec.

El servei tindrà les següents característiques:

- Disposarà d'un punt d'entrada únic d'incidències i peticions, accessible telefònicament i per correu electrònic.
- Servei d'assistència en modalitat 24 x 7, tots els dies de l'any.
- La mà d'obra, els desplaçaments i els recanvis estaran inclosos en el preu del servei.
- Nombre il·limitat casos.

La qualitat del servei de manteniment estarà determinat per les següents variables:

- Temps de resposta remot, per incidències i consultes de programari: 2 hores.
- Temps de resposta presencial, per avaries de maquinari: 4 hores.

El temps de resposta remot és el temps transcorregut entre l'obertura de la incidència, fins que el tècnic encarregat de la resolució del problema contacta amb els tècnics de l'ORGT.

El temps de resposta presencial és el temps transcorregut entre l'obertura de la incidència, fins que el tècnic encarregat de la resolució del problema accedeixi a la ubicació del maquinari, tan per solventar l'avaria com per substituir el maquinari.

5. SERVEI DE MONITORITZACIÓ, GESTIÓ i ADMINISTRACIÓ DELS COMMUTADORS I EQUIPS DE SEGURETAT PERIMETRAL.

El contractista serà el responsable de la seguretat de les xarxes LAN dels CPD i la seguretat perimetral de l'ORGT. Per això haurà de garantir el funcionament continu de la infraestructura en horari 24*7, 365 dies a l'any.

Els dispositius a monitoritzar, gestionar i administrar seran els especificats a la clàusula 7 d'aquest plec.

Les tasques a dur a terme són:

- Monitoritzar els commutadors i tallafocs a fi de detectar, el més aviat possible, el mal funcionament (incidències) d'aquests dispositius.
- Implementar les accions necessàries per la correcció de les incidències detectades en la monitorització, o reportades per la Direcció de Serveis d'Informàtica.
- Fer el seguiment del registre d'activitat del tallafocs, mitjançant el SIEM, per detectar possibles ciberatacs. L'empresa contractista haurà de proposar possibles modificacions en la seguretat perimetral per evitar que fructifiquin els atacs detectats.
- Revisió periòdica preventiva (apartat 5.8 d'aquest plec) de la plataforma de commutadors de LAN i tallafocs.
- Anàlisi dels incidents i les alertes de seguretat detectades.
- Proposar les millores que consideri oportunes per l'òptim funcionament de l'entorn de xarxa dels CPD i de la seguretat perimetral de l'ORGT.
- Implementar les peticions sol·licitades per l'ORGT. Una vegada exposades per l'ORGT les seves necessitats, i el contractista proposarà i executarà les solucions oportunes.
- Anàlisi de les amenaces i incidents de seguretat publicats pels Equips de Resposta a Emergències informàtiques (CERT de l'anglès Computer Emergency Response Team) per tal de verificar si l'ORGT es troba afectat per l'amenaça i en cas afirmatiu informar a la Direcció de Serveis d'informàtica de l'ORGT.
- Suport tecnològic en matèria de Ciberseguretat.
- Elaborar els informes de seguiment del servei (apartat 5.10 d'aquest plec.

5.1. Protocol d'actuació.

El contractista elaborarà, de manera consensuada amb la Direcció de Serveis d'informàtica, el *Protocol d'actuació*. Aquest document ha de recollir els procediments a seguir a fi de notificar i resoldre les incidències detectades en els serveis de manteniment, monitorització, gestió i administració dels commutadors del centre de processament de dades (CPD) i equips de seguretat perimetral. Com a mínim ha de tractar els següents aspectes:

- Descripció del serveis, recursos humans que es dedicaran, identificació de la persona responsable del servei.
- Procediment d'actuació per a cada tipus d'incidència.
- Procediment de comunicació de les incidències (apartat 5.6 d'aquest plec).
- Procediment d'escalat de les incidències, depenent de la seva gravetat.
- Procediment de comunicació de peticions (apartat 5.7 d'aquest plec).
- Acords de servei que han de complir la gestió de peticions i la d'incidències.
- Classificació dels ciberatacs detectats pel SIEM i procediment de resposta.
- Tasques que es realitzaran a les revisions periòdiques mensuals (apartat 5.8 d'aquest plec).

El contractista ha de lliurar el *Protocol d'actuació* a la Direcció de Serveis d'informàtica en el termini de 15 dies hàbils a comptar de la data de la signatura del contracte.

5.2. Infraestructura necessària.

La monitorització, gestió i administració de l'equipament de seguretat es realitzarà mitjançant una connexió remota segura a la xarxa de l'ORGT. El contractista aportarà les eines, llicències i línies de comunicacions necessàries.

5.3. Comunicació de les incidències i les peticions.

El contractista oferirà una adreça de correu electrònic i un telèfon de contacte per a que l'ORGT pugui comunicar les incidències i les peticions.

5.4. Responsable del servei.

L'empresa contractista nomenarà una persona responsable del servei que serà la interlocutora amb l'ORGT i coordinarà els serveis objecte del contracte.

El responsable realitzarà, entre d'altres, les següents tasques:

- Elaborar els informes de seguiment del servei (apartat 5.10 d'aquest plec).
- Convocar les reunions trimestrals (apartat 5.9 d'aquest plec).
- Fer l'acta de les reunions trimestrals,
- Elaborarà les propostes dels serveis addicionals (apartat 6 d'aquest plec).

5.5. Sistema de Gestió d'esdeveniments (SIEM).

L'empresa contractista aportarà un SIEM que recollirà els esdeveniments de seguretat del tallafocs, farà una detecció de patrons de ciberatacs i permetrà automatitzar les respostes. Aquest SIEM ha de ser capaç de tractar 400 esdeveniments per segon, tal com fa el SIEM actual.

Quan es detecti un ciberatac l'empresa contractista haurà d'informar a l'ORGT i proposar possibles modificacions en la seguretat perimetral per evitar que aquest fructifiqui, i quan la Direcció de Serveis d'Informàtica hi doni el vistiplau, durà a terme les modificacions necessàries en la infraestructura de seguretat per evitar el ciberatac.

5.6. Gestió d'incidències.

Les incidències són un mal funcionament del sistema. De vegades seran detectades pel servei de monitorització i d'altres vegades seran reportades pel propi ORGT. El contractista proposarà la solució més adequada, i amb el vistiplau de la Direcció de Serveis d'Informàtica, la durà a terme en els equips de seguretat corresponents.

A criteri dels tècnics de l'ORGT, les incidències es classificaran en dos nivells d'importància: greu i lleu. Les incidències es consideraran lleus excepte les de la següent enumeració, que es considaran greus:

- Indisponibilitat dels dos commutadors del CPD actiu.
- Indisponibilitat en un dels tallafocs si l'altre no pren el relleu.

En cas d'incidències greus, en que la correcció remota sigui inviable, l'ORGT sol·licitarà la presència in situ d'un tècnic a les dependències de l'ORGT (instal·lacions on es troben els CPD o oficina de la Direcció de Serveis d'informàtica)

Les incidències s'atendran en horari 24*7 amb els següents temps de resposta:

- Temps de resposta remot incidència greu: 30 minuts.
- Temps de resposta presencial incidència greu: 2 hores
- Temps de resposta remot incidència lleu: 2 hores.
- Temps de resposta presencial incidència lleu: Proper dia laborable, de dilluns a divendres.

El temps de resposta remot és el temps transcorregut entre l'obertura de la incidència, fins que el tècnic encarregat de la resolució del problema contacta amb els tècnics de l'ORGT.

El temps de resposta presencial és el temps transcorregut entre l'obertura de la incidència, fins que el tècnic encarregat de la resolució del problema accedeixi a la ubicació del maquinari avariat.

El contractista haurà de fer d'interlocutor amb la Diputació de Barcelona i amb l'operador de comunicacions de dades, en les incidències de l'ORGT en les que pugui comportar una afectació a l'anell de dades de la Diputació de Barcelona o la interconnexió amb les xarxes de Diputació de Barcelona.

5.7. Gestió de peticions.

L'ORGT realitzarà peticions de canvis en la configuració de la xarxa LAN del CPD i la ciberseguretat. El contractista proposarà l'opció més adequada, i amb el vistiplau de la

Direcció de Serveis d'Informàtica, la durà a terme en els equips de xarxa relacionats a la clàusula 7 d'aquest plec.

Relació no exhaustiva de tipus de peticions:

- Configuració de ports del commutador.
- Assignació de VLAN.
- Canvis d'adreçament.
- Canvis d'encaminament.
- Canvi de paraula de pas d'accés als equips.
- Afegir o modificar una política del tallafocs.
- Afegir o modificar una política NAT (Network Address Translation).
- Crear un túnel IPSEC amb una empresa col·laboradora.
- Crear un túnel SSL-VPN amb una empresa col·laboradora.
- Configurar en el SIEM notificacions d'alertes en funció del nivell de criticitat amb execució de procediments d'escalat.
- Configurar en el SIEM respostes automàtiques a esdeveniments.
- Crear en el SIEM quadres de comandament i informes.
- Forçar l'actualització de les signatures de malware en el tallafocs.

A criteri dels tècnics de l'ORGT, les peticions es classificaran en dos nivells d'importància: normals i urgents.

Les peticions s'atendran en horari de 8:00 h a 21:00 h, (de dilluns a divendres no festius) amb els següents temps de resposta:

- Temps de resposta petició urgent: 30 minuts.
- Temps de resposta petició normal 2 hores.

El temps de resposta és el temps transcorregut entre l'obertura de la petició, fins que el tècnic encarregat de la resolució contacta amb els tècnics de l'ORGT.

5.8. Revisions periòdiques.

Periòdicament es realitzarà un seguit de comprovacions de l'equipament de ciberseguretat (tallafocs i commutadors de CPD). Aquestes revisions seran mensuals i inclouran com a mínim les següents tasques:

- Anàlisi de les noves versions de programari de l'equipament i de la necessitat d'aplicar-les.
- Anàlisi d'actualitzacions de seguretat de l'equipament i de la necessitat d'aplicar-les.
- Anàlisi del rendiment dels dispositius a fi de detectar necessitats d'escalat de l'equipament.
- Anàlisi de la política de seguretat dels tallafocs.
- Anàlisi de la configuració del SIEM.
- Realització de còpies de seguretat de la configuració dels dispositius: commutadors dels CPD i tallafocs.
- Anàlisi de les amenaces i incidents de seguretat publicats pels CERT (Equips de resposta a Incidents) com per exemple INTECO-CERT, CCN-CERT o

CESICAT-CERT. Comprovar si l'ORGT està afectat per aquestes amenaces i si és necessari, proposar les mesures preventives adequades.

El resultat d'aquestes tasques s'inclouran en l'informe mensual de seguiment del servei (apartat 5.10 d'aquest plec).

5.9. Reunions de seguiment del servei.

El responsable del servei convocarà trimestralment una reunió de seguiment del servei en la que es tractaran, com a mínim, els següents temes:

- Incidències més habituals.
- Revisió dels serveis addicionals portats a terme (apartat 6 d'aquest plec).
- Seguiment de la qualitat del servei.
- Millores possibles en el servei.
- Millores possibles a la infraestructura de seguretat.

El responsable del servei elaborarà l'acta de la reunió i la lliurarà en un termini màxim d'una setmana.

5.10. Informes de seguiment del servei.

5.10.1. Informe setmanal

El contractista entregarà setmanalment un informe, en format full de càlcul, en el que hi constaran tots els casos (incidències i peticions) que s'han dut a terme. Per a cadascun dels casos s'especificarà la següent informació:

- Identificador de cas,
- Descripció del cas,
- Tipus de cas (incidència o petició),
- Hora de l'avís,
- Hora d'atenció,
- Hora de tancament,
- Indicador de si s'ha assolit l'acord de nivell de servei (ANS).

L'informe setmanal s'entregarà abans del dimarts de la setmana següent.

5.10.2. Informe mensual

També s'emetrà un informe mensual de seguiment del servei que ha de contenir la següent informació:

- Inventari d'equips gestionats.
- Llistat de casos (incidències i peticions) del mes, informant si s'ha assolit l'acord de nivell de servei (ANS).
- Volum de casos oberts, tancats i en curs.

- Tipologia dels casos oberts, tancats i en curs.
- Resum de serveis addicionals portats a terme (apartat 6 d'aquest plec) que inclourà una descripció del servei i el nombre d'hores consumides.
- Disponibilitat dels dispositius gestionats.
- Resum d'esdeveniments detectats pel SIEM.
- Detall dels esdeveniments de SIEM que han comportat un canvi en la infraestructura de seguretat de l'ORGT.
- Proposta de millores en la ciberseguretat de l'ORGT.
- Resum de noticies relacionades amb la ciberseguretat.
- Taula de versions de software dels dispositius gestionats i data de finalització del suport.
- Gràfics de trànsit dels ports més importants dels commutadors de CPD's i dels ports dels tallafocs.
- Gràfics de consum de CPU dels equips gestionats: tallafocs i commutadors de xarxa.
- Configuració dels commutadors dels CPD i tallafocs.

L'informe mensual s'ha d'entregar abans del dia 15 del mes següent.

5.11. Volumetria del servei.

El nombre estimat de peticions i incidències anuals, basat en l'experiència del vigent contracte, és de 300 casos. Aquest nombre és purament orientatiu. El contractista executarà totes les incidències i peticions que l'ORGT sol·liciti durant la vigència del contracte.

6. SERVEIS ADDICIONALS DE CIBERSEGURETAT

En funció dels resultats d'auditories, d'avisos d'amenaces publicats pels CERT, o bé perquè cal complir alguna normativa, com l'Esquema Nacional de Seguretat (ENS) o el Reglament General de protecció de dades (RGPD), l'ORGT requerirà al contractista que es facin projectes relacionats amb la ciberseguretat, que no es troben inclosos dins el servei de monitorització, gestió i administració (detallat a l'apartat 5 d'aquest plec).

Un llistat no exhaustiu de possibles projectes de ciberseguretat pot ser el següent:

- Instal·lar millores de seguretat en l'equipament de seguretat (clàusula 7 d'aquest plec), a fi d'eliminar vulnerabilitats conegudes.
- Instal·lar millores de seguretat en els servidors Windows, a fi d'eliminar vulnerabilitats conegudes.
- Instal·lació i configuració de nou maquinari de seguretat.
- Configuració de noves funcionalitats de l'equipament de seguretat.
- Millores en la política de seguretat de l'ORGT.

- Afegir fonts d'informació al SIEM.
- Formació sobre nous productes i tendències, relacionats amb la ciberseguretat.
- Simulació de ciberatacs: Phishing, DDOS ...
- Auditoria de seguretat d'aplicacions software.
- Auditoria de seguretat de la xarxa interna de l'ORGT.
- Auditoria de seguretat de les xarxes WiFi.
- Auditoria de seguretat d'informació accessible des de Internet.
- Auditoria d'enginyeria social.
- Auditories de Hacking ètic.

Quan l'ORGT necessiti dur a terme algun dels projectes enumerats en l'apartat anterior, o qualsevol altra tasca que estigui relacionada amb la ciberseguretat, se li exposarà a la persona responsable del servei del contractista qui elaborarà una *Proposta d'Implantació*, en la que es detallarà quines tasques es duran a terme, quina dedicació dels tècnics del contractista caldrà i quina documentació s'entregarà al final del projecte.

La *Proposta d'Implantació* del projecte s'entregarà a la Direcció d'Informàtica de l'ORGT en un màxim de 30 dies naturals a comptar de la data de la petició.

L'ORGT decidirà quin és el millor moment per a realitzar la implantació del projecte, de manera que els serveis que ofereix l'ORGT es vegin afectats el mínim possible. Això pot comportar que algunes de les tasques del projecte sigui necessari executar-les en horari nocturn (de les 21:00 a les 8:00), en dissabte o en dia festiu. Aquestes hores de treball les anomenem extraordinàries.

En contraposició amb les hores extraordinàries hi haurà les hores ordinàries, les quals seran les que es portin a terme de dilluns a divendres, no festiu, de les 8:00 del matí a les 21:00h.

La dedicació a aquests projectes addicionals de ciberseguretat, s'estima en un màxim de 200 hores ordinàries i 40 hores extraordinàries anuals. El contractista les facturarà trimestralment en funció de la seva realització efectiva. L'ORGT no està obligat a exhaurir l'esmentat nombre de hores.

7. DISPOSITIUS A MANTENIR

En la següent taula s'enumeren els dispositius dels que caldrà dur a terme el manteniment i els serveis addicionals de ciberseguretat. De cadascun d'ells s'especifica la seva localització, el model, el nom, el número de sèrie i la data d'adquisició.

OFICINA	MODEL	NOM	SERIAL NUMBER	DATA ADQUISICIÓ
CDG TERRASSA	N5K-C5548UP-SUP	NXT1	FOC18150CLZ	6/10/2014
CDG TERRASSA	Nexus 5548 Chassis	NXT1	SSI180304ZB	6/10/2014
CDG TERRASSA	N55-M16UP	NXT1	FOC1809409U	6/10/2014
CDG TERRASSA	N55-D160L3-V2	NXT1	FOC181186M7	6/10/2014
CDG TERRASSA	N55-PAC-750W	NXT1	ART1808102B	6/10/2014
CDG TERRASSA	N55-PAC-750W	NXT1	ART18081018	6/10/2014
CDG TERRASSA	N5K-C5548UP-SUP	NXT2	FOC19441SVJ	1/1/2016
CDG TERRASSA	Nexus 5548 Chassis	NXT2	SSI192000PS	1/1/2016
CDG TERRASSA	N55-M16UP	NXT2	FOC194520YP	1/1/2016
CDG TERRASSA	N55-D160L3-V2	NXT2	FOC194184HY	1/1/2016
CDG TERRASSA	N55-PAC-750W	NXT2	PST1941U0FV	1/1/2016
CDG TERRASSA	N55-PAC-750W	NXT2	PST1941U01N	1/1/2016
CDG TERRASSA	Cisco Nexus 2224	NXT3	SSI1921001E	1/1/2016
CDG TERRASSA	N2200-PAC-400W-B	NXT3	LIT19440SWX	1/1/2016
CDG TERRASSA	N2200-PAC-400W-B	NXT3	LIT19440T4G	1/1/2016
CDG TERRASSA	N2K-C2224TP-1GE	NXT3	FOC19470SEK	1/1/2016
CDG TERRASSA	PAN-PA-3020	FWT1	1801028002	1/1/2016
ED. RELLOTGE	N5K-C5548UP-SUP	NXR1	FOC19441SWP	1/1/2016
ED. RELLOTGE	Nexus 5548 Chassis	NXR1	SSI192000SN	1/1/2016
ED. RELLOTGE	N55-M16UP	NXR1	FOC19441ZZL	1/1/2016
ED. RELLOTGE	N55-D160L3-V2	NXR1	FOC1941880P	1/1/2016
ED. RELLOTGE	N55-PAC-750W	NXR1	PST1941U0HL	1/1/2016
ED. RELLOTGE	N55-PAC-750W	NXR1	PST1941U0GL	1/1/2016
ED. RELLOTGE	N5K-C5548UP-SUP	NXR2	FOC19441SXT	1/1/2016
ED. RELLOTGE	Nexus 5548 Chassis	NXR2	SSI192000SP	1/1/2016
ED. RELLOTGE	N55-M16UP	NXR2	FOC1944202X	1/1/2016
ED. RELLOTGE	N55-D160L3-V2	NXR2	FOC19393GJT	1/1/2016
ED. RELLOTGE	N55-PAC-750W	NXR2	PST1941U080	1/1/2016
ED. RELLOTGE	N55-PAC-750W	NXR2	PST1941U033	1/1/2016
ED. RELLOTGE	Cisco Nexus 2224	NXR3	SSI192100C7	1/1/2016
ED. RELLOTGE	N2200-PAC-400W-B	NXR3	LIT19360B8Q	1/1/2016
ED. RELLOTGE	N2200-PAC-400W-B	NXR3	LIT19360B6F	1/1/2016
ED. RELLOTGE	N2K-C2224TP-1GE	NXR3	FOC19381ESV	1/1/2016
ED. RELLOTGE	PAN-PA-3020	FWR1	1801028005	1/1/2016

Els commutadors NXT1, NXT2, NXR1 i NXR2 disposen de convertidors GBIC dels que també caldrà fer el manteniment. En la següent taula s'especifiquen aquests convertidors i s'informa l'equip en que està connectat, a quin port, el tipus, el part-number i el número de sèrie del convertidor.

EQUIP	PORT	TIPUS	PART-NUMBER	NÚMERO DE SÈRIE
NXT1	Ethernet1/1	10Gbase-SR	SFBR-709SMZ-CS1	AVD1741A5ZB
NXT1	Ethernet1/2	10Gbase-SR	SFBR-709SMZ-CS1	AVD1741A5ZA
NXT1	Ethernet1/4	10Gbase-SR	SFBR-709SMZ-CS1	AVD1741A5YE

EQUIP	PORT	TIPUS	PART-NUMBER	NÚMERO DE SÈRIE
NXT1	Ethernet1/5	10Gbase-SR	SFBR-709SMZ-CS1	AVD1741A5X2
NXT1	Ethernet1/6	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A7ES
NXT1	Ethernet1/7	Fabric Extender Transceiver	PLRXPL-VC-S43-CG	JUR1932B9DU
NXT1	Ethernet1/8	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A7EM
NXT1	Ethernet1/9	SFP-1000BASE-T	SP7041_Rev_F	MTC1803048Q
NXT1	Ethernet1/10	SFP-1000BASE-T	SP7041_Rev_F	MTC180304XA
NXT1	Ethernet1/11	SFP-1000BASE-T	SP7041_Rev_F	MTC180304Z9
NXT1	Ethernet1/12	SFP-1000BASE-T	SP7041_Rev_F	MTC180304Y3
NXT1	Ethernet1/13	SFP-1000BASE-T	SP7041_Rev_F	MTC180302U8
NXT1	Ethernet1/14	SFP-1000BASE-T	SP7041_Rev_F	MTC1803031Q
NXT1	Ethernet1/15	SFP-1000BASE-T	SP7041_Rev_F	MTC1803046W
NXT1	Ethernet1/16	SFP-1000BASE-T	SP7041_Rev_F	MTC18030465
NXT1	Ethernet1/17	SFP-1000BASE-T	SP7041_Rev_F	MTC180304P4
NXT1	Ethernet1/18	SFP-1000BASE-T	SP7041_Rev_F	MTC180302U9
NXT1	Ethernet1/19	SFP-1000BASE-T	SP7041_Rev_F	MTC180304G6
NXT1	Ethernet1/20	SFP-1000BASE-T	SP7041_Rev_F	MTC180304TB
NXT1	Ethernet1/21	SFP-1000BASE-T	SP7041_Rev_F	MTC180304VF
NXT1	Ethernet1/22	SFP-1000BASE-T	SP7041_Rev_F	MTC1803046Y
NXT1	Ethernet1/23	SFP-1000BASE-T	SP7041_Rev_F	MTC180304WF
NXT1	Ethernet1/24	SFP-1000BASE-T	SP7041_Rev_F	MTC180304EN
NXT1	Ethernet1/25	SFP-1000BASE-T	SP7041_Rev_F	MTC1803046U
NXT1	Ethernet1/26	SFP-1000BASE-T	SP7041_Rev_F	MTC180304EM
NXT1	Ethernet1/27	SFP-1000BASE-T	SP7041_Rev_F	MTC180303HD
NXT1	Ethernet1/28	SFP-1000BASE-T	SP7041_Rev_F	MTC180303GE
NXT1	Ethernet1/29	SFP-1000BASE-T	SP7041_Rev_F	MTC180303FG
NXT1	Ethernet1/30	SFP-1000BASE-T	SP7041_Rev_F	MTC180304ER
NXT1	Ethernet1/31	SFP-1000BASE-T	SP7041_Rev_F	MTC1803053R
NXT1	Ethernet1/32	SFP-1000BASE-T	SP7041_Rev_F	MTC180303B4
NXT1	Ethernet2/1	SFP-1000BASE-T	SP7041_Rev_F	MTC1803049E
NXT1	Ethernet2/2	SFP-1000BASE-T	SP7041_Rev_F	MTC180303LM
NXT1	Ethernet2/3	SFP-1000BASE-T	SP7041_Rev_F	MTC180304RU
NXT1	Ethernet2/4	SFP-1000BASE-T	SP7041_Rev_F	MTC1803045Y
NXT1	Ethernet2/5	SFP-1000BASE-T	SP7041_Rev_F	MTC180304S9
NXT1	Ethernet2/6	SFP-1000BASE-T	SP7041_Rev_F	MTC180304RW
NXT1	Ethernet2/7	SFP-1000BASE-T	SP7041_Rev_F	MTC180304W4
NXT1	Ethernet2/8	SFP-1000BASE-T	SP7041_Rev_F	MTC180303R9
NXT1	Ethernet2/9	SFP-1000BASE-T	SP7041_Rev_F	MTC180304F1
NXT1	Ethernet2/10	SFP-1000BASE-T	ABCU-5710RZ-CS4	AGM18062275
NXT1	Ethernet2/11	SFP-1000BASE-T	SP7041_Rev_F	MTC180302UH
NXT1	Ethernet2/13	10Gbase-SR	FTLX8574D3BCL-CS	FNS220614FN
NXT1	Ethernet2/14	10Gbase-SR	FTLX8574D3BCL-CS	FNS220614E2
NXT1	Ethernet2/15	10Gbase-SR	FTLX8574D3BCL-CS	FNS220614FB
NXT1	Ethernet2/16	10Gbase-SR	FTLX8574D3BCL-CS	FNS220614CX

EQUIP	PORT	TIPUS	PART-NUMBER	NÚMERO DE SÈRIE
NXT2	Ethernet1/1	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A62V
NXT2	Ethernet1/2	10Gbase-SR	FTLX8571D3BCL-C2	FNS19430WCU
NXT2	Ethernet1/3	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A63W
NXT2	Ethernet1/4	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A612
NXT2	Ethernet1/5	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A63G
NXT2	Ethernet1/6	10Gbase-SR	SFBR-709SMZ-CS1	AVD1937A6H1
NXT2	Ethernet1/7	Fabric Extender Transceiver	PLRXPL-VC-S43-CG	JUR1932B9D4
NXT2	Ethernet1/8	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A63C
NXT2	Ethernet1/9	SFP-1000BASE-T	SP7041-R	MTC194005UP
NXT2	Ethernet1/10	SFP-1000BASE-T	SP7041-R	MTC194005UX
NXT2	Ethernet1/11	SFP-1000BASE-T	SP7041-R	MTC1940034X
NXT2	Ethernet1/12	SFP-1000BASE-T	SP7041-R	MTC194005RT
NXT2	Ethernet1/13	SFP-1000BASE-T	SP7041-R	MTC194005UC
NXT2	Ethernet1/14	SFP-1000BASE-T	SP7041-R	MTC194005XH
NXT2	Ethernet1/15	SFP-1000BASE-T	SP7041-R	MTC19400A08
NXT2	Ethernet1/16	SFP-1000BASE-T	SP7041-R	MTC194005Z6
NXT2	Ethernet1/17	SFP-1000BASE-T	SP7041-R	MTC19400352
NXT2	Ethernet1/18	SFP-1000BASE-T	SP7041-R	MTC19400A0T
NXT2	Ethernet1/19	SFP-1000BASE-T	SP7041-R	MTC1940036Y
NXT2	Ethernet1/20	SFP-1000BASE-T	SP7041-R	MTC194005VG
NXT2	Ethernet1/21	SFP-1000BASE-T	SP7041-R	MTC19400A0C
NXT2	Ethernet1/22	SFP-1000BASE-T	SP7041-R	MTC19400FQS
NXT2	Ethernet1/23	SFP-1000BASE-T	SP7041-R	MTC194005Y8
NXT2	Ethernet1/24	SFP-1000BASE-T	SP7041-R	MTC194005WD
NXT2	Ethernet1/25	SFP-1000BASE-T	SP7041-R	MTC194005YT
NXT2	Ethernet1/26	SFP-1000BASE-T	SP7041-R	MTC194005W9
NXT2	Ethernet1/27	SFP-1000BASE-T	SP7041-R	MTC19400FVV
NXT2	Ethernet1/28	SFP-1000BASE-T	SP7041-R	MTC19400A12
NXT2	Ethernet1/29	SFP-1000BASE-T	SP7041-R	MTC1940035V
NXT2	Ethernet1/30	SFP-1000BASE-T	SP7041-R	MTC194005YB
NXT2	Ethernet1/31	SFP-1000BASE-T	SP7041-R	MTC19400A0Q
NXT2	Ethernet1/32	SFP-1000BASE-T	SP7041-R	MTC19400FD4
NXT2	Ethernet2/1	SFP-1000BASE-T	SP7041-R	MTC194005UT
NXT2	Ethernet2/2	SFP-1000BASE-T	SP7041-R	MTC19400FRW
NXT2	Ethernet2/3	SFP-1000BASE-T	SP7041-R	MTC194005U2
NXT2	Ethernet2/4	SFP-1000BASE-T	SP7041-R	MTC19400A0R
NXT2	Ethernet2/5	SFP-1000BASE-T	SP7041-R	MTC1940036Q
NXT2	Ethernet2/6	SFP-1000BASE-T	SP7041-R	MTC19400FVZ
NXT2	Ethernet2/7	SFP-1000BASE-T	SP7041-R	MTC1940033L
NXT2	Ethernet2/8	SFP-1000BASE-T	SP7041-R	MTC19400AN7
NXT2	Ethernet2/13	10Gbase-SR	FTLX8574D3BCL-CS	FNS220612GZ
NXT2	Ethernet2/14	10Gbase-SR	FTLX8574D3BCL-CS	FNS220612GS
NXT2	Ethernet2/15	10Gbase-SR	FTLX8574D3BCL-CS	FNS220612H5

EQUIP	PORT	TIPUS	PART-NUMBER	NÚMERO DE SÈRIE
NXT2	Ethernet2/16	10Gbase-SR	FTLX8574D3BCL-CS	FNS220612E4
NXR1	Ethernet1/1	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A5YR
NXR1	Ethernet1/2	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A5Z7
NXR1	Ethernet1/3	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A1AZ
NXR1	Ethernet1/4	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A18F
NXR1	Ethernet1/5	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A1AJ
NXR1	Ethernet1/6	10Gbase-SR	FTLX8571D3BCL-C2	FNS19430JQL
NXR1	Ethernet1/7	Fabric Extender Transceiver	PLRXPL-VC-S43-CG	JUR1932B29G
NXR1	Ethernet1/8	10Gbase-SR	FTLX8571D3BCL-C2	FNS19430JQN
NXR1	Ethernet1/9	SFP-1000BASE-T	SP7041-R	MTC1940062G
NXR1	Ethernet1/10	SFP-1000BASE-T	SP7041-R	MTC194008J9
NXR1	Ethernet1/11	SFP-1000BASE-T	SP7041-R	MTC194008LD
NXR1	Ethernet1/12	SFP-1000BASE-T	SP7041-R	MTC194008H3
NXR1	Ethernet1/13	SFP-1000BASE-T	SP7041-R	MTC1940038H
NXR1	Ethernet1/14	SFP-1000BASE-T	SP7041-R	MTC194008M8
NXR1	Ethernet1/15	SFP-1000BASE-T	SP7041-R	MTC194008HH
NXR1	Ethernet1/16	SFP-1000BASE-T	SP7041-R	MTC194008FJ
NXR1	Ethernet1/17	SFP-1000BASE-T	SP7041-R	MTC194008LR
NXR1	Ethernet1/18	SFP-1000BASE-T	SP7041-R	MTC194008JF
NXR1	Ethernet1/19	SFP-1000BASE-T	SP7041-R	MTC19400AP5
NXR1	Ethernet1/20	SFP-1000BASE-T	SP7041-R	MTC194008LV
NXR1	Ethernet1/21	SFP-1000BASE-T	SP7041-R	MTC194008HL
NXR1	Ethernet1/22	SFP-1000BASE-T	SP7041-R	MTC194008J3
NXR1	Ethernet1/23	SFP-1000BASE-T	SP7041-R	MTC194008MA
NXR1	Ethernet1/24	SFP-1000BASE-T	SP7041-R	MTC194008FN
NXR1	Ethernet1/25	SFP-1000BASE-T	SP7041-R	MTC194008MC
NXR1	Ethernet1/26	SFP-1000BASE-T	SP7041-R	MTC194008MB
NXR1	Ethernet1/27	SFP-1000BASE-T	SP7041-R	MTC194008H2
NXR1	Ethernet1/28	SFP-1000BASE-T	SP7041-R	MTC194008J5
NXR1	Ethernet1/29	SFP-1000BASE-T	SP7041-R	MTC19400B6K
NXR1	Ethernet1/30	SFP-1000BASE-T	SP7041-R	MTC19400851
NXR1	Ethernet1/31	SFP-1000BASE-T	SP7041-R	MTC194008JC
NXR1	Ethernet1/32	SFP-1000BASE-T	SP7041-R	MTC194008JP
NXR1	Ethernet2/1	SFP-1000BASE-T	SP7041-R	MTC194002QD
NXR1	Ethernet2/2	SFP-1000BASE-T	SP7041-R	MTC19400B6L
NXR1	Ethernet2/3	SFP-1000BASE-T	SP7041-R	MTC194008FM
NXR1	Ethernet2/4	SFP-1000BASE-T	SP7041-R	MTC194008LM
NXR1	Ethernet2/5	SFP-1000BASE-T	SP7041-R	MTC194002PQ
NXR1	Ethernet2/6	SFP-1000BASE-T	SP7041-R	MTC19400AN9
NXR1	Ethernet2/7	SFP-1000BASE-T	SP7041-R	MTC194008HT
NXR1	Ethernet2/8	SFP-1000BASE-T	SP7041-R	MTC194008LX
NXR1	Ethernet2/13	10Gbase-SR	FTLX8574D3BCL-CS	FNS220705DW
NXR1	Ethernet2/14	10Gbase-SR	FTLX8574D3BCL-CS	FNS220614DW

EQUIP	PORT	TIPUS	PART-NUMBER	NÚMERO DE SÈRIE
NXR1	Ethernet2/15	10Gbase-SR	FTLX8574D3BCL-CS	FNS220612GK
NXR1	Ethernet2/16	10Gbase-SR	FTLX8574D3BCL-CS	FNS2207065F
NXR2	Ethernet1/1	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A8B2
NXR2	Ethernet1/2	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A8BT
NXR2	Ethernet1/3	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A8BG
NXR2	Ethernet1/4	10Gbase-SR	FTLX8571D3BCL-C2	FNS19430JQU
NXR2	Ethernet1/5	10Gbase-SR	FTLX8571D3BCL-C2	FNS19430JQJ
NXR2	Ethernet1/6	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A1B4
NXR2	Ethernet1/7	Fabric Extender Transceiver	PLRXPL-VC-S43-CG	JUR1932B9DK
NXR2	Ethernet1/8	10Gbase-SR	SFBR-709SMZ-CS1	AVD1940A1BF
NXR2	Ethernet1/9	SFP-1000BASE-T	SP7041-R	MTC194008JR
NXR2	Ethernet1/10	SFP-1000BASE-T	SP7041-R	MTC19400625
NXR2	Ethernet1/11	SFP-1000BASE-T	SP7041-R	MTC194008LL
NXR2	Ethernet1/12	SFP-1000BASE-T	SP7041-R	MTC19400386
NXR2	Ethernet1/13	SFP-1000BASE-T	SP7041-R	MTC194003BY
NXR2	Ethernet1/14	SFP-1000BASE-T	SP7041-R	MTC1940060X
NXR2	Ethernet1/15	SFP-1000BASE-T	SP7041-R	MTC1940061W
NXR2	Ethernet1/16	SFP-1000BASE-T	SP7041-R	MTC19400626
NXR2	Ethernet1/17	SFP-1000BASE-T	SP7041-R	MTC194005ZK
NXR2	Ethernet1/18	SFP-1000BASE-T	SP7041-R	MTC194005WH
NXR2	Ethernet1/19	SFP-1000BASE-T	SP7041-R	MTC1940061Y
NXR2	Ethernet1/20	SFP-1000BASE-T	SP7041-R	MTC194005ZS
NXR2	Ethernet1/21	SFP-1000BASE-T	SP7041-R	MTC1940062R
NXR2	Ethernet1/22	SFP-1000BASE-T	SP7041-R	MTC19400395
NXR2	Ethernet1/23	SFP-1000BASE-T	SP7041-R	MTC19400628
NXR2	Ethernet1/24	SFP-1000BASE-T	SP7041-R	MTC1940064V
NXR2	Ethernet1/25	SFP-1000BASE-T	SP7041-R	MTC194003BD
NXR2	Ethernet1/26	SFP-1000BASE-T	SP7041-R	MTC1940061S
NXR2	Ethernet1/27	SFP-1000BASE-T	SP7041-R	MTC194005R6
NXR2	Ethernet1/28	SFP-1000BASE-T	SP7041-R	MTC194005UW
NXR2	Ethernet1/29	SFP-1000BASE-T	SP7041-R	MTC1940063S
NXR2	Ethernet1/30	SFP-1000BASE-T	SP7041-R	MTC19400617
NXR2	Ethernet1/31	SFP-1000BASE-T	SP7041-R	MTC1940032L
NXR2	Ethernet1/32	SFP-1000BASE-T	SP7041-R	MTC19400FV9
NXR2	Ethernet2/1	SFP-1000BASE-T	SP7041-R	MTC194005R8
NXR2	Ethernet2/2	SFP-1000BASE-T	SP7041-R	MTC1940063K
NXR2	Ethernet2/3	SFP-1000BASE-T	SP7041-R	MTC194005RH
NXR2	Ethernet2/4	SFP-1000BASE-T	SP7041-R	MTC19400636
NXR2	Ethernet2/5	SFP-1000BASE-T	SP7041-R	MTC1940062Z
NXR2	Ethernet2/6	SFP-1000BASE-T	SP7041-R	MTC194005RA
NXR2	Ethernet2/7	SFP-1000BASE-T	SP7041-R	MTC19400FQZ
NXR2	Ethernet2/8	SFP-1000BASE-T	SP7041-R	MTC1940062K
NXR2	Ethernet2/13	10Gbase-SR	FTLX8574D3BCL-CS	FNS2207065B

EQUIP	PORT	TIPUS	PART-NUMBER	NÚMERO DE SÈRIE
NXR2	Ethernet2/14	10Gbase-SR	FTLX8574D3BCL-CS	FNS2207065D
NXR2	Ethernet2/15	10Gbase-SR	FTLX8574D3BCL-CS	FNS2207062X
NXR2	Ethernet2/16	10Gbase-SR	FTLX8574D3BCL-CS	FNS22070640

En total són 43 convertidors del tipus *10Gbase-SR*, 4 del tipus *Fabric Extender Transceiver* i 131 del tipus *SFP-1000BASE-T*.

Barcelona, 15 d'octubre de 2019

El cap de la Secció d'Explotació i Sistemes

Fulgencio Giménez Sanchiz