Treball fi de Màster

Pla Director de Seguretat de la Informació

Juanjo Carrasco Puy

2019

Programa: Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)

Àrea: Sistemes de Gestió de la Seguretat de la Informació

Consultor: Arsenio Tortajada Gallego

Professor responsable de l'assignatura:

Centre: Universitat Oberta de Catalunya (www.uoc.edu)

Data Lliurament: 7 de juny de 2019

AGRAÏMENTS:

Un cop arribat fins aquí, vull agrair el suport incondicional als meus pares que durant la meva etapa d'estudiant d'ETIG (Enginyeria Tècnica en Informàtica de Gestió) van ajudar-me cuidant de la meva filla Vanessa per a que pogués entregar a temps les PACs.

No vull deixar d'agrair les forces i l'acompanyament de «la Moreneta», figura clau en els moments d'exàmens i notes finals; *Ho sé, aniré a veure't per complir amb les promeses fetes durant tot aquest cicle d'estudiant*.

Alberto Durán, han estat molts sopars, whiskies i sessions de coaching i gràcies a tot això ara sóc qui sóc. Moltes gràcies pel teu suport company !!!

També vull agrair el suport incondicional a la Gemma Marí que sempre m'ha animat a continuar i a acabar el Màster; *El meu èxit és el teu èxit*.

Finalment no vull deixar de banda tots aquells que per algun motiu o per un altre no van creure que això fos possible. A tots ells; *Para tener éxito, tus deseos de triunfar deberían ser más grandes que tu miedo de fracasar – Bill Cosby (12 de Juliol de 1937, Philadelphia, Pennsylvania, USA).*

Una vez llegado aquí, quiero agradecer el soporte incondicional a mis padres que durante mi etapa de estudiante de ITIG (Ingeniería Técnica en Informática de Gestión) me ayudaron cuidando de mi hija Vanessa para que pudiera entregar a tiempo las PACs.

No quiero dejar de agradecer las fuerzas y el acompañamiento de «la Moreneta», figura clave en los momentos de exámenes y notas finales; *Lo sé, iré a verte para cumplir con las promesas hechas durante este ciclo de estudiante*.

Alberto Durán, han sido muchas cenas, whiskies y sesiones de coaching y gracias a todo eso ahora soy quien soy. Muchas gracias por tu apoyo compañero !!!

También quiero agradecer el soporte incondicional a Gemma Marí que siempre me ha animado a continuar y a acabar el Máster; *Mi éxito es tu éxito*.

Finalmente no quiero dejar de banda a todos aquellos que por algún motivo u otro no creyeron que esto fuera posible. A todos ellos; *Para tener éxito, tus deseos de triunfar deberían ser más grandes que tu miedo de fracasar – Bill Cosby (12 de Juliol de 1937, Philadelphia, Pennsylvania, USA).*

FITXA DEL TREBALL FINAL

Títol del treball	Treball fi de Màster
Nom de l'autor	Juanjo Carrasco Puy
Nom del consultor/a	Arsenio Tortajada Gallego
Nom del PRA	Pla Director de Seguretat de la Informació
Data de lliurament (mm/aaaa):	05/2019
Titulació o programa	Màster InterUniversitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions (MISTIC)
Àrea del Treball Final	Sistemes de Gestió de la Seguretat de la Informació
Idioma del treball	Català
Paraules clau	SGSI, Seguretat, ISO 27001

Resum del Treball (màxim 250 paraules)

Aquest Treball de Fi de Màster pertany als estudis del Màster InterUniversitari de Seguretat de les Tecnologies de la Informació i les Comunicacions (abreviat MISTIC).
L'objectiu del projecte és l'elaboració d'un Pla Director de Seguretat per una consultora TI, anomenada manera fictícia **SCRIPTIX**.
El Pla Director de Seguretat s'emmarca dins la norma ISO/IEC 27001:2013, i els codis de bones pràctiques esmentats en la ISO/IEC 27002:2013, que estableixen les especificacions per implementar, gestionar, supervisar i millorar un Sistema de Gestió de Seguretat de la Informació (SGSI). S'ha realitzat un anàlisi de la situació actual de la seguretat en l'àmbit de les Tecnologies de la Informació i la Comunicació, per tal de poder definir uns objectius a curt i llarg termini i proposar un conjunt de projectes per tal d'arribar-hi. Dins d'aquest anàlisi realitzat podem destacar l'anàlisi diferencial, l'anàlisi de riscos (utilitzant MAGERIT com a metodologia) i l'anàlisi de compliment de la ISO. Els progressos aconseguits en la implantació del SGSI són:

- Precisar l'estat de la seguretat de la informació actual en relació als diferents aspectes de la norma (GAP) i fixar l'abast i objectius.
- Establir una base documental i determinar les responsabilitats de cada un dels components de l'estructura organitzativa de seguretat, de manera que s'asseguri la realització de totes les tasques necessàries i proporcionar Revisió i Millora.
- Identificar i inventariar els actius crítics de l'organització, determinar la magnitud de les amenaces i, en darrer terme, concretar els riscos als que estan exposats els diferents elements dels Sistemes d'Informació de l'organització.
- A partir dels riscos trobats, s'han seleccionat i prioritzat un seguit de projectes i mesures que permetran millorar la seguretat de l'organització.

Abstract (in English, 250 words or less)

This final Master studies belongs to the Inter-University Master's Degree in Information

Technology and Communications Security (MISTIC abbreviated) studies.
The objective of the project is the development of a Security Master Plan for an IT consultancy, called the **SCRIPTIX** fictional way.
The Security Master Plan is part of the ISO / IEC 27001: 2013 standard, and codes of good practices mentioned in the ISO / IEC 27002: 2013, which establish the specifications for implementing, managing, monitoring and improving a Management System of Information Security (ISMS). An analysis of the current security situation in the field of Information Technology and Communication has been carried out in order to define short and long term goals and propose a set of projects to reach -his Within this analysis we can highlight the differential analysis, the analysis of risks (using MAGERIT as a methodology) and the analysis of compliance with the ISO. The progress achieved in the implementation of the ISMS are:

- Identify the state of the security of the current information in relation to the different aspects of the standard (GAP) and set the scope and objectives.
- Establish a documentary base and determine the responsibilities of each of the components of the organizational security structure, in such a way that it ensures the accomplishment of all the necessary tasks and provide Review and Improvement.
- Identify and inventory the critical assets of the organization, determine the magnitude of the threats and, ultimately, specify the risks to which the different elements of the Information Systems of the organization are exposed.
- Based on the risks found, a series of projects and measures have been selected and prioritized that will allow to improve the security of the organization.

Sumari

Índex de taules

Índex de figures

Introducció

A continuació es donarà una breu descripció de les normes ISO/IEC 27001 i ISO/IEC 27002 que es faran servir com a base en el desenvolupament d'aquest estudi.

La norma **ISO/IEC 27001** és un estàndard per a la seguretat de la informació (Information technology - Security techniques - Information security management systems – Requirements) aprovat i publicat com estàndard internacional en octubre del 2005 per la International Organization for Standardization (les seves sigles en anglès - ISO) i per la comissió International Electrotechnical Commission (les seves sigles en anglès - IEC).

Aquesta norma especifica els requeriments necessaris per establir, implantar, mantenir i millorar la gestió de la seguretat de la informació (SGSI) segons els conegut com a «Cicle de Deming»: PDCA – acrònim de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Fer, Verificar i Actuar). És consistent amb les millors pràctiques descrites en la ISO/IEC 27002, anteriorment coneguda com ISO/IEC 17799, amb orígens en les normes BS 7799-2:2002, desenvolupada per la entitat de normalització britànica, la *British Standards Institution* (les seves sigles en anglès – BSI).

La norma ISO/IEC 27001 és certificable, mentre que la norma ISO/IEC 27002 és en general un conjunt de bones pràctiques i controls suggerits. La versió més recent de la ISO/IEC 27002 és la ISO/IEC 27002:2013.

Contextualització

Descripció de l'organització objecte de l'estudi

La empresa seleccionada objecte del Pla Director de Seguretat de la Informació basat en la implementació i compliment de la norma ISO/IEC 27001:2013 i en els controls normatius de la ISO/IEC 27002, a partir d'ara EMPRESA, és una companyia dedicada a la consultoria i l'outsourcing. Està organitzada per sectors econòmics; banca, assegurança, industria, sector public, aeroespacial i defensa, telecomunicacions, entre altres.

Activitat i entorn

La empresa SCRIPTIX compte avui en dia amb més de 20 anys d'experiència en el sector IT i d'Outsourcing. Atès que el seu àmbit d'actuació està diversificat per sectors, la seva activitat està subjecta a les normatives legals d'aplicació en funció del sector; Banca, Assegurances, Aeroespacial i Defensa, Sector Public, etc.

El sector financer a nivell mundial és el que compte amb les mesures més estrictes pel que fa a la normativa en el tractament de la informació personal de clients. Algunes normatives d'aplicació al tractament d'informació personal són PCI-DSS (**P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard) i GDPR (**G**eneral **D**ata **P**rotection **R**egulation) i d'altres d'aplicació general com Basilea III i PSD2 (**P**ayment **S**ervices **D**irective 2).

Les normes de seguretat de dades de la industria de les targetes de pagament (PCI-DSS) es van desenvolupar per a fomentar i millorar la seguretat del titula de la targeta i facilitar l'adopció de mesures de seguretat uniformes a nivell mundial. Les PCI-DSS proporcionen una referencia de requeriments tècnics i operatius desenvolupats per a protegir les dades dels titulars de les targetes. Les PCI-DSS s'apliquen a totes les entitats que participen en el processament de targetes de pagament, entre els que s'inclouen comerciants, processadors, adquirents, entitats emissores i proveïdors de serveis, com també totes les demés entitats que emmagatzemen, processen o transmeten CHD (dades del titular de la targeta) o SAD (dades d'autentificació confidencials).

Les PCI-DSS constitueixen un conjunt mínim de requeriments per a protegir les dades dels titulars de les targetes i es poden millorar mitjançant controls i pràctiques addicionals a fi de mitigar altres riscos.

El Reglament (UE) 2016/679 (RGDPR), és el reglament europeu relatiu a la protecció de les persones físiques pel que fa al tractament de les seves dades personals i a la lliure circulació d'aquestes dades. Va entrar en vigor el 25 de maig del 2016 i va se d'aplicació el 25 de maig del 2018, dos anys mitjançant els quals les empreses, organitzacions, els organismes i les institucions han hagut d'adaptar-se de manera gradual per al seu compliment. És una normativa a nivell de la Unió Europea i les multes per el no compliment del RGDPR pot arribar als 20 milions d'euros.

En Espanya, el RGDPR va deixar obsoleta la Llei Orgànica de Protecció de dades de Caràcter Personal (LOPD) de 1999, essent substituïda el 6 de desembre del 2018 per la Llei Orgànica de Protecció de Dades i Garantia dels Drets Digitals, concorde el RGDP.1.

Com s'ha comentat anteriorment la EMPRESA presta serveis IT i d'Outsourcing al sector financer amb el que li són properes les normatives de PCI-DSS i GDPR i li són d'aplicació en el desenvolupament d'aplicacions informàtiques i serveis que tracten amb informació personal de clients.

Mida i estructura de l'organització

La EMPRESA compte avui en dia amb més de 21.000 professionals i amb presència a 17 països d'Àsia-Pacífic, Orient Mitjà, Europa, Amèrica Llatina i Amèrica del Nord i una facturació de 1.173 milions d'euros (1.173 M€)

El creixement de la EMPRESA va vindre al 2015 de la unió amb el grup REDOX, la vuitena companyia de serveis IT del món.

El Consell d'Administració de la EMPRESA està format per un president, un conseller delegat a més de sis consellers delegats de REDOX i quatre consellers independents.

Pel que fa a la seguretat, la EMPRESA disposa d'una Àrea de Seguretat Corporativa. Aquesta àrea és l'encarregada de dirigir la Seguretat Corporativa en tota la companyia. Aquesta àrea no presta servei a clients externs, el seu client directe és la EMPRESA. Per això forma part de l'Àrea de Suport a Negoci (BSA – Business Support Area en anglès).

L'Àrea de Seguretat Corporativa està dirigida per un *Chief Information Security Officer* (CISO). Les responsabilitats del CISO són:

- Liderar l'àrea de Seguretat Corporativa de la companyia
- Supervisar les activitats relacionades amb la seguretat corporativa de la EMPRESA, segons l'establert en la política de seguretat corporativa de la EMPRESA

- Liderar el Comitè de Seguretat Corporativa de la EMPRESA

Addicionalment el CISO és responsable de les mesures de seguretat per a la protecció de dades personals de tota la companyia.

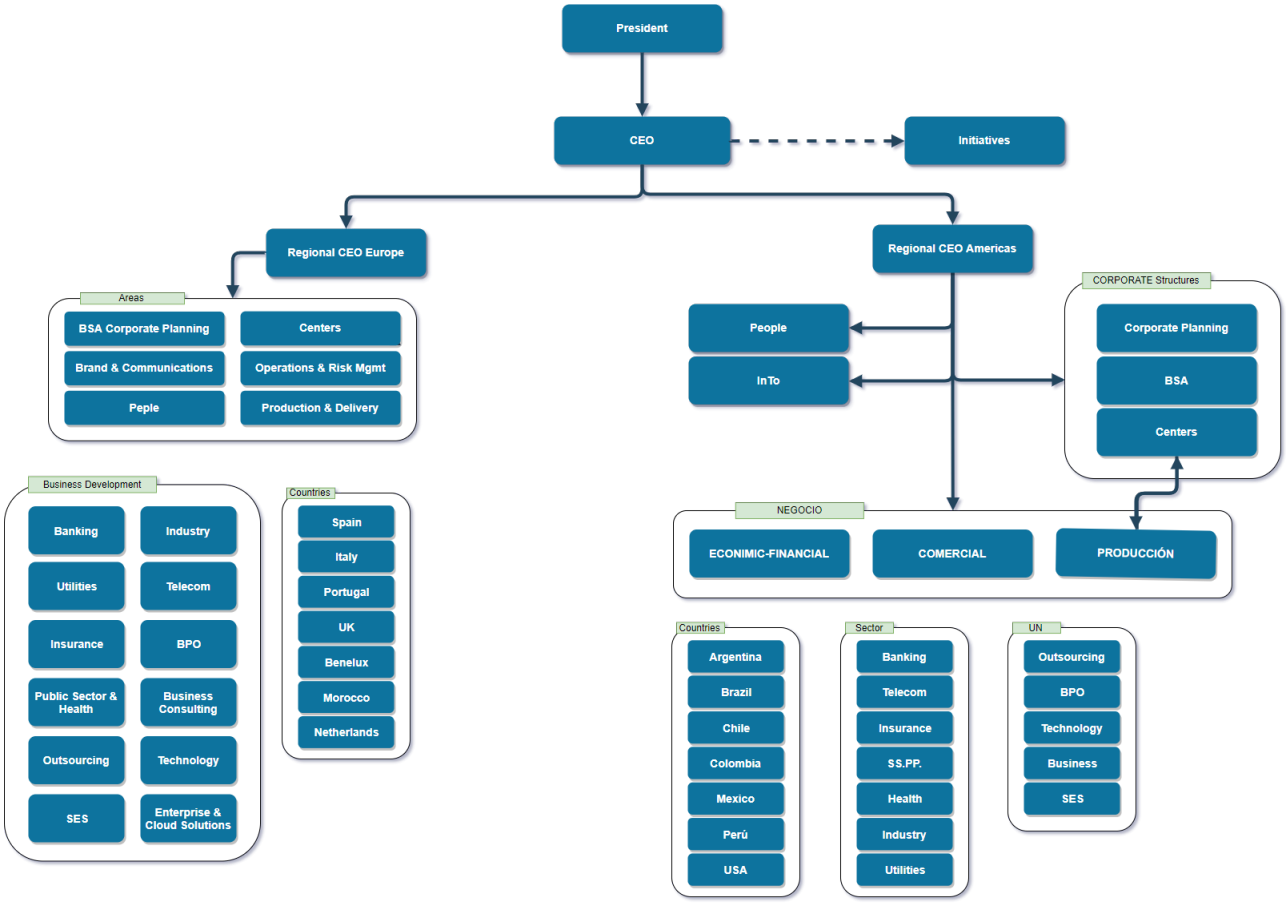


Figura 1: Organigrama EMPRESA

President: President del grup REDOX

CEO: Director executiu de grup REDOX

Initiatives: Unitat de negoci estratègica que promou la emprenedoria i el talent dintre del grup REDOX

Regional CEO: Director executiu. Dintre del grup la direcció executiva es reparteix entre la regió d'Europa i d'Amèrica.

Àrees:

- *BSA Corporate Planning*: Àrea cross de suport a negoci.
- *Brand & Communications*: Informació i comunicació amb els mitjans.
- People: Recursos Humans i gestió de tot el personal
- Centers: Software factories en modalitats in-shore, near-shore i far-shore
- Operation Risk & Management: Administració del risc operacional de la companyia
- Production & Delivery: Producció
- Business Development: Desenvolupament de software

Atès que el negoci principal de SCRIPTX és el desenvolupament de solucions, l'àrea de *Business Development* s'organitza en funció del sector aconseguint així especialització i coneixement a nivell de sector.

Localització

SCRIPTIX està present en 17 països repartits en dos grans regions; Europa i Amèrica. La seu es troba a Madrid i disposa de centres en:

- Andorra
- Argentina
- Bèlgica
- Brasil
- Chile
- Colombia
- Italia
- Luxemburg
- Mèxic
- Marroc
- Holanda
- Perú
- Portugal

- Espanya
- Suïssa
- UK
- USA

Figura 2: Mapa presència SCRIPTIX

IT Infraestructures

Els elements dels que disposa SCRIPTIX a nivell de Tecnologies de la Informació i Comunicacions s'han categoritzat en:

- Sistemes
- CPDs
- Xarxes de comunicacions

- Worksatations i desktops

Sistemes

SCRIPTX disposa de servidors tant a nivell virtual, físic i en cloud. Les infraestructures que donen suport als sistemes són;

- Windows 2016 Server
- Windows 7 i Windows 10
- IBM Aix 7.2.
- IBM AS/400 V7R3

Aquestes infraestructures donen suport a tota l'àrea de negoci, tant interna com a nivell de *Business Develpment*.

Pel que fa als sistemes cloud, es disposa dels següents serveis;

- Unitat d'emmagatzematge al núvol (similar a DROPBOX)
- Servidor Exchange de correu corporatiu

Addicionalment també es disposa de servidors d'aplicacions. Els servidors d'aplicacions que donen suport a negoci son;

- IIS (Internet Information Service)
- Apache / Tomcat 8
- BEA WebLogic 12c Release 3 (12.1.3)
- IBM WebSphere Application Server (WAS) 8.5

Les bases de dades que donen suport als sistemes esmentats anteriorment així com a les àrees de tota la companyia son;

- Oracle
- SQL Server

- MySQL (per a aplicacions departamentals)
- Informix
- Access (per aplicacions d'usuari locals)

CPDs

SCRIPTIX disposa de 4 CPDs ubicats a Madri i Barcelona. Cada un dos CPDs disposa de la seva rèplica de contingència en mode Actiu / Passiu ubicades a centres diferents dels CPD principals.

Els CPDs disposen doble comesa elèctrica, mesures de seguretat en cas d'incendi o inundació; drenatges, extintors, vies d'evacuació, portes ignífugues, etc.

Pel que fa a la seguretat física, els CPDs disposen de:

- Panys electromagnètics
- Torniquets
- Càmeres de seguretat
- Detectors de moviment
- Targetes d'identificació

Xarxes de comunicacions

Les xarxes de comunicacions són gestionades des de les ubicacions des de els servidors ubicats als diferents CPDs. Les directives son gestionades íntegrament des de el centre de Madrid.

La xarxa de dades disposa de sis tallafocs (3 principals i 3 redundants).

A nivell global (donada la complexitat de la infraestructura) la topologia de xarxa de SCRIPTIX és la següent.

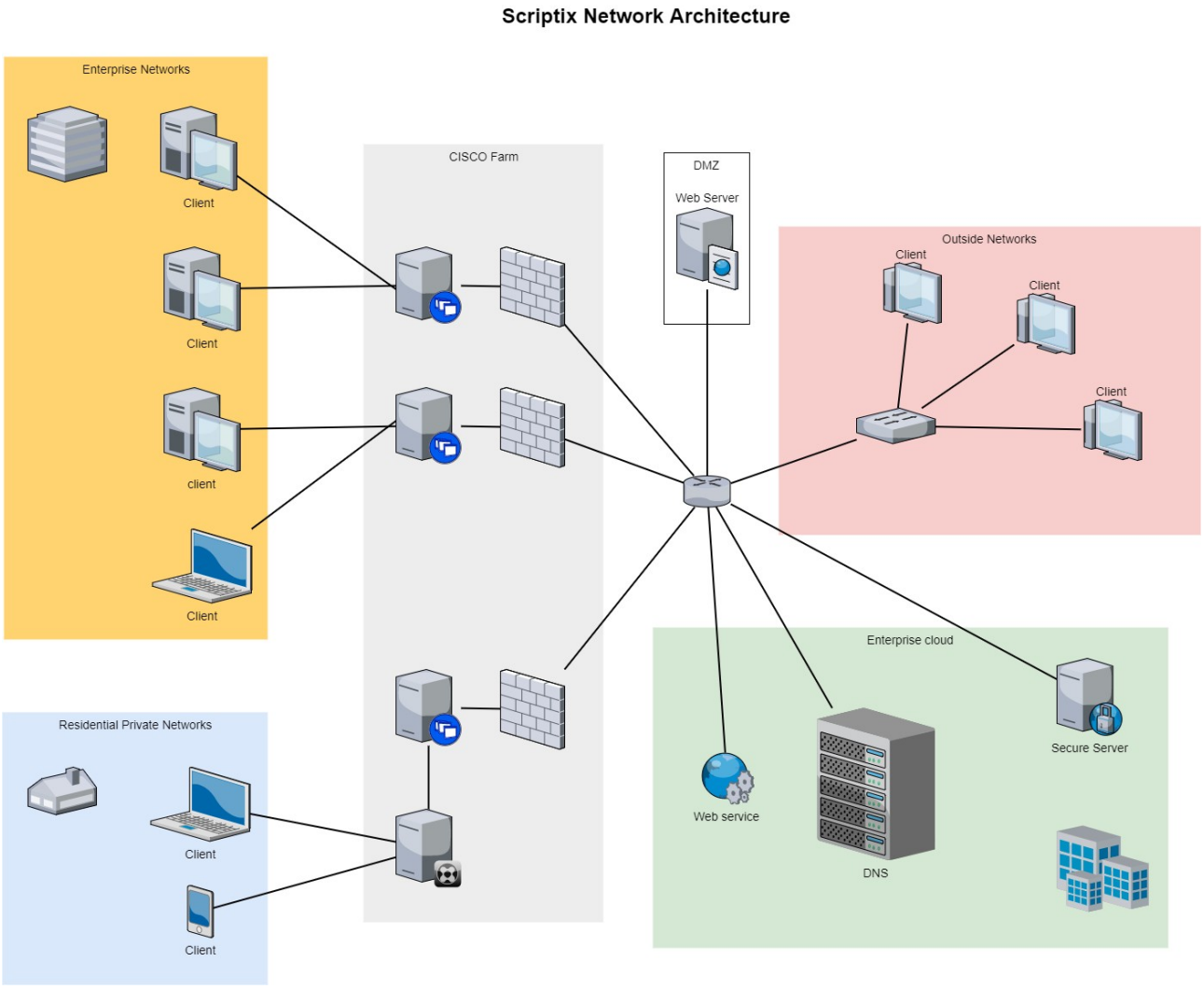


Figura 3: Topologia xarxa SCRIPTIX

WorkStation i Desktop

Tots els empleats disposen d'ordinador portàtil. Excepcionalment i només per requeriments de projecte, es disposa de ordinadors de sobretaula.

La plantilla corporativa de portàtils és Windows 7 i Windows 10. Cada 3 anys es du a terme, per política corporativa, la migració dels equips als empleats.

La validació de les credencials d'accés (usuari/contrasenya) es fa mitjançant Active Directory. Si l'inici e sessió es fa fora de la xarxa corporativa, es requereix OPT que s'envia al dispositiu mòbil associat a l'usuari.

Tots els equips disposen de VPN (Virtual Private Network) per a la connexió a la xarxa corporativa, cosa que permet el tele-treball.

Dispositius mòbils

A partir de la categoria PL (Project Leader) els usuaris disposen de telèfon corporatiu amb sistema operatiu Android. Els gerents, directors i socis disposen de iPhone.

En cas de requeriments de projecte, la resta de personal pot demanar l'assignació d'un telèfon mòbil. Inicialment el telèfon assignat serà Android.

Definició dels objectius del Pla Director de Seguretat

El Pla Director de Seguretat com a *road map* que ha de seguir la EMPRESA per aconseguir gestionar de forma adequada la seguretat, tindrà com abast els diferents projectes que per la seva naturalesa tracten dades personals de clients.

Els objectius del Pla Director de Seguretat seran els següents:

1) Garantir la confidencialitat, integritat i disponibilitat de la informació personal de clients propietat del client per al que la EMPRESA presta servei
2) Establir de manera clara els requeriments de seguretat que la EMPRESA ha de complir a fi de garantir la protecció de la informació front les diferents amenaces a las que està exposada, minimitzant d'aquesta manera els riscos i complint amb les seves obligacions vers els seus clients
3) Realitzar un anàlisis diferencial de l'estat actual de la seguretat dels actius versus el compliment de la norma ISO/IEC 27001 i ISO/IEC 27002, per a que a partir d'aquest anàlisi s'identifiquin els recursos necessaris i puguin establir-se els plans de treball adients

Sistemes d'informació que donen suport a l'organització

Addicionalment a tots els sistemes d'informació transversals que donen suport a l'organització tal com Servidors de Base de Dades, Cabines d'emmagatzematge, Recursos compartits de xarxa, Ethernet, Proxies, Firewalls, Routers, Sharepoint, etc., els treballadors disposen de portàtil per a la realització de la seva feina.

Les característiques dels portàtils que fan servir els empleats són:

- Ordinador Dell i5 amb 8Gb de memòria RAM i HD de 69Gb
- Sistema Operatiu Windows 7 Enterprise / Windows 10 Enterprise
- Suite Office instal·lada amb llicència corporativa
- Antivirus McAfee
- Missatgeria instantània amb Microsoft LYNC
- Aplicació VPN *CISCO Systems VPN Client*
- Navegador web *Internet Explorer*

Pel que fa a les polítiques de seguretat cal considerar (es citen les més importants):

- L'usuari de domini és administrador en local
- Es permet la instal·lació de programari
- No existeix programari Firewall en local. El firewall de Windows està desactivat
- L'equip disposa de ports USB
- Es permet l'accés a la RAM i el canvi de la seqüència del Boot

Els usuaris utilitzen els seus equips personals per a les tasques que tenen encomanades, bé sigui programació d'aplicacions, gestió de la demanada amb el client mitjançant correu electrònic, ús de fulles de càlcul amb Microsoft Excel, realització d'informes amb Microsoft PowerPoint, etc. Tota aquesta documentació en la majoria dels casos és enviada a client.

Addicionalment també es permet la instal·lació de programari lliure per a l'accés a Base de Dades (p.e. SQL Developer), accés FTP (WinSCP), accés a terminal TTY (p.e. Putty), etc. Mitjançant aquestes aplicacions també s'accedeix als sistemes d'informació del client.

Podem resumir que l'abast del *Pla Director de Seguretat de la Informació* seran els actius assignats al personal que executa un projecte determinat i que per la pròpia naturalesa del projecte és necessari l'accés a sistemes d'informació del client i el tractament de dades personals de clients.

Anàlisi diferencial

Anàlisi diferencial de l'estat actual versus ISO/IEC 27001 i ISO/IEC 27002

Donada la naturalesa del negoci on l'execució de projectes informàtics pot portar associada la gestió de dades personals de clients, és necessari la avaluació dels punts de control establers en la ISO 27002:2013.

A continuació s'annexa la taula amb la llista de controls de seguretat de la ISO 27002:2013 en el que es relaciona el nivell de compliment del control a través d'un percentatge i unes observacions sobre els controls no avaluats.

A continuació es mostra la taula amb l'avaluació dels diferents controls de seguretat sota la norma ISO/IEC 27002:2013.

AUDITORIA EN SEGURIDAD DE LA INFORMACIÓN		CRITERIOS DE EVALUACIÓN	
		No realizado	0 %
		Realizado informalmente	20 %
Herramienta de Evaluacion y Diagnostico bajo la Norma ISO/IEC 27002:2013		Planificado	40 %
		Bien definido	60 %
		Cuantitativamente controlado	80 %
		Mejora continua	100 %
Norma	**Seccion**	**Cumplimiento**	
5	**POLITICAS DE SEGURIDAD**	**80 %**	
5,1	**Directrices de la Dirección en seguridad de la información**	**80 %**	
5.1.1	Conjunto de políticas para la seguridad de la información	**Cuantitativamente controlado**	80 %
5.1.2	Revisión de las políticas para la seguridad de la información	**Cuantitativamente controlado**	80 %
8	**GESTION DE ACTIVOS**	**44 %**	
8,1	**Responsabilidad sobre los Activos**	**65 %**	
8.1.1	Inventario de activos.	**Cuantitativamente controlado**	80 %
8.1.2	Propiedad de los activos.	**Cuantitativamente controlado**	80 %
8.1.3	Uso aceptable de los activos.	**Realizado informalmente**	20 %
8.1.4	Devolución de activos.	**Cuantitativamente controlado**	80 %
8,2	**Clasificacion de la Informacion**	**0 %**	
8.2.1	Directrices de clasificación.	**No realizado**	0 %
8.2.2	Etiquetado y manipulado de la información.	**No realizado**	0 %
8,3	**Manejo de los soportes de almacenamiento**	**67 %**	
8.3.1	Gestión de soportes extraíbles.	**Bien definido**	60 %
8.3.2	Eliminación de soportes.	**Bien definido**	60 %
8.3.3	Soportes físicos en tránsito	**Cuantitativamente controlado**	80 %
9	**CONTROL DE ACCESO**	**65 %**	
9,1	**Requisitos de negocio para el control de accesos**	**80 %**	
9.1.1	Política de control de accesos.	**Cuantitativamente controlado**	80 %
9.1.2	Control de acceso a las redes y servicios asociados.	**Cuantitativamente controlado**	80 %
9,2	**Gestión de acceso de usuario.**	**48 %**	
9.2.1	Gestión de altas/bajas en el registro de usuarios.	**Bien definido**	60 %
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	**Bien definido**	60 %
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	**Cuantitativamente controlado**	80 %
9.2.5	Revisión de los derechos de acceso de los usuarios.	**Realizado informalmente**	20 %
9.2.6	Retirada o adaptación de los derechos de acceso	**Realizado informalmente**	20 %
9,4	**Control de acceso a sistemas y aplicaciones**	**68 %**	
9.4.1	Restricción del acceso a la información.	**Cuantitativamente controlado**	80 %
9.4.2	Procedimientos seguros de inicio de sesión.	**Mejora continua**	100 %
9.4.3	Gestión de contraseñas de usuario.	**Mejora continua**	100 %
9.4.4	Uso de herramientas de administración de sistemas.	**Planificado**	40 %
9.4.5	Control de acceso al código fuente de los programas	**Realizado informalmente**	20 %
11	**SEGURIDAD FISICA Y AMBIENTAL**	**62 %**	
11,1	**Areas Seguras**	**63 %**	
11.1.1	Perímetro de seguridad física.	**Cuantitativamente controlado**	80 %
11.1.2	Controles físicos de entrada.	**Cuantitativamente controlado**	80 %
11.1.3	Seguridad de oficinas, despachos y recursos.	**Cuantitativamente controlado**	80 %
11.1.4	Protección contra las amenazas externas y ambientales.	**Bien definido**	60 %
11.1.5	El trabajo en áreas seguras.	**Bien definido**	60 %
11.1.6	Áreas de acceso público, carga y descarga	**Realizado informalmente**	20 %
11,2	**Seguridad de los Equipos**	**60 %**	
11.2.1	Emplazamiento y protección de equipos.	**Cuantitativamente controlado**	80 %
11.2.2	Instalaciones de suministro.	**Bien definido**	60 %
11.2.3	Seguridad del cableado.	**Cuantitativamente controlado**	80 %
11.2.4	Mantenimiento de los equipos.	**Bien definido**	60 %
11.2.5	Salida de activos fuera de las dependencias de la empresa.	**Planificado**	40 %
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	**Cuantitativamente controlado**	80 %
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	**Cuantitativamente controlado**	80 %
11.2.8	Equipo informático de usuario desatendido.	**No realizado**	0 %
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	**Bien definido**	60 %
12	**SEGURIDAD EN LA OPERATIVA**	**80 %**	
12,2	**Protección contra código malicioso**	**100 %**	
12.2.1	Controles contra el código malicioso.	**Mejora continua**	100 %
12,3	**Copias de seguridad**	**60 %**	
12.3.1	Copias de seguridad de la información	**Bien definido**	60 %
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**	**48 %**	
13,1	**Gestión de la seguridad en las redes.**	**60 %**	
13.1.1	Controles de red.	**Planificado**	40 %
13.1.2	Mecanismos de seguridad asociados a servicios en red.	**Bien definido**	60 %
13.1.3	Segregación de redes.	**Cuantitativamente controlado**	80 %
13,2	**Intercambio de información con partes externas.**	**35 %**	
13.2.1	Políticas y procedimientos de intercambio de información.	**Realizado informalmente**	20 %
13.2.2	Acuerdos de intercambio.	**Planificado**	40 %
13.2.3	Mensajería electrónica.	**Planificado**	40 %
13.2.4	Acuerdos de confidencialidad y secreto	**Planificado**	40 %
14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**	**40 %**	
14,2	**Seguridad en los procesos de desarrollo y soporte**	**40 %**	
14.2.1	Política de desarrollo seguro de software.	**Realizado informalmente**	20 %
14.2.6	Seguridad en entornos de desarrollo.	**Bien definido**	60 %
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	**Realizado informalmente**	20 %
14.2.9	Pruebas de aceptación	**Bien definido**	60 %

Tabla 1: Avaluació Controls Seguretat

Les següents gràfiques mostren el nivell de maduresa percentual dels diferents controls. Amb aquesta informació s'obté una visió de l'estat de la seguretat en conjunt.

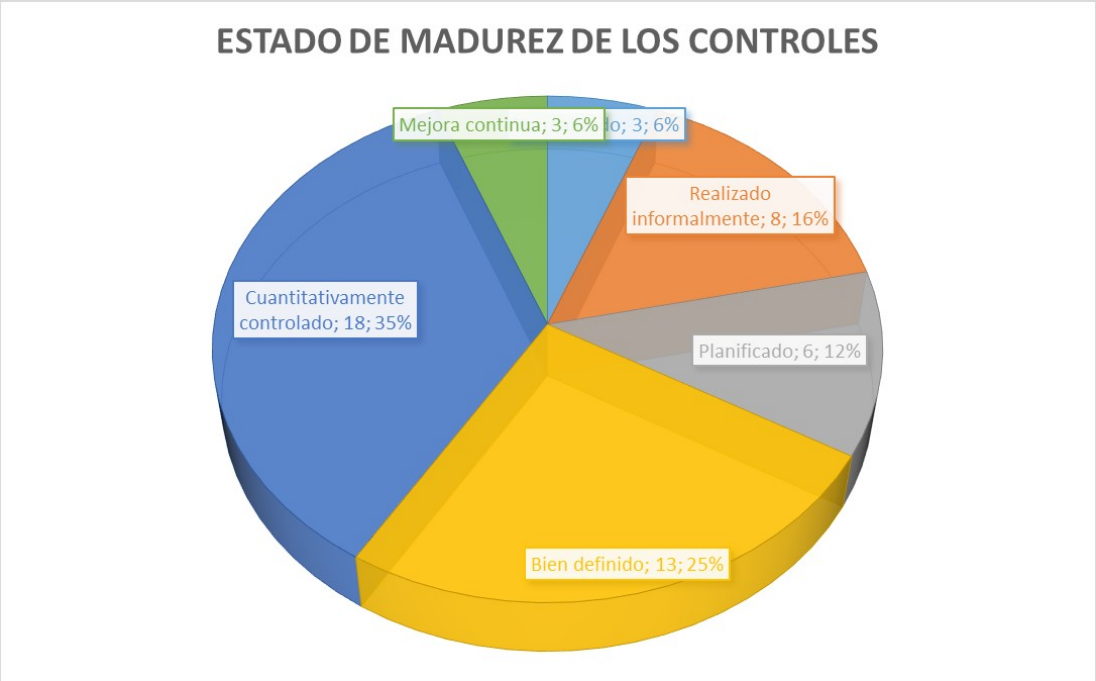


Figura 4: Maduresa CMM dels controls ISO

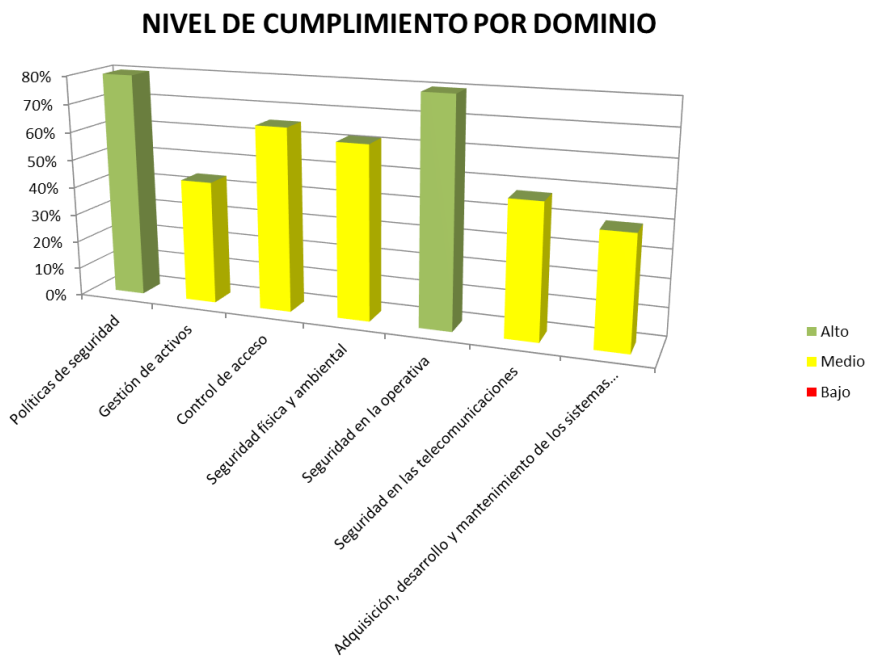


Figura 5: Nivell de compliment per domini - 1

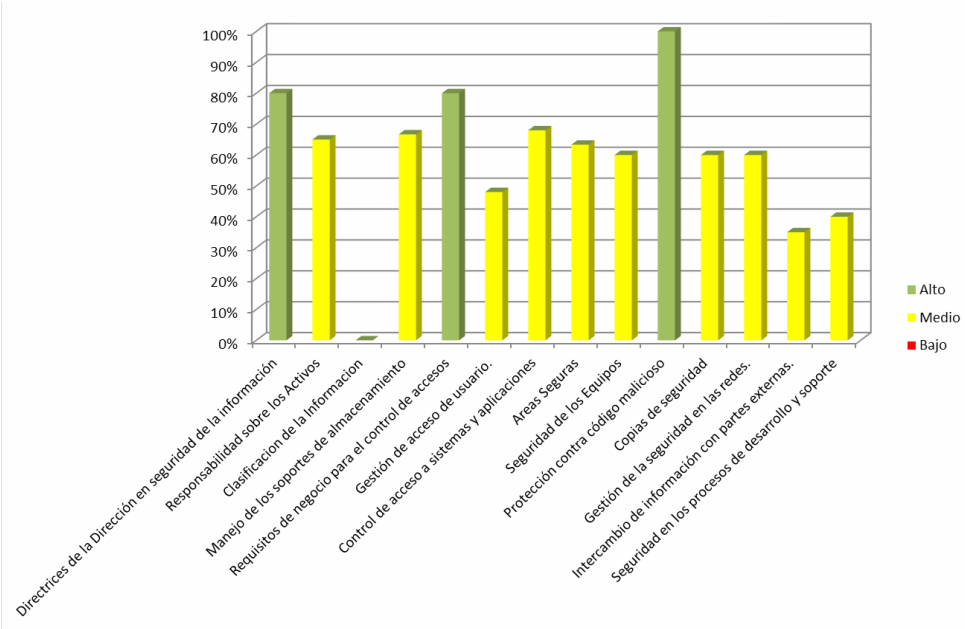


Figura 6: Nivell de compliment per domini - 2

En termes generals es pot determinar que el compliment general de l'estat dels controls de seguretat de la EMPRESA és del 60% i es reparteix de la següent manera;

- 5 Polítiques de seguretat 80%
- 8 Gestió d'actius 44%
- 9 Control d'accés 65%
- 11 Seguretat física i ambiental 62%
- 12 Seguretat en la operativa 80%
- 13 Seguretat en les telecomunicacions 48%
- 14 Adquisició, desenvolupament i manteniment dels sistemes d'informació 40%

El següent quadre il·lustra les dades indicades anteriorment.

Norma	Dominios	Estado
5	Políticas de seguridad	80 %
8	Gestión de activos	44 %
9	Control de acceso	65 %
11	Seguridad física y ambiental	62 %
12	Seguridad en la operativa	80 %
13	Seguridad en las telecomunicaciones	48 %
14	Adquisición, desarrollo y mantenimiento de los sistemas de información	40 %
Cumplimiento General		60 %

Tabla 2: Compliment general

Es determina que la catalogació dels dominis entre Alt, Mitjà i Baix queda de la següent manera;

Dominios	Bajo	Medio	Alto
Políticas de seguridad	0 %	0 %	80 %
Gestión de activos	0 %	44 %	0 %
Control de acceso	0 %	65 %	0 %
Seguridad física y ambiental	0 %	62 %	0 %
Seguridad en la operativa	0 %	0 %	80 %
Seguridad en las telecomunicaciones	0 %	48 %	0 %
Adquisición, desarrollo y mantenimiento de los sistemas de información	0 %	40 %	0 %

Tabla 3: Catalogació dels dominis

Resultats de Anàlisis diferencial ISO/IEC 27002:2013

A continuació es dona un anàlisis detallat del GAP en funció dels resultats obtinguts.

Directrius de la Direcció en seguretat de la informació (5.1)

Un document anomenat «política» és aquell que expressa la intenció i instrucció global en la manera que formalment ha estat expressada per la Direcció de l'organització.

El contingut de les polítiques es basa en el context en el que opera una organització i solen ser considerades en relació amb els objectius de la organització, les estratègies adoptades per assolir els objectius, la estructura i els processos adoptats per l'organització, els objectius generals i específics relacionats amb el tema de la política i requeriments de les polítiques procedents de nivells més superiors (legals d'obligat compliment, del sector al que pertany l'organització, de la pròpia organització de nivells superiors o més amplis, ...) relacionades.

La gerència haurà d'establir de forma clara les línies de la política d'actuació i manifestar el seu recolzament i compromís a la seguretat de la informació, publicant i mantenint polítiques de seguretat en tota la organització.

Segons l'anàlisi el compliment del control 5.1 és del 80%, és a dir, els controls de seguretat de la informació estan subjectes a verificació per establir el seu niell d'efectivitat.

Responsabilitats sobre els actius (8.1)

Tots els actius haurien d'estar justificats i tenir assignat un propietari i s'hauria d'identificar als propietaris per a tots els actius i assignar-lis la responsabilitat del manteniment dels controls adequats.

La implantació dels controls específics podria ser delegada pel propietari. Tot i això, el propietari roman com a responsable de l'adequada protecció dels actius.

En aquest cas l'anàlisi determina que la implantació d'aquest control és de només del 65%, és a dir, entre el criteri de classificació «Ben definit» i «Quantitativament controlat».

Classificació de la informació (8.2)

La informació te diversos graus de sensibilitat i criticitat. Alguns ítems podrien requerir nivells de protecció addicionals o un tractament especial. Hauria d'utilitzar-se un esquema de classificació de la informació per a definir el conjunt adequat de nivells de protecció i comunicar la necessitat de mesures especials per al seu tractament.

La qualificació d'aquest ítem és 0% atès que es desconeix si existeix tal qualificació.

Maneig dels suports d'emmagatzematge (8.3)

S'han d'establir els procediments operatius adequats per a protegir els documents, mitjans informàtics (discos, cintes, etc.), dades d'entrada o de sortida i documentació del sistema contra la divulgació, modificació, retirada o destrucció d'actius no autoritzats.

L'anàlisi determina que el grau de compliment és només del 65%.

Requisits de negoci per al control d'accessos (9.1)

Les regulacions per el control d'accessos hauria de considerar les polítiques de distribució d'informació i d'autoritzacions.

Els propietaris dels actius de la informació que són responsables vers la direcció de la protecció dels «seus» actius haurien de tenir la capacitat de definir i/o aprovar les regles de control d'accés o altres controls de seguretat.

En aquest cas, el compliment del control 9.1 segons l'anàlisi del GAP és del 80%; quantitativament controlat.

Gestió d'accés d'usuari (9.2)

Els procediments haurien de cobrir totes les etapes del cicle de vida del accés del usuaris, des de el registre inicial dels nous usuaris fins la baixa quant no sigui necessari el seu accés als sistemes i serveis d'informació.

El compliment d'aquest control és només del 48%, és a dir, entre «Planificat» i «Ben definit».

Control d'accés a sistemes i aplicacions (9.4)

S'haurien d'establir els procediments operatius adequats per a protegir els documents, medis informàtics (discos, cintes, etc.), dades d'entrada i sortida i documentació del sistema contra la divulgació, modificació, retirada o destrucció d'actius no autoritzats.

En aquest sentit el compliment del control és només del 68% podent-se considerar «Ben definit».

Àrees Segures (11.1)

Els mitjans de processament de la informació crítica o confidencial haurien d'ubicar-se en àrees segures, protegides pels perímetres de seguretat definits, amb les barreres de seguretat i controls d'entrada apropiats.

L'anàlisi del GAP indica que el compliment d'aquest control és del 63%.

Seguretat dels Equips (11.2)

Els equips haurien de protegir-se contra amenaces físiques i ambientals. La protecció de l'equip és necessària per a reduir el risc d'accés no autoritzat a la informació i la seva protecció contra pèrdua i robatori.

El compliment del control és només del 60% (Ben definit) segons l'anàlisi del GAP realitzat.

Protecció contra codi maliciós (12.2)

El programari i els mitjans de processament de la informació són vulnerables a la introducció de codi maliciós i requereix de precaucions per evitar i detectar la introducció de codi de programació maliciós i codi amb capacitat de reproducció i distribució automàtica no autoritzada per a la protecció de la integritat del programari i de la informació que sustenten.

Es determina que el compliment d'aquest control és del 100% segons es desprèn de l'anàlisi del GAP.

Còpies de seguretat (12.3)

S'haurien d'establir procediments rutinaris per aconseguir la estratègia acceptada de «backup» per a realitzar còpies de seguretat i provar puntualment la seva recuperació.

En aquest sentit el control te un compliment del 60% (Ben definit), estant els controls planificats, documentats i implementats en tota la EMPRESA.

Gestió de la seguretat en les xarxes (13.1)

L'accés dels usuaris a les xarxes i serveis de xarxa no haurien de comprometre la seguretat.

L'anàlisi del control determina un 60% de compliment.

Intercanvi d'informació amb parts externes (13.2)

S'haurien de realitzar els intercanvis sobre la base de una política formal d'intercanvi, segons els acords d'intercanvi i complir amb la legislació corresponent.

S'haurien d'establir els procediments i normes per a protegir la informació i els mitjans físics que contenen la informació en trànsit.

L'anàlisi del GAP determina un 35% de compliment del control.

Seguretat en els processos de desenvolupament i suport (14.2)

Els directius responsables dels sistemes d'aplicacions haurien de ser també responsables de la seguretat del projecte i de l'entorn de suport. Ells haurien de garantir que totes les propostes de canvi en els sistemes són revisat per a verificar que no comprometen la seguretat del sistema i de l'entorn operatiu.

El compliment d'aquest control és només del 40%.

Gestió Documental

Política de Seguretat

SCRIPTIX és una consultora multinacional que ofereix solucions de negoci, estratègia, desenvolupament i manteniment d'aplicacions tecnologies i outsourcing.

Els professionals, la informació i el coneixement són els actius principals de de la companyia. També cal considerar com actius crítics els centres de treball e instal·lacions, i als nostres col·laboradors i proveïdors atès que són el suport a les nostres activitats de negoci.

Les premisses fonamentals de la Política de Seguretat de la Informació Corporativa de SCRIPTIX són:

- ✔ La protecció i seguretat de les persones i dels nostres actius clau, i la garantia de continuïtat de les nostres operacions de negoci.
- ✔ El compliment de la legislació local en els països en els que opera, les regulacions sectorials que li apliquen, i els requeriments dels nostres clients en matèria de seguretat.

Més informació a l'Annexe II – Política de Seguretat.

Procediment d'Auditories Internes

La metodologia del Pla que s'emprarà engloba tot el procés de millora contínua d'un sistema de gestió, és a dir, Planificar, Fer, Verificar i Actuar (PDCA). Tal i com indica el cicle Deming hi ha d'haver-hi la fase de verificar.

SCRIPTIX realitzarà anualment auditories per verificar que els controls, processos i procediments del Sistema de Gestió de Seguretat de la Informació segueix conforme la norma i la legislació vigent, així com validar que els objectius de seguretat de l'organització estan implementats, mantinguts amb eficàcia i tenen el rendiment esperat.

Més informació a l'Annexe III – Procediment d'auditories internes

Gestió d'Indicadors de Seguretat

La creació d'indicadors està orientada a la mesura de l'efectivitat, eficiència i eficàcia dels components implementats i gestió definits en el model d'operació del marc de seguretat de la informació, indicadors que serviran com a input per a la millora continua permetent adoptar decisions de millora.

Els objectius d'aquests processos de mesura pel que fa a la seguretat de la informació son:

- Avaluar la efectivitat de la implementació dels controls de seguretat.
- Avaluar la eficiència del Model de Seguretat de la Informació dintre de la companyia.
- Proveir d'estats de seguretat que serveixin de guia en les revisions del Model de Seguretat de la Informació, facilitant millores en la seguretat de la informació i noves entrades a auditar.
- Comunicar valors de seguretat a la companyia.
- Servir com a input al Pla d'Anàlisi i Tractament dels Riscos.

Tot indicador consta de vuit components bàsics:

- **Nom de l'indicador**; Identificador curt del control que doni una visió de l'objectiu d'aquest i el mesurament que fa.
- **Descripció de l'indicador**; Breu explicació de l'objectiu de l'indicador
- **Control de seguretat al que dona suport**
- **Fórmula de mesurament**; Descripció de la fórmula que s'aplica al control per a obtenir la mesura.
- **Unitats de mesura**; La unitat de mesura assignada. Aquestes han d'estar clarament especificades.
- **Freqüència de mesura dels indicadors**; Defineix la iteració (setmanal, mensual, anual, etc.) en l'obtenció del control.
- **Valor objectius i valor llindar**; Valor correcte per a la companyia i valor de tall a partir del que cal aixecat alarma respectivament.
- **Responsable**; Sobre qui (persona o departament) recau la responsabilitat de proporcionar la mesura.

A l'hora de seleccionar un indicador, és important que el mesurament sigui **fiable** i **repetible**, és a dir, que s'ha de basar en evidències objectives,

Hi ha diferents tipus d'indicadors;

- **Indicadors de gestió**
  - Nombre d'hores de formació impartides.
  - Pressupost dedicat a personal de manteniment de sistemes.
  - Nombre de treballadors amb responsabilitats en seguretat de la informació.
  - Nombre de suggeriments de millora de l'SGSI rebuts dels treballadors.
- **Indicadors d'operació**
  - Temps total de caiguda d'un determinat servei en l'últim mes.
  - Nombre d'avaries d'equips informàtics en l'últim mes.
  - Trànsit mitjà del tallafoc.
  - Nombre d'intents de penetració detectats per l'IDS respecte del nombre d'intents rebutjats.
  - Nombre de virus detectats respecte del nombre d'incidències per virus.
- **Indicadors d'entorn**
  - Alertes per un virus nou.
  - Temps mitjà d'exposició d'un sistema des que es detecta una vulnerabilitat fins que s'aplica el pegat.
  - Alertes meteorològiques per onades de calor, tempestes elèctriques, inundacions...
  - Canvis en la legislació.

A continuació es detallen els Indicadors de Seguretat ja implementats en SCRIPTIX. Informació addicional en Annexe IV – Gestió d'indicadors de Seguretat,

Control	Definit	En procés	No existeix
5 – Política de Seguretat		X	
8 – Gestió d'actius	X		
9 – Control d'Accés	X		
11 – Seguretat física i ambiental	X		
12 – Seguretat en la operativa		X	
13 – Seguretat de les telecomunicacions	X		
14 – Adquisició, desenvolupament i manteniment dels sistemes	X		

Tabla 4: Indicadors de seguretat

Procediment de Revisió per Direcció

Tal i com està definit en SCRIPTIX, tota la documentació d'alt nivell té definit una revisió periòdica per part de direcció. Aquesta revisió del Sistema de Gestió de Seguretat de la Informació es obligada com a mínim un cop l'any, i te com a objectiu assegurar que és adequada pels propòsits i objectius de l'organització.

Gestió de Rols i Responsabilitats

L'organització de la seguretat de la informació és una de les primeres tasques que cal abordar a l'hora d'implantar un SGSI (Sistema de Gestió de la Seguretat de la Informació). Tots els esforços en matèria de seguretat de la informació seran inútils o molt poc eficaços si la companyia no té clar qui té autoritat, sobre quins aspectes i qui és responsable de quines tasques o de quins àmbits.

A continuació s'exposa estructura organitzativa de seguretat de la informació, habitual en moltes organitzacions.

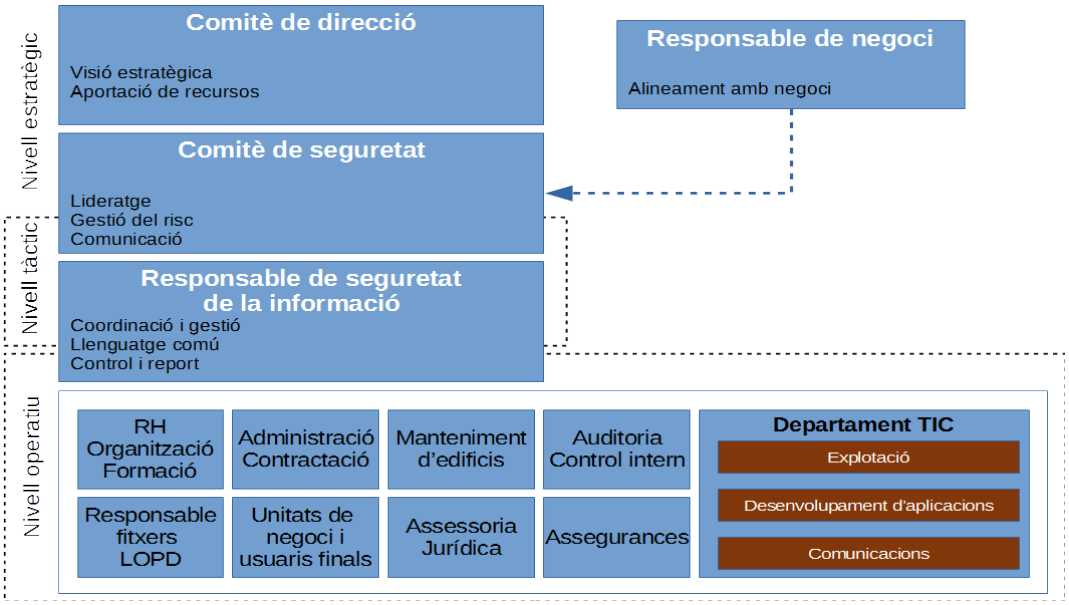


Figura 7: Estructura organitzativa

El comitè de direcció de la companyia

Les funcions en matèria de seguretat de la informació del comitè de direcció de la companyia són les següents:

- Fer de la seguretat de la informació un punt de l'agenda del comitè de direcció de la companyia.
- Nomenar els membres d'un comitè de seguretat de la informació i donar-hi suport, dotar-lo dels recursos necessaris i establir-hi les directrius de treball.
- Aprovar la política, les normes i responsabilitats generals en matèria de seguretat de la informació.
- Determinar el llindar de risc acceptable en matèria de seguretat.
- Analitzar riscos possibles introduïts per canvis en les funcions o en el funcionament de la companyia per a adoptar les mesures de seguretat més adequades.
- Aprovar el pla de seguretat de la informació, que recull els principals projectes i iniciatives en la matèria.
- Fer el seguiment del quadre de comandament de la seguretat de la informació.

Les decisions preses pel comitè de direcció en matèria de seguretat de la informació han de quedar recollides en acta.

El comitè de seguretat de la informació

Les decisions en matèria de seguretat de la informació les pren de manera consensuada un grup format per diferents responsables dins de la companyia.

Les funcions en matèria de seguretat de la informació del comitè de seguretat de la informació són les següents:

- Implantar les directrius del comitè de direcció
- Assignar rols i funcions en matèria de seguretat.
- Presentar a aprovació al comitè de direcció les polítiques, normes i responsabilitats en matèria de seguretat de la informació.
- Validar el mapa de riscos i les accions de mitigació que ha proposat el responsable de seguretat de la informació.

- Validar el pla de seguretat de la informació o pla director de seguretat de la informació i presentar-lo a aprovació al comitè de direcció. Supervisar-ne la implantació i fer-ne el seguiment.
- Supervisar i aprovar el desenvolupament i manteniment del pla de continuïtat de negoci.
- Vetllar perquè es compleixi la legislació que sigui aplicable en matèria de seguretat.
- Promoure la conscienciació i formació d'usuaris i liderar la comunicació necessària.
- Revisar les incidències més destacades.
- Aprovar i revisar periòdicament el quadre de comandament de la seguretat de la informació i de l'evolució del SGSI.

El comitè de seguretat de la informació ha de tenir representació de diverses àrees de suport i també de les principals unitats de negoci (les que estan sotmeses a més riscos).

Els components habituals del comitè de seguretat de la informació seran:

1) Membres permanents. Els membres permanents són el director de recursos humans, el director d'organització, el director de tecnologies de la informació i la comunicació, seguretat física (si existeix de forma diferenciada), el responsable de seguretat de la informació i els responsables de les àrees de negoci més crítiques o sensibles (unitats amb alts riscos, amb distribució territorial, etc.).
2) Membres per invitació. Són els representants d'altres unitats, com assessoria jurídica, auditoria o control. Pel que fa a la freqüència de reunió, al començament de la implantació del SGSI és convenient que el comitè de seguretat es reuneixi sovint (cada dues setmanes o cada mes). Una vegada superades les dues primeres fases del SGSI (planificar i fer), n'hi pot haver prou d'una reunió cada dos o tres mesos, i sempre que sigui necessari en cas de crisi.

Responsable de seguretat de la informació

La designació del responsable de seguretat de la informació (RSI) és l'única via per a avançar de manera organitzada i gradual en seguretat de la informació, ja que garanteix que hi ha algú per a qui la seguretat de la informació és una prioritat.

Les funcions en matèria de seguretat de la informació dels RSI són coordinar les accions orientades a garantir la seguretat de la informació en qualsevol de les formes que té (digital, òptica, paper, etc.)

i en tot el cicle de vida d'aquesta informació (creació, manteniment, distribució, emmagatzematge i destrucció), per a protegir-la en termes de confidencialitat, privadesa, integritat, disponibilitat,

autenticitat i traçabilitat.

Tot plegat es concreta en els punts següents:

- Implantar les directrius del comitè de seguretat de la informació de la companyia.
- Elaborar, promoure i mantenir una política de seguretat de la informació, i proposar anualment objectius en matèria de seguretat de la informació.
- Desenvolupar i mantenir el document d'Organització de la seguretat de la informació en col·laboració amb l'àrea d'organització o recursos humans, en el qual es recull qui assumeix cadascuna de les responsabilitats en seguretat i també una descripció detallada de funcions i dependències.
- Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.
- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions (seguretat física, prevenció, emergències, relacions amb la premsa, etc.), a fi de gestionar la seguretat de la informació de manera global.
- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).
- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.
- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques. Aquesta revisió ha de permetre proposar o actualitzar el pla de seguretat de la informació i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla i el pressupost, l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Vetllar pel compliment legal (LOPD, RD 3/2010, Esquema nacional de seguretat, Basilea, SOX, etc.) i coordinar les actuacions necessàries amb les unitats responsables.

- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic (gestió de traces, vulnerabilitats, canvis, etc.), fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.
- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable deformació de la companyia.
- Fer el seguiment de les incidències de seguretat, revisar-les i escalar-les al CSI si correspon.
- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat. L'RSI ha d'analitzar i mantenir actualitzat aquest quadre de comandament i presentar-lo al CSI amb la periodicitat que s'estableixi.

L'RSI pot delegar algunes de les seves funcions en segones persones, però en continua essent el responsable final i s'ha d'assegurar que es porten a terme correctament.

L'RSI s'ha de comunicar amb tot el negoci, però hi ha d'haver una relació estreta amb unitats com recursos humans o organització (seguretat relativa al personal i procediments transversals), àrea de les TIC (seguretat en l'operació, seguretat en el desenvolupament de nous sistemes d'informació, seguretat en les comunicacions, etc.) o seguretat física.

Altres responsabilitats distribuïdes per la companyia

Responsables funcionals de la informació

Tenen les funcions següents:

- Classificar la informació de la qual són responsables segons la criticitat que aquesta tingui per a la companyia en termes de confidencialitat, privadesa, integritat, continuïtat, autenticitat, no-repudi, traçabilitat i impacte mediàtic i determinar l'ús que s'ha de fer de la informació i qui hi pot accedir.
- Tenir coneixement de la normativa general o sectorial aplicable a la informació de la qual són responsables, inclosa la normativa vigent en matèria de protecció de dades de caràcter personal.
- Definir els requisits de seguretat per al tractament de la informació, sia de manera automatitzada o manual, en tot el cicle de vida de la informació (creació, modificació, conservació i destrucció si escau).

- Fer el seguiment de l'estat de la seguretat dels sistemes d'informació que tractin la informació de què són responsables i gestionar la mitigació de riscos dins del seu nivell de decisió.
- Impulsar l'elaboració de plans de continuïtat de negoci, implicar-s'hi i definir procediments alternatius en cas d'indisponibilitat del sistema o falta d'integritat de la informació.
- Col·laborar a fer revisions i auditories de seguretat de la informació.

Personal en general

Tot el personal intern o extern amb accés a la informació de la companyia (treballadors, proveïdors en prestació de serveis) té les obligacions següents:

- Mantenir la confidencialitat de la informació.
- Fer un bon ús dels equips i de la informació a què tenen accés i protegir-la d'accessos no autoritzats.
- Respectar les normes i els procediments vigents en matèria de seguretat de la informació i vetllar perquè la respectin terceres parts en prestació de serveis.
- Utilitzar adequadament les credencials d'accés als sistemes d'informació.
- Respectar la legislació vigent en matèria de protecció de dades de caràcter personal i qualsevol altra legislació que sigui aplicable.
- Notificar, per la via establerta, insuficiències, anomalies o incidències de seguretat i situacions sospitoses que poden posar en perill la seguretat de la informació.

Àrea de tecnologies de la informació i comunicacions (TIC)

Té les funcions següents:

- Complir les polítiques, les normes i els procediments en matèria de seguretat de la informació. Col·laborar amb l'RSI a definir-los.
- Implantar en els sistemes d'informació els controls de seguretat prescrits i les accions correctores establertes i gestionar les vulnerabilitats detectades.
- Requerir la participació de l'RSI en nous projectes de desenvolupament o adaptació o implantació de productes de mercat, especialment quan puguin ser crítics en termes de confidencialitat, privadesa, integritat, continuïtat, autenticitat, no-repudi i traçabilitat, o puguin tenir un impacte mediàtic important.

- Requerir la participació de l'RSI en la implantació o gestió dels canvis de maquinari i programari.
- Garantir la inclusió de la seguretat en tot el cicle de vida de les dades (creació, manteniment, conservació i destrucció) i en els processos de gestió de maquinari i programari.
- Adoptar mesures per a protegir la informació segons la classificació que n'ha fet el responsable de la informació.
- Col·laborar amb l'RSI a identificar riscos i a proposar solucions, i col·laborar en les revisions o auditories de seguretat que es duguin a terme.

Àrea de seguretat física

Té les funcions següents:

- Proporcionar els mitjans tècnics necessaris per a la protecció física de la informació, tant pel que fa a desastres físics (incendi, inundació, fallades de subministrament elèctric, etc.) com a accessos no autoritzats. La definició de controls que cal implantar s'ha de fer coordinadament amb l'RSI.
- Disposar de mesures de recuperació de la situació normal d'operació d'acord amb els requisits de continuïtat establerts pel negoci.
- Conèixer i implantar els procediments de seguretat establerts en la política de seguretat de la informació.
- L'RSI i el responsable de seguretat física s'han de reportar mútuament i tan aviat com puguin les incidències de seguretat detectades quan puguin afectar l'àmbit de competència de l'altra part.
- Implicar l'RSI en els projectes d'obra i rehabilitació d'edificis, per a tenir en compte a priori qüestions d'emplaçament d'elements de xarxa i comunicacions, protecció d'equips, etc.

Àrea de recursos humans

Té les funcions següents:

- Informar les unitats gestores de recursos d'informació sobre canvis o moviments de personal per a fer una bona gestió de recursos: altes, baixes definitives i temporals, canvis de categoria o de funcions, canvis organitzatius, etc.

- Treballar juntament amb l'RSI per a desenvolupar la política de seguretat de la informació en les qüestions referents al personal.
- Aplicar procediments disciplinaris en cas de vulneració del marc normatiu.

Àrea d'assessoria jurídica

Té les funcions següents:

- Col·laborar amb l'RSI a emetre noves polítiques i normes de seguretat i a investigar i resoldre incidències de seguretat quan se'n poden derivar accions legals (reclamacions de terceres parts, accions contra un treballador, etc.).
- Col·laborar amb l'RSI a definir clàusules específiques de seguretat de la informació i a incloure-les en els contractes amb terceres parts i contractes de personal extern.
- Informar l'RSI de nova legislació o canvis en la legislació aplicable, que poden tenir impacte sobre la seguretat de la informació, i donar suport a l'hora d'interpretar-los.

Altres àrees

Cada àrea dins de la companyia ha de col·laborar amb l'RSI a desplegar la seguretat en el seu àmbit d'actuació i a aconseguir treballar i fer treballar l'organització de manera segura. Així, doncs, també s'han d'identificar funcions de seguretat en els àmbits d'auditoria, assegurances, formació, organització, etc.

Metodologia d'anàlisi de riscos

Una anàlisi de riscos correspon, des del punt de vista de la seguretat, al procés d'identificació d'aquests riscos: en determina la magnitud i n'identifica les àrees que requereixen mesures de protecció.

Cal destacar que un procés d'anàlisi de riscos dóna com a resultat una informació i no una mesura de seguretat com a tal; és a dir, el procés en si no evitarà que l'organització tingui incidències de seguretat, sinó que permetrà identificar els perills a què està exposada. Això vol dir que, si tenim ben identificats els perills, a l'organització li serà més fàcil protegir-se de les situacions que representen un risc més gran.

A Annexe VI – Metodologia d'anàlisi de riscos es troba el procediment que té com a objectiu establir les activitats i responsabilitats necessàries per a la realització i gestió de riscos.

Declaració d'aplicabilitat

La política de Seguretat de la Informació de l'organització, aplica però no es limita a:

- La informació dels seus clients, socis de negoci, proveïdors i clients finals.
- La informació generada com a resultat de les operacions normals de negoci.
- Tots els actius d'informació a través del seu cicle de vida, incloent creació, transmissió, emmagatzematge i disposició final, prioritzant la seva protecció d'acord les avaluacions de riscos.
- Els diferents ambients de processament de la informació que inclou producció, proves, contingència i certificació.
- Tots els recursos humans que participen en el cicle del negoci de l'organització, incloent terceres companyies.

A l'apartat Annexe V – Declaració d'aplicabilitat pot trobar-se el document.

Anàlisi de Riscos

Introducció

La metodologia utilitzada per a l'anàlisi de riscos és MAGERIT v.3

> Referència: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Tal i com està detallat en document *Metodologia d'anàlisi de riscos* (Annexe VI – Metodologia d'anàlisi de riscos) MAGERIT arriba a la identificació de tots els riscos de l'organització a través de les següents fases:

1. Presa de dades i processos d'Informació.
2. Establiment dels paràmetres.
3. Anàlisi d'actius.
4. Anàlisi d'amenaces.
5. Establiment de les vulnerabilitats.
6. Valoració d'impactes.
7. Anàlisi de riscos intrínsecs.
8. Influència dels controls de seguretat.
9. Anàlisi dels riscos efectius.

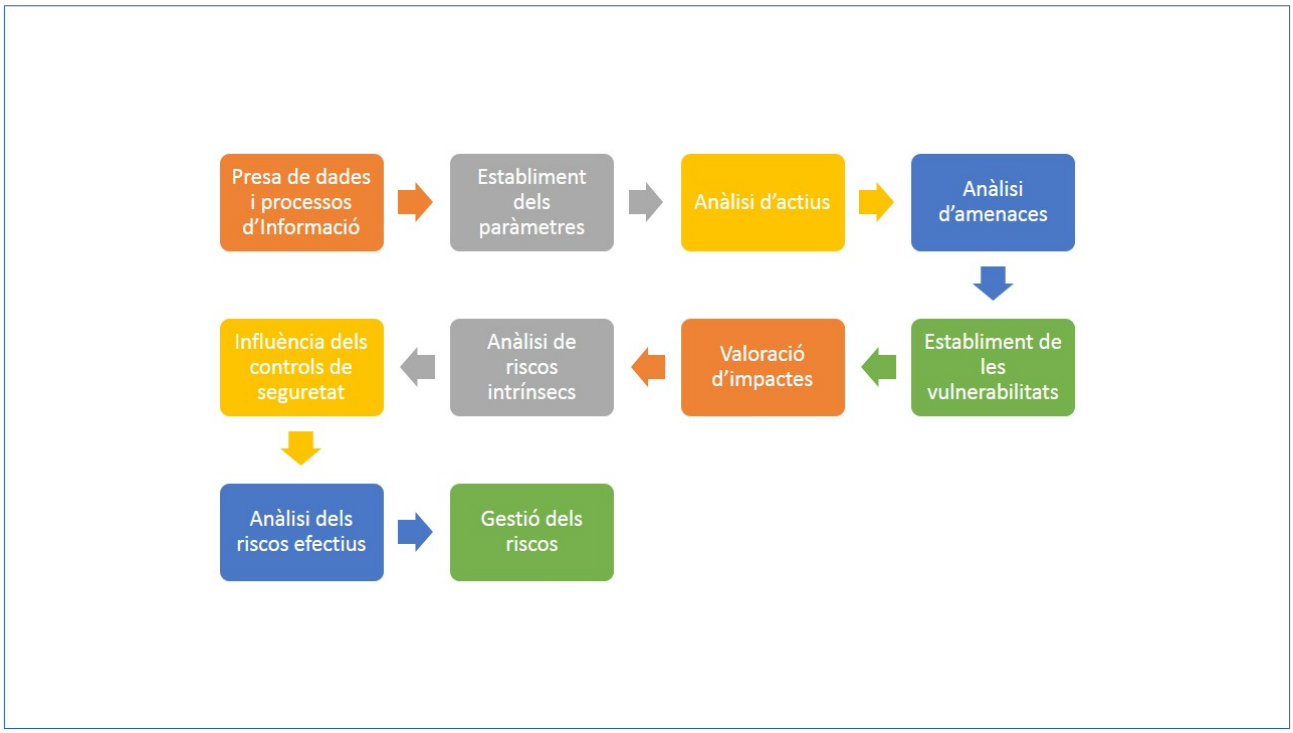


Figura 8: Fases MAGERIT v.3

A continuació es es detallen els elements que es tindran en consideració en el procés d'anàlisi de riscos;

Actius: Component o funcionalitat d'un sistema d'informació susceptible de ser atacat deliberada o accidentalment amb conseqüències per a l'organització. Inclou: informació, dades, serveis, aplicacions (software), equips (hardware), comunicacions, recursos administratius, recursos físics i recursos humans. [UNE 71504:20].

Amenaces: Causa potencial d'un incident que pot causar danys a un sistema d'informació o a una organització [UNE 71504:2008].

Vulnerabilitats: Es denomina vulnerabilitat a tota debilitat que pot ser aprofitada per una amenaça, o més detalladament a les debilitats dels actius o dels seus mitjans de protecció que faciliten l'èxit d'una amenaça potencial.

Impactes: Es denomina impacte a la mesura del dany sobre un actiu derivat de la materialització d'una amenaça. Coneixent el valor dels actius (en varies dimensions) i la degradació que causen les amenaces, es directe derivar l'impacte que aquestes tindran sobre el sistema.

Inventari d’actius

Els actius considerats en aquest anàlisi són els vinculats als Sistemes d’Informació, necessaris per al desenvolupament normal del negoci.

Els actius s’han classificat segons la següent categorització;

- **Instal·lacions**: Són tots els elements dels que disposa l’organització i que són necessaris perquè la resta funcioni correctament. En aquesta categoria podríem incloure ,per exemple, els sistemes d'aire condicionat o el cablejat de dades i de corrent elèctric, etc.
- **Hardware**: Són el conjunt d’elements físics o materials que constitueixen una computadora o un sistema informàtic, per exemple, ordinadors, servidors, portàtils, PDA, telèfons mòbils, impressores, etc.
- **Aplicació i software**: Són el conjunt de programari i rutines que permeten a un sistema informàtic realitzar determinades tasques, per exemple, sistemes operatius, aplicacions pròpies, etc.
- **Dades**: Són la representació simbòlica, bé sigui mitjançant números o lletres d’una recopilació d’informació fitxers, BBDD, copies de seguretat, etc.
- **Xarxa**: Són tots els elements que intervenen en la comunicació de dades d'un lloc a un altre, per exemple, Internet, routers, xarxes sense fil WiFi, telefonia mòbil, etc.
- **Serveis**: Són els elements que satisfà una necessitat dels usuaris.
- **Equipament auxiliar**: Són els elements que estan relacionats directament amb el tractament de dades. Per exemple: sistemes de refrigeració, sistemes d’alimentació ininterrompuda, cablejat, robots de cinta, caixes fortes, equips de destrucció, etc.
- **Personal**: Són les persones, des del punt de vista de rols o perfils que intervenen en el desenvolupament de les activitats de l'organització, per exemple, responsable de seguretat, administrador de la xarxa, personal d'administració, secretaris, usuaris, etc.

La següent taula mostra l’inventari d’actius de la companyia segons la categorització anterior.

Indicador	Categoria Actiu	Codi	Actiu
AH	Hardware	*AH-1*	CPD Principal
		AH-2	CPD Secundari
		AH-3	Switchs
		AH-4	Routers
		AH-5	Punt d'accés Wifi
		AH-6	Unitat de cinta
		AH-7	Portàtils (empleats)
		AH-8	Smartphones Android
		AH-9	Smartphones Appel
		AH-10	Unitats d'Emmagatzematge
AA	Aplicació i Software	*AA-1*	Windows Server 2016
		AA-2	Programari VMWare
		AA-3	Base de dades MySQL
		AA-4	Base de dades Oracle
		AA-5	Base de dades Informix
		AA-6	Firewall (programari lliure)
		AA-7	ERP SAP (Gestió RRHH, compres, facturació)
		AA-8	Windows 7 (SO portàtils)
		AA-9	Windows 10 (SO portàtils)
AS	Serveis	*AS-1*	Contracte seguretat física
		AS-2	Contracte de lloguer oficines
		AS-3	Contracte recursos Sistemes Informàtics
		AS-4	Pàgina web de la organització
		AS-5	Contracte servei de neteja
AX	Xarxa	*AX-1*	Comunicacions CPD Secundari
		AX-2	Comunicacions línia mòbil i 3G/4G
		AX-3	Comunicacions llocs de treball amb CPD principal
		AX-4	Comunicacions Internet
		AX-5	Comunicacions Unitats d'Emmagatzematge núvol
AP	Personal	*AP-1*	Directius de la companyia
		AP-2	Comandaments intermedis de la companyia
		AP-3	Administradors de xarxa
		AP-4	Administradors base de dades (DBA)
		AP-5	Personal d'estructura
		AP-6	Personal d'staff
AD	Dades	*AD-1*	Backups
		AD-2	Informació de clients
		AD-3	Informació de proveïdors
		AD-4	Informació d'empleats
		AD-5	Inventari d'actius
AE	Equipament Auxiliar	*AE-1*	Sistema refrigeració CPDs
		AE-2	Equips de destrucció de paper
		AE-3	Sistema d'alarmes
		AE-4	Armaris ignífugs
AI	Instal·lacions	*AI-1*	Edifici corporatiu
		AI-2	Seus corporatives
		AI-3	Llocs de treball

Table 5: Inventari d'actius

Valoració dels actius

En aquesta fase de Magerit s'assignarà una valoració econòmica al perímetre d'actius considerats en l'anàlisi de riscos.

La següent taula mostra la categorització per rangs econòmics:

Valor de l'actiu		
Valor	**Valoració**	**Rang**
5	Molt Alta	Valor > 200.000 €
4	Alta	100.000 € < valor > 200.000 €
3	Mitjana	50.000 € < valor > 100.000 €
2	Baixa	10.000 € < valor > 50.000 €
1	Molt Baixa	valor < 10.000 €

Table 6: Classificació quantitativa

A l'hora d'assignar una valoració a cada actiu s'ha de tenir en consideració el següent:

- El ***valor de reposició*** és el valor que té per a l'organització reposar aquest actiu en cas que es perdi o que no es pugui utilitzar.
- El ***valor de configuració*** és el temps que es necessita des que s'adquireix el nou actiu fins que es configura o es posa a punt perquè es pugui utilitzar per a la funció que desenvolupava l'anterior actiu.
- El ***valor d'ús*** de l'actiu és el valor que perd l'organització durant el temps que no pot utilitzar aquest actiu per a la funció que desenvolupa.
- El ***valor de pèrdua d'oportunitat*** és el valor que perd potencialment l'organització pel fet de no poder disposar d'aquest actiu durant un temps.

A l'Annexe VII – Valoració econòmica dels actius es te el detall de la valoració a nivell d'actiu.

A mode resum, la següent taula mostra la valoració (mitjana aritmètica) dels actius de l'organització segons la qualificació per rang econòmic anterior.

Resum valoració		
Indicador	**Categoria Actiu**	**Valoració**
AH	Hardware	1
AA	Aplicació i Software	1
AS	Serveis	2
AX	Xarxa	2
AP	Personal	2
AD	Dades	3
AE	Equipament Auxiliar	1
AI	Instal·lacions	5

Tabla 7: Resum valoració mitja actius

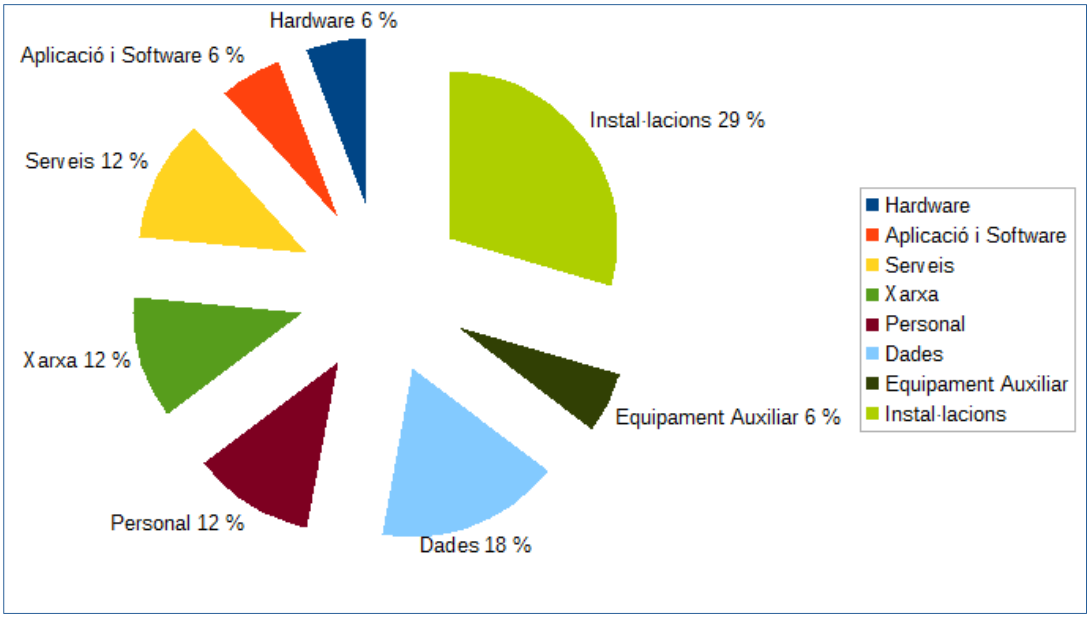


Figura 9: Distribució percentual actius

Dimensions de seguretat

A fi de poder determinar l'impacte que tindrà sobre l'organització un incident que afecta a la seguretat de la informació o dels sistemes, i poder establir la categoria del sistema, es tindran en compte les següents dimensions de seguretat, que seran identificades per les seves corresponents inicials en majúscules.

a) **Disponibilitat** [D]: És la característica, qualitat o condició de la informació de trobar-se a la disposició dels qui han d'accedir a ella, ja siguin persones, processos o aplicacions.

b) **Autenticitat** [A]: És la propietat que permet identificar el generador de la informació.

c) **Integritat** [I]: És la propietat que busca mantenir les dades lliures de modificacions no autoritzades. La integritat és el mantenir amb exactitud la informació tal qual va ser generada, sense ser manipulada o alterada per persones o processos no autoritzats.

d) **Confidencialitat** [C]: És la propietat que impedeix la divulgació d'informació a persones o sistemes no autoritzats. Assegura l'accés a la informació únicament a aquelles persones que comptin amb la deguda autorització.

e) **Traçabilitat** [T]: És possible reproduir un històric o seqüència d'accions sobre un determinat procés i determinar qui ha estat l'autor de cada acció.

Un cop explicades les cinc dimensions, s'ha de tenir present l'escala a la que es realitzaran les valoracions. En aquest cas utilitzarem una escala de valoració de deu valors, seguint els següents criteris.

Dimensió de seguretat	
Valor	**Criteri**
10	Dany molt greu
7-9	Dany greu
4-6	Dany important
1-3	Dany menor
0	Dany irrellevant

Tabla 8: Valoració dimensions de seguretat

La valoració realitzada es troba a l'Annexe VIII – Valoració dimensions de seguretat dels actius.

Anàlisi d’amenaces

Les amenaces són les situacions que es poden arribar a donar en una organització i que desembocarien en un problema de seguretat.

La classificació de les amenaces que poden afectar a l’organització es classifiquen en quatre grans grups:

- **Accidents**. Són les situacions no provocades voluntàriament que sovint no es poden evitar, sinó que passen per efectes naturals. Dins d'aquesta categoria d'accidents n'hi ha de diferents tipus, com ara:
  - Accident físic (inundació, incendi, terratrèmol, explosió, etc.).
  - Avaria.
  - Interrupció dels serveis essencials (talls en el subministrament elèctric, en les telecomunicacions, etc.).
  - Accidents mecànics o electromagnètics (xoc, caiguda, radiació, etc.).
- **Errors**. Són les situacions que són comeses de manera involuntària pel desenvolupament mateix de les activitats diàries de l'organització, sia per desconeixement o per distracció del personal de l’organització o de tercers que són contractats per l'organització mateixa. Entre aquestes situacions esmentem les següents:
  - Errors en la utilització dels sistemes, provocats per un mal ús.
  - Errors en el disseny conceptual de les aplicacions.
  - Errors en el desenvolupament de les aplicacions.
  - Errors d'actualització o aplicació de pegats als sistemes o aplicacions.
  - Errors en el monitoratge.
  - Errors de compatibilitat entre aplicacions.
  - Errors inesperats (virus, cavalls de Troia, etc.).
- **Amenaces intencionals presencials**. Són les provocades pel personal ma- teix de l'organització de manera voluntària quan fan accions que saben que provoquen un dany, tant des del punt de vista físic com del lògic. Entre aquestes amenaces esmentem les següents:
  - Accés físic no autoritzat, sia amb destrucció de la informació o amb subministració.

- Accés lògic no autoritzat, intercepció passiva de la informació o subtracció o alteració de la informació en trànsit.
- Indisponibilitat de recursos, tant si són humans (baixes, vacances, abandonament, malaltia, etc.) com tècnics (bloqueig de sistema, per exemple).
- Filtració de dades a terceres organitzacions, tant si són dades personals (LOPD) com tècniques.

- **Amenaces intencionals remotes**. Amenaces provocades per terceres persones, és a dir, per persones alienes a l'organització i que aconsegueixen danyar-la. Entre aquestes amenaces esmentem les següents:
  - Accés lògic no autoritzat. Accés d'un tercer no autoritzat, que explota una vulnerabilitat del sistema per utilitzar-la en benefici propi.
  - Suplantació de l'origen. Intercepció d'una comunicació escoltant o falsejant les dades intercanviades.
  - Cucs. Virus que utilitzen les capacitats de servidors i clients per a pro- pagar-se per Internet.
  - Denegació de servei, sigui contra l'amplada de banda (consumir tota l'amplada de banda de la màquina que es vol atacar) o contra els recursos del sistema (consumir tota la memòria i els recursos de la màquina utilitzada per a oferir un servei).

A l'Annexe IX – Anàlisi d'amenaces pot trobar-se el detall de l'anàlisi. A mode resum, el següent quadre mostra el número d'amenaces per actiu.

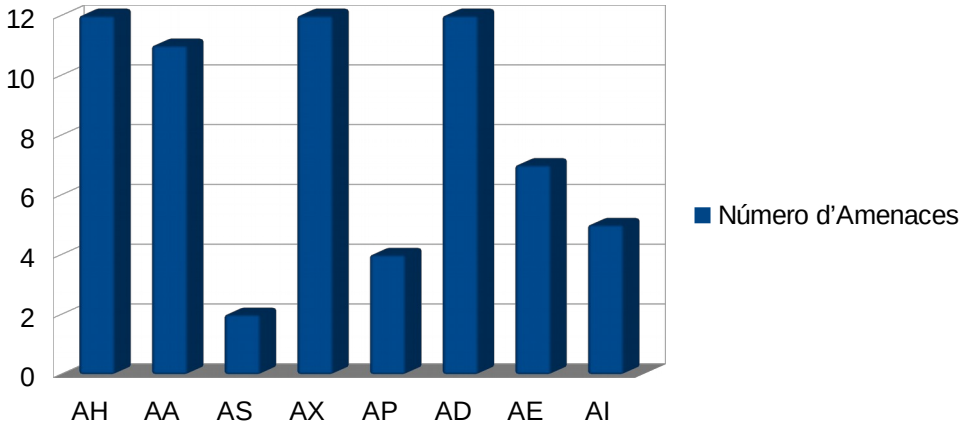


Figura 10: Amenaces per actiu

Un cop s'han establert i identificar les amenaces, s'ha de realitzar una valoració de la seva influència en el valor dels actius. En aquesta anàlisi s'ha avaluat la freqüència:

Freqüència			
Abreviatura	**Valoració**	**Rang**	**Valor**
EF	Extremadament freqüent	1 vegada /dia	1,000000000
MF	Molt freqüent	1 vegada / 2 setmanes	0,071232877
F	Freqüent	1 vegada / 2 mesos	0,016438356
PF	Poc freqüent	1 vegada / 4 mesos	0,010958904
MPF	Molt poc freqüent	1 vegada / 6 mesos	0,005479452
D	Inapreciable	1 vegada / any	0,002739726

Tabla 9: Freqüència vulnerabillitats

A l'Annexe X – Anàlisis d'actius i dimensions de seguretat es pot veure el detall la freqüència d'actius vs amenaces.

Impacte potencial

El primer element a calcular és l'Impacte Potencial, que identificarà la magnitud del dany que podria causar en l'organització el fet que arribes a ocórrer alguna de les amenaces. El càlcul de l'impacte potencial es realitza mitjançant la següent formula;

$$Impacte\ potencial = Valor\ de\ l'actiu \times Impacte$$

S'entén per impacte des de el punt de vista de Margarit per l'impacte en % del valor de l'actiu que es perd en el cas que es produeixi una incidència sobre aquest actiu.

Impacte		
Abreviatura	**Descripció**	**Valor**
C	Crític	90,00 %
A	Alt	75,00 %
M	Mitjà	50,00 %
B	Baix	20,00 %

A l'Annexe XI – Anàlisi d'impacte versus Impacte Potencial pot trobar-se la taula amb el detall.

El Risc intrínsec es calcula utilitzant l'impacte potencial i la freqüència. La formula per al seu càlcul és la següent;

$$Risc\ Intrínsec = Impacte\ Potencial \times Freqüència$$

Pot trobar-se el detall del de l'anàlisi del risc intrínsec a l'Annexe XII – Anàlisi del risc intrínsec.

Nivell de Risc Acceptable i Risc Residual

Un cop realitzat tots els càlculs, l'organització ha de determinar el nivell de risc està disposada a assumir i quin decideix mitigar mitjançant l'aplicació de controls de seguretat.

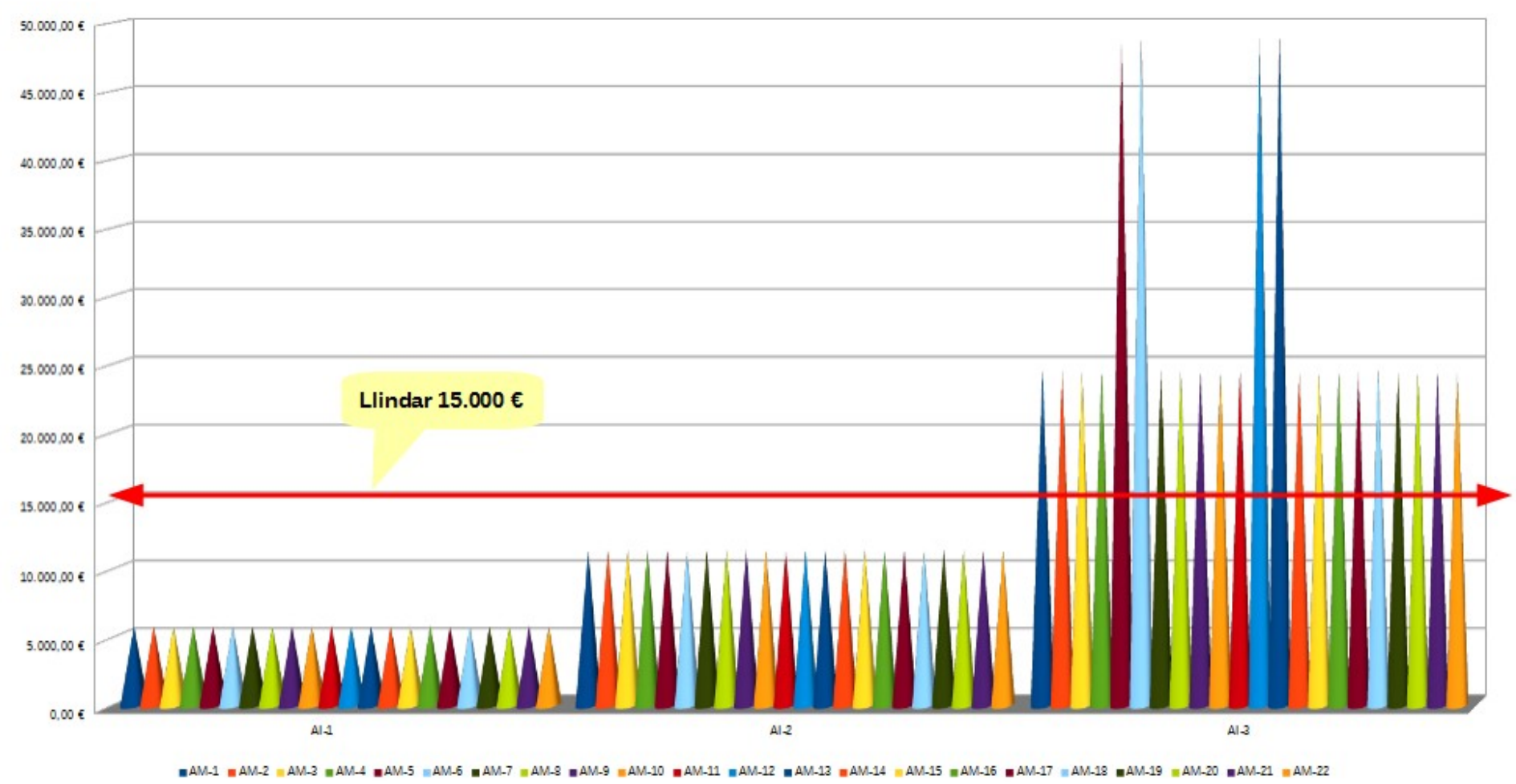
El **Risc Acceptable** es defineix com el risc que ha quedat per sota del llindar marcat per l'Organització.

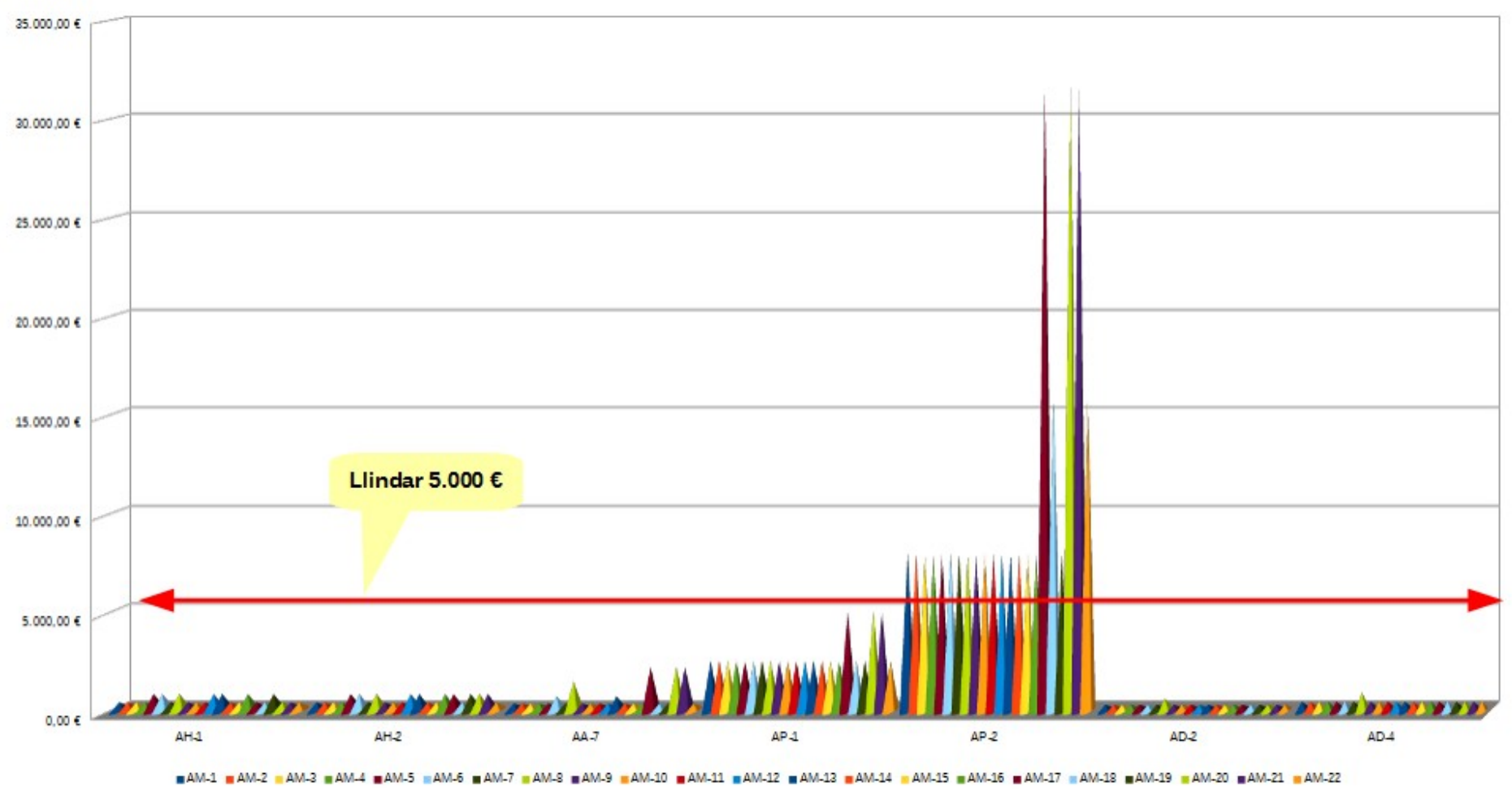
El **Risc Residual** és el risc romanent després d'haver desplegat el conjunt de mesures de seguretat.

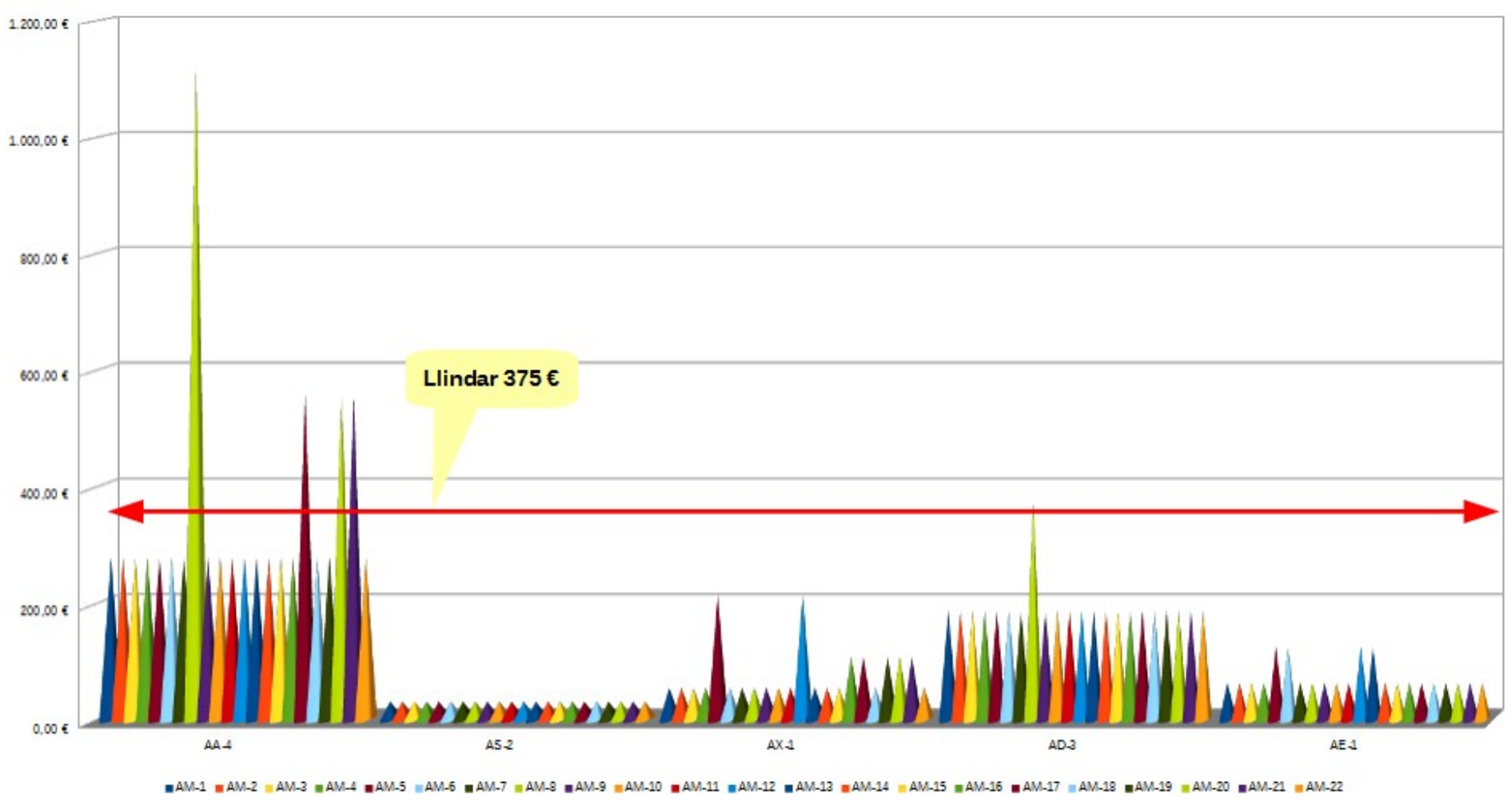
SCRIPTIX ha d'establir el llindar considerant el límit de riscos que està disposada a assolir. En aquest sentit s'ha decidit establir un llindar acord a cada categorització d'actiu;

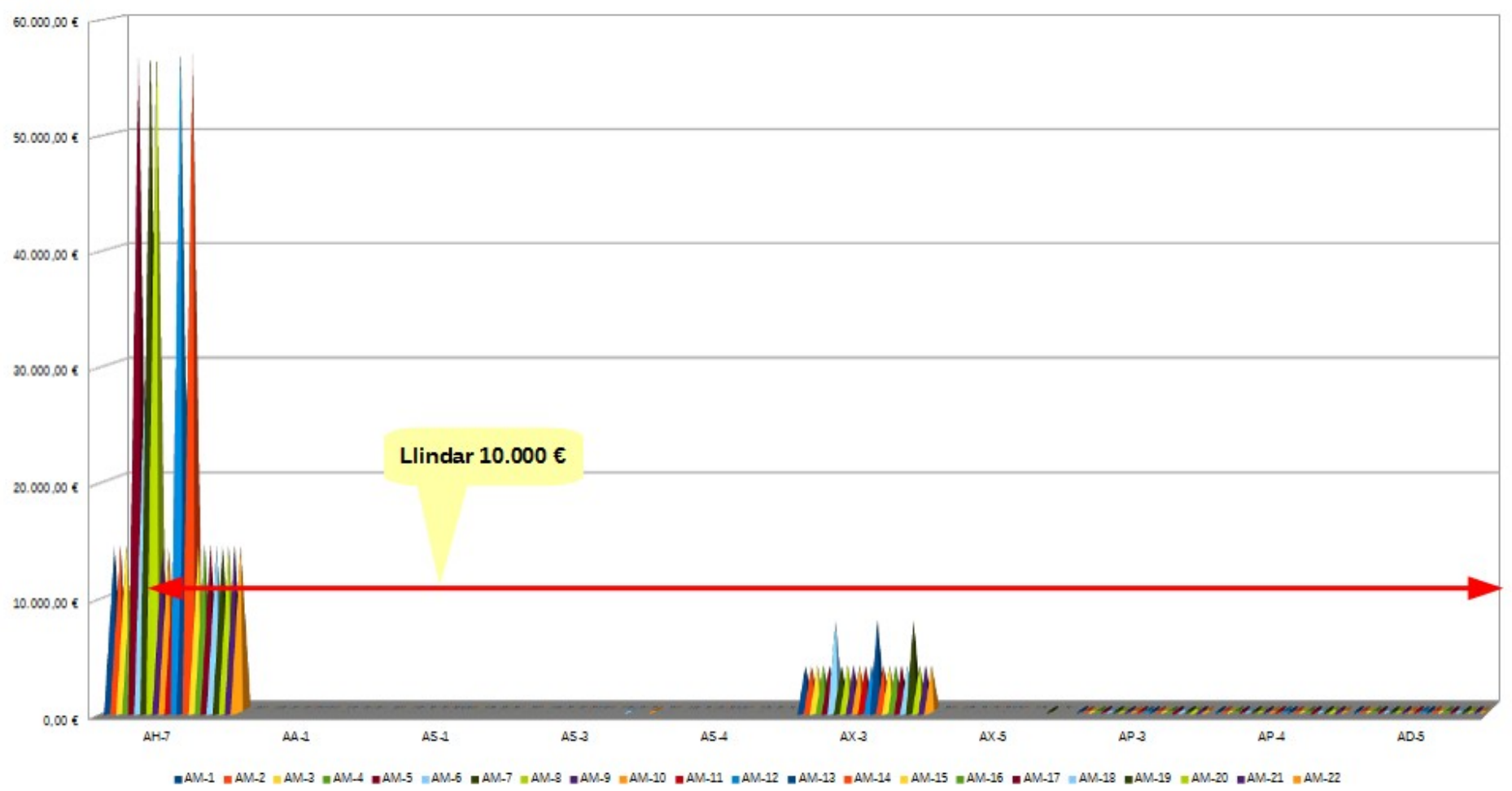
- [5] «Molt Alt»: 15.000 euros
- [4] «Alta»: 5.000 euros.
- [3] «Mitjana»: 375 euros.
- [2 «Baixa»: 10.000 euros
- [1] «Molt Baixa»: 40.000 euros

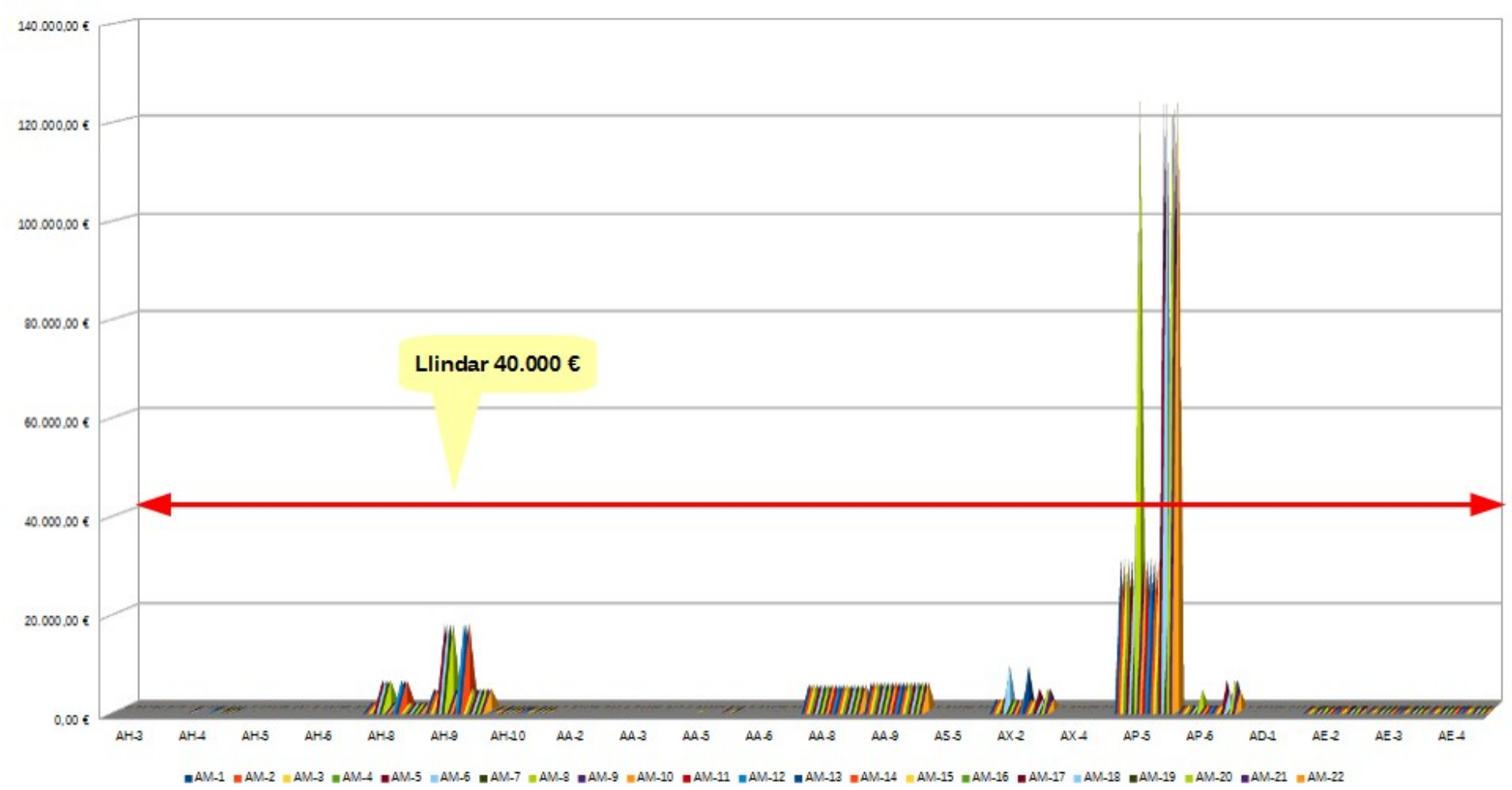
Les següents gràfiques mostren el risc intrínsec per amenaça dels actius així com el llindar per a cada categoria.






1.200,00 €
1.000,00 €
800,00 €
600,00 €
400,00 €
200,00 €
0,00 €
Llindar 375 €
AA-4
AS-2
AX-1
AD-3
AE-1
AM-1 AM-2 AM-3 AM-4 AM-5 AM-6 AM-7 AM-8 AM-9 AM-10 AM-11 AM-12 AM-13 AM-14 AM-15 AM-16 AM-17 AM-18 AM-19 AM-20 AM-21 AM-22

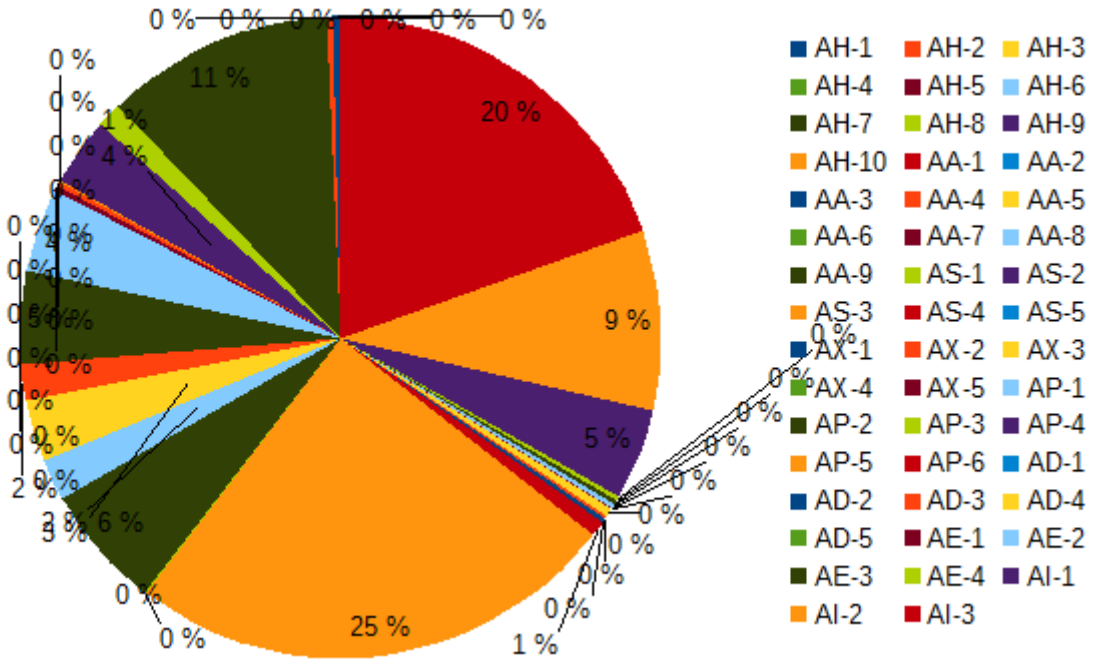



140.000,00 €
120.000,00 €
100.000,00 €
80.000,00 €
60.000,00 €
40.000,00 €
20.000,00 €
0,00 €
Llindar 40.000 €
AH-3 AH-4 AH-5 AH-6 AH-8 AH-9 AH-10 AA-2 AA-3 AA-5 AA-6 AA-8 AA-9 AS-5 AX-2 AX-4 AP-5 AP-6 AD-1 AE-2 AE-3 AE-4
AM-1 AM-2 AM-3 AM-4 AM-5 AM-6 AM-7 AM-8 AM-9 AM-10 AM-11 AM-12 AM-13 AM-14 AM-15 AM-16 AM-17 AM-18 AM-19 AM-20 AM-21 AM-22

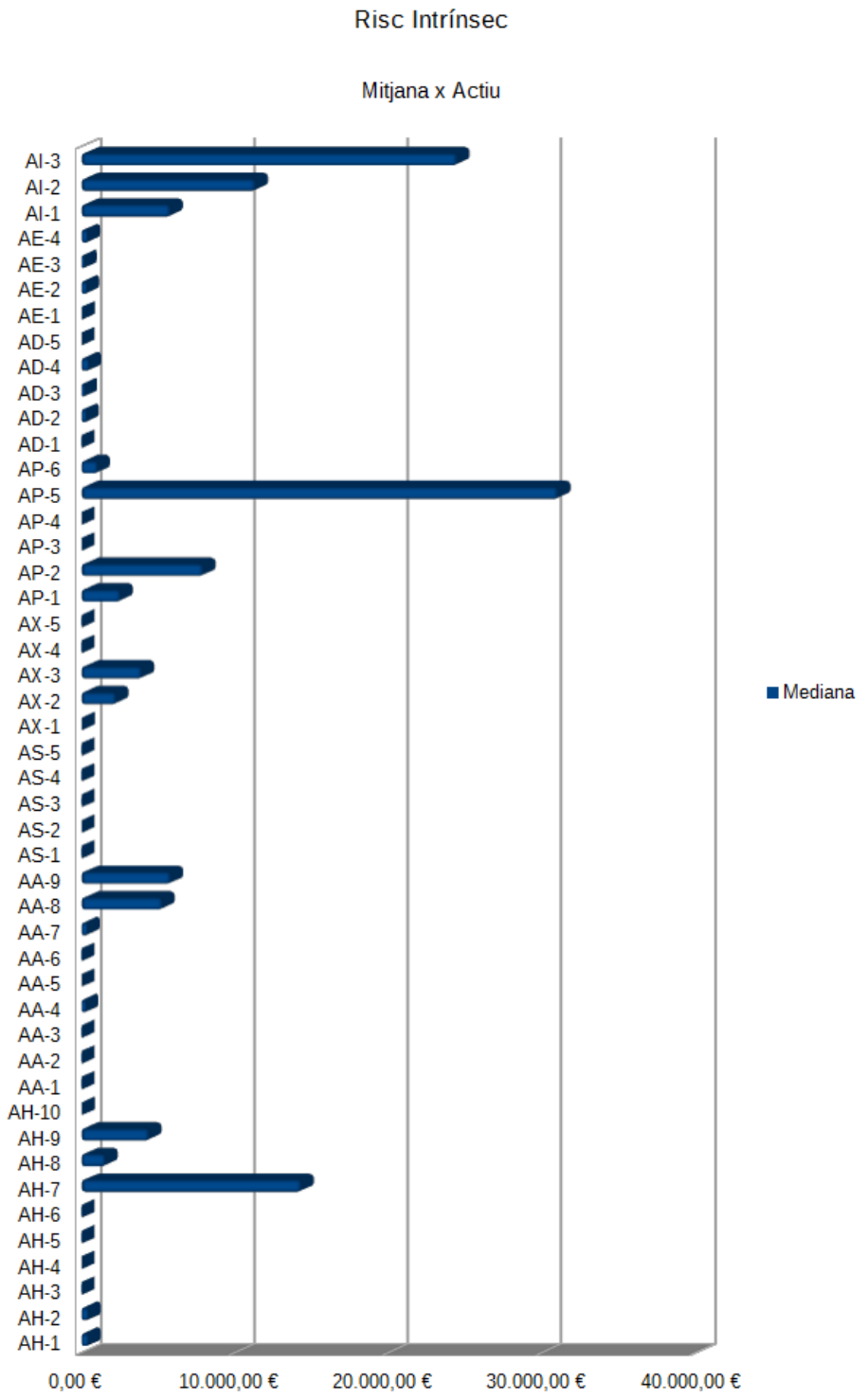
Resum

En l'Anàlisi de Riscos hem pogut determinar els actius que són més crítics per a SCRIPTIX, les amenaces que poden afectar-los i finalment el Risc Intrínsec al qual estan exposats, i sobretot, el risc acceptable que està disposat assumir l'organització.

A continuació es mostra la mitjana del Risc Intrínsec (%) categoritzat per actiu.



La següent gràfica mostra la mateixa informació en valors absoluts.


Risc Intrínsec
Mitjana x Actiu
AI-3
AI-2
AI-1
AE-4
AE-3
AE-2
AE-1
AD-5
AD-4
AD-3
AD-2
AD-1
AP-6
AP-5
AP-4
AP-3
AP-2
AP-1
AX-5
AX-4
AX-3
AX-2
AX-1
AS-5
AS-4
AS-3
AS-2
AS-1
AA-9
AA-8
AA-7
AA-6
AA-5
AA-4
AA-3
AA-2
AA-1
AH-10
AH-9
AH-8
AH-7
AH-6
AH-5
AH-4
AH-3
AH-2
AH-1
0,00 €
10.000,00 €
20.000,00 €
30.000,00 €
40.000,00 €
Mediana

Les principals amenaces que afronta l'organització són:

- AI-1: Edifici corporatiu
- AI-2: Seus corporatives
- AI-3: Llocs de treball
- AH-9: Smartphone Apple
- AH-8: Smartphone Android
- AH-7: Portàtils (empleats)
- AA-9: Windows 7 (SO portàtils)
- AA-8: Windows 10 (SO portàtils)

A continuació es detallen els riscos identificats per a cada actiu.

AI-1: Edifici corporatiu

L'organització disposa d'edifici corporatiu propi (en propietat). Addicionalment aquest edifici forma part d'una «illa» d'edificis ocupats per altres empreses de diferents sectors.

Qualsevol incident del tipus incendi, inundació, etc. que es pugui produir als edificis del voltant pot afectar a les oficines de SCRIPTIX. Cal tenir present que el ramal elèctric és comú a la illa d'edificis així com la seguretat privada i altres serveis comunitaris.

AI-2: Seus corporatives

Les seus corporatives distribuïdes arran de les ciutats on es present SCRIPTIX són de lloguer. No totes les seus disposen de seguretat física atès que és el propietari de l'edifici qui determina la necessitat. En aquest sentit és necessari revisar quins són els acords amb el llogater i proposar aquelles mesures necessàries per tal de garantir la seguretat.

Addicionalment el contracte de subministrament elèctric és a nom del llogater amb el que fa difícil minimitzar el risc de tall elèctric.

AI-3: Llocs de treball

Els llocs de treball que disposa la companyia no estan assignats directament al personal, a excepció del personal d'estructura.

La gestió dels llocs de treball es realitza mitjançant una APP desenvolupada per la pròpia companyia. Aquesta APP permet que un treballador reservi un lloc de treball durant un període concret degut a la limitació d'espai i amb l'objectiu d'optimitzar els recursos de la companyia.

Per a complir amb l'objectiu i que l'empleat pugui fer ús del lloc de treball és necessari que la configuració del lloc de treball sigui correcte. Això es tradueix en:

1) Connexió de xarxa amb connectivitat interna i externa (Internet).
2) Endolls, com a mínim 1, per poder endollar el portàtil.
3) Monitor amb cable HDMI o VGA.
4) Teclat USB.

Si falla qualsevol component de la configuració anterior l'ús del lloc de treball no és l'òptim. En aquest sentit i per a minimitzar els riscos és necessari una gestió del lloc de treball per part d'IT un cop aquest ha quedat lliure.

AH-9: Smartphone Apple

La literatura existent a Internet respecte els problemes de seguretat dels smarphones Apple és coneguda per tothom. Un dels aspectes més importants per a preservar la seguretat dels smarphones Apple és actualitzat el software amb les ultimes novetats del fabricant.

Segons la NVD (National Vulnerability Database) hi han, a data de redacció d'aquest apartat, 3172 coincidències utilitzant la cerca «ios». La publicació més recent és del 22 d'abril del 2019 i correspon a la vulnerabilitat identificada com CVE-2019-6155.

Donat aquest escenari, és imperatiu aplicar una política d'actualització de patchs de seguretat per tal de minimitzar (minimitzar atès que les vulnerabilitats «day-0» no són conegudes) el màxim possible qualsevol risc que afecti a la seguretat del dispositiu.

AH-8: Smartphone Android

La literatura existent a Internet respecte els problemes de seguretat dels smarphones Android és coneguda per tothom. Un dels aspectes més importants per a preservar la seguretat dels smarphones Android és actualitzat el software amb les ultimes novetats del fabricant.

Segons la NVD (National Vulnerability Database) hi han, a data de redacció d'aquest apartat, 114 vulnerabilitats detectades.

Donat aquest escenari, és imperatiu aplicar una política d'actualització de patchs de seguretat per tal de minimitzar (minimitzar atès que les vulnerabilitats «day-0» no són conegudes) el màxim possible qualsevol risc que afecti a la seguretat del dispositiu

AH-7: Portàtils (empleats)

Els portàtils és la eina de treball indispensable de l'empleat. Atès que molts dels empleats desenvolupen les seves tasques en les instal·lacions del client, s'identifiquen els següents riscos inherents a l'ús;

- Pèrdua / robatori
- Trencament de l'equip per accident
- Accés no autoritzat

Davant aquests riscos és necessari dotar de mesures de seguretat tal com cadenat per fixar el portàtil i evitar el robatori, PIN d'accés (BitLocker), xifrat del disc, etc. Utilitzar l'opció de renting és recomanable per disposar d'un altre equip en el menor temps possible.

AA-9: Windows 7 (SO portàtils) / AA-8: Windows 10 (SO portàtils)

Mantenir els sistemes operatius actualitzats és primordial per evitar qualsevol incident de seguretat. Cal evitar que es pugui desactivar l'opció «Windows Update» així com que es pugui desactivar o canviar les polítiques del Firewall de Windows o de l'antivirus.

Un altre risc és el derivat de la instal·lació de software llicenciat no corporatiu per part de l'usuari o d'aplicacions del tipus P2P (Peer-to-Peer) per a compartir arxius amb tercers a través d'una connexió a Internet.

Propostes de projectes

El Sistema de Gestió de la Seguretat de la Informació (SGSI), és el procés de millora continua de les amenaces a les que està exposada SCRIPTIX.

En la fase anterior s'han determinat els riscos als quals està exposada l'Organització i, en conseqüència, les necessitats en matèria de seguretat.

En aquest apartat seleccionarem i prioritzarem una sèrie de mesures en forma de projectes que permetran millorar la seguretat de SCRIPTIX.

És important realitzar una renovació i actualització de les mesures de seguretat seguint el cicle Deming (PDCA), incrementant el nivell de maduresa de l'anàlisi de riscos per prendre-ho com a punt de partida en la selecció dels projectes de seguretat, alineats amb els objectius de l'Organització.

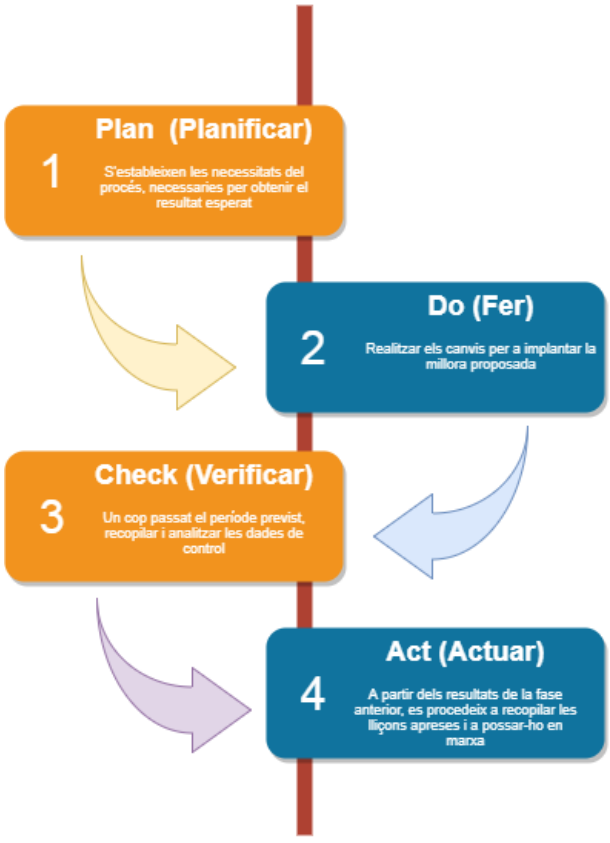


Figura 11: Cicle Deming - PDCA

Mitjançant aquesta progressió sobre el SGSI i el control del risc s'aconseguirà un compliment adequat de la norma ISO/IEC 27001:2013

El pla d'execució i implantació dels diferents projectes es contempla dins d'un període de tres anys, corresponent amb el cicle de la ISO 27001. S'han definit tres fases d'execució o implantació durant els quals es duran a terme les diferents implementacions dels projectes:

- ➔ **Projectes a curt termini**: realització i implantació durant el primer any.
- ➔ **Projectes a mig termini**: realització i implantació durant el segon any.
- ➔ **Projectes a llarg termini**: realització i implantació durant el tercer any.

Propostes

Projectes a curt termini

A continuació s'enumeren els projectes a implantar durant el primer any:

- ✔ SGSI-1-1 Inventari d'actius (CMDB)
- ✔ SGSI-2-1 Implementació d'un ATD (Advanced Threat Detection)
- ✔ SGSI-3-1 Implementació d'un sistema de traçabilitat
- ✔ SGSI-4-1 Programa de conscienciació sobre la seguretat
- ✔ SGSI-5-1 Implementació d'auditories de compliment normatiu
- ✔ SGSI-6-1 Procediments i gestió d'auditories internes i externes
- ✔ SGSI-7-1 Política de gestió de backups

El detall de les tasques pot trobar-se a l'Annexe XIII – Projectes a curt termini.

Projectes a mig termini

A continuació es llisten els projectes a abordar durant el segon any.

- ✔ SGSI-1-2 Actualització de software; SO i aplicacions corporatives

- ✔ SGSI-2-2 Actualització del sofware de backups
- ✔ SGSI-3-2 Millora dels Centre de Processament de Dades
- ✔ SGSI-4-2 Migració Windows 2003 a Windows server 2012
- ✔ SGSI-5-2 Migració Oracle 10g a Oracle 12c
- ✔ SGSI-6-2 Actualització patchs mòbils Apple
- ✔ SGSI-7-2 Actualització patchs mòbils Android

El detall de les tasques pot trobar-se a l'Annexe XIV – Projectes a mig termini.

Projectes a llarg termini

A continuació s'indiquen quins projectes caldrà abordar durant el tercer any.

- ✔ SGSI-1-3 Reestructuració del departament TIC
- ✔ SGSI-2-3 Pla de continuïtat de negoci
- ✔ SGSI-3-3 Externalització de serveis

El detall de les tasques pot trobar-se a l'Annexe XV – Projectes a llarg termini.

Resultats

Un cop definits tots els projectes planificats per cadascun dels períodes, realitzem un resum dels resultats obtinguts;

- Segons l'anàlisi de riscos
- Segons la ISO27001

A continuació la planificació definida per l'execució dels diferents projectes així com la el càlcul de costos dels diferents projectes que formen la proposta.

	Nombre	Duracion	Inicio	Terminado
1	**Projectes curt termini**	**283 days**	**2/09/19 8:00**	**30/09/20 17:00**
2	SGSI-1-1 Inventari d'actius (CMDB)	26,25 days	2/09/19 8:00	8/10/19 10:00
3	SGSI-2-1 Implementació d'un ATD (Advanced Threat Detection)	48,75 days	8/10/19 10:00	13/12/19 17:00
4	SGSI-3-1 Implementació d'un sistema de traçabilitat	39 days	16/12/19 8:00	6/02/20 17:00
5	SGSI-4-1 Programa de conscienciació sobre la seguretat	24,88 days	7/02/20 8:00	12/03/20 16:02
6	SGSI-5-1 Implementació d'auditories de compliment normatiu	51,25 days	12/03/20 16:02	25/05/20 9:02
7	SGSI-6-1 Procediments i gestió d'auditories internes i externes	38,75 days	25/05/20 9:02	16/07/20 16:02
8	SGSI-7-1 Política de gestió de backups	54,12 days	16/07/20 16:02	30/09/20 17:00
9	**Projectes mig termini**	**258 days**	**1/10/20 8:00**	**27/09/21 17:00**
10	SGSI-1-2 Actualització de software; SO i aplicacions corporatives	32,5 days	1/10/20 8:00	16/11/20 13:00
11	SGSI-2-2 Actualització del sofware de backups	15 days	16/11/20 13:00	7/12/20 13:00
12	SGSI-3-2 Millora dels Centre de Processament de Dades	97,75 days	7/12/20 13:00	22/04/21 10:00
13	SGSI-4-2 Migració Windows 2003 a Windows server 2012	10 days	22/04/21 10:00	6/05/21 10:00
14	SGSI-5-2 Migració Oracle 10g a Oracle 12c	15 days	6/05/21 10:00	27/05/21 10:00
15	SGSI-6-2 Actualització patchs mòbils Apple	32,63 days	27/05/21 10:00	12/07/21 16:02
16	SGSI-7-2 Actualització patchs mòbils Android	55,12 days	12/07/21 16:02	27/09/21 17:00
17	**Projectes llarg termini**	**296 days**	**28/09/21 8:00**	**15/11/22 17:00**
18	SGSI-1-3 Reestructuració del departament TIC	122,5 days	28/09/21 8:00	17/03/22 13:00
19	SGSI-2-3 Pla de continuïtat de negoci	86,75 days	17/03/22 13:00	18/07/22 10:00
20	SGSI-3-3 Externalització de serveis	86,75 days	18/07/22 10:00	15/11/22 17:00

Figura 12: Planificació - Resum tasques

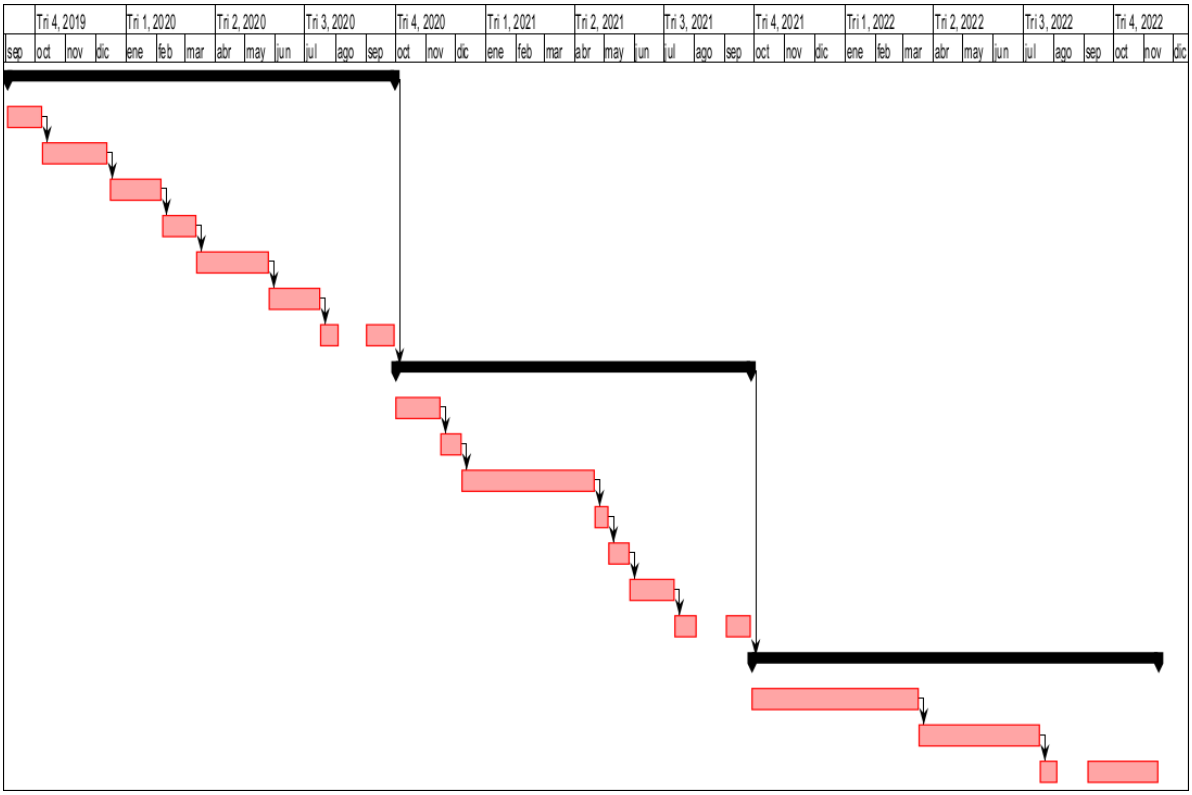


Figura 13: Planificació - Diagrama de Gantt

El següent quadre mostra els costos associats a cada projecte;

Codi	Descripció	Planificació i cost		
		Data Inici	Data Fí	Cost (€)
SGSI-1-1	Inventari d'actius (CMDB)	02/09/2019	08/10/2019	12.705,00 €
SGSI-2-1	Implementació d'un ATD (Advanced Threat Detection)	08/10/2019	13/12/2019	23.595,00 €
SGSI-3-1	Implementació d'un sistema de traçabilitat	16/12/2019	06/02/2020	18.452,50 €
SGSI-4-1	Programa de conscienciació sobre la seguretat	07/02/2020	12/03/2020	12.039,50 €
SGSI-5-1	Implementació d'auditories de compliment normatiu	12/03/2020	25/05/2020	24.805,00 €
SGSI-6-1	Procediments i gestió d'auditories internes i externes	25/05/2020	16/07/2020	18.755,00 €
SGSI-7-1	Política de gestió de backups	16/07/2020	30/09/2020	15.730,00 €
SGSI-1-2	Actualització de software; SO i aplicacions corporatives	30/09/2020	16/11/2020	15.730,00 €
SGSI-2-2	Actualització del sofware de backups	13/11/2020	07/12/2020	7.260,00 €
SGSI-3-2	Millora dels Centre de Processament de Dades	04/12/2020	22/04/2021	47.311,00 €
SGSI-4-2	Migració Windows 2003 a Windows server 2012	21/04/2021	06/05/2021	4.840,00 €
SGSI-5-2	Migració Oracle 10g a Oracle 12c	05/05/2021	27/05/2021	7.260,00 €
SGSI-6-2	Actualització patchs mòbils Apple	26/05/2021	12/07/2021	15.790,50 €
SGSI-7-2	Actualització patchs mòbils Android	09/07/2021	27/09/2021	15.790,50 €
SGSI-1-3	Reestructuració del departament TIC	24/09/2021	17/03/2022	59.290,00 €
SGSI-2-3	Pla de continuïtat de negoci	16/03/2022	18/07/2022	41.987,00 €
SGSI-3-3	Externalització de serveis	14/07/2022	15/11/2022	31.520,50 €
	TOTAL	02/09/2019	15/11/2022	372.861,50 €

Tabla 10: Costos projectes

El següent gràfic resumeix les despeses per termini que ha de realitzar l'organització.

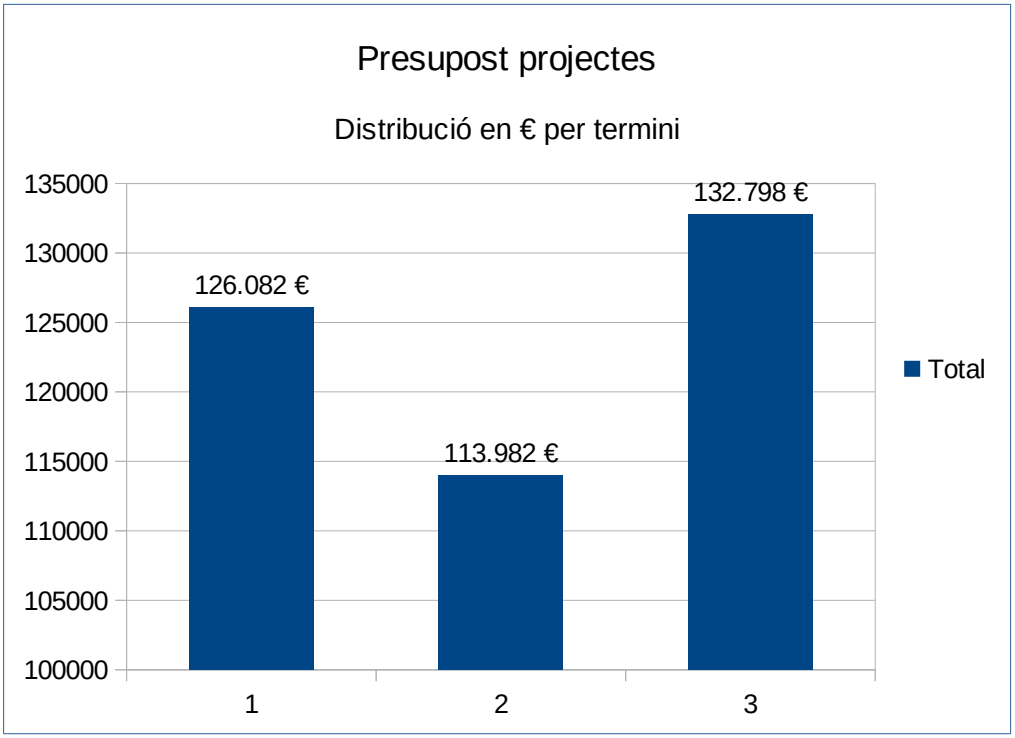


Figura 14: Despeses per termini en €

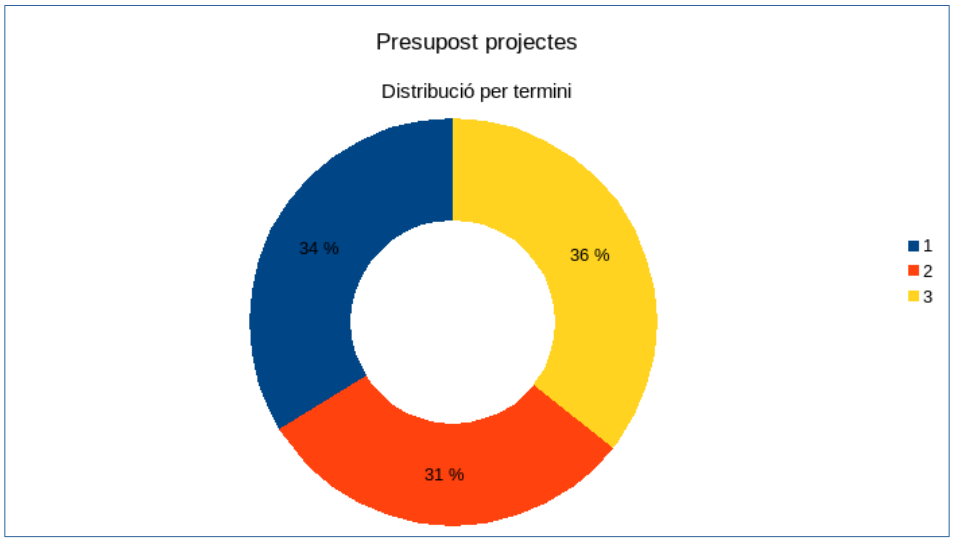


Figura 15: Distribució (%) de les despeses per termini

NOTA:

Per tal de facilitar el càlcul s'ha fixat un preu mig/hora de 60,50€

El calendari de la planificació considera els següents paràmetres:

1. La jornada laboral és de 8 hores
2. El mes d'agost es considera un mes inhàbil per vacances

Auditoria de compliment

Introducció

El cicle de millora contínua (PDCA) en el que està basat el Sistema de Gestió de la Seguretat de la Informació (SGSI) implantat, defineix la necessitat de realitzar una fase de validació (***C***heck) de l'estat i la idoneïtat del seu disseny.

La validació es realitzarà mitjançant una Auditoria de Compliment que proporcionarà una visió independent del grau de maduresa de la seguretat respecte les especificacions de la ISO/IEC 27001. Aquestes auditories s'han de fer amb una periodicitat anual i de planificar dins el Pla d'Auditoria.

Al finalitzar la implementació dels projectes, prevista la seva finalització la primera quinzena de novembre del 2022, s'iniciarà l'auditoria que tindrà caràcter inicial. Els resultats d'aquesta auditoria proporcionen una sèrie de "No Conformitats" i "Recomanacions" que seran utilitzades a la fase de millora del SGSI. Finalitzat el termini per a les *correccions* d'aquestes «No Conformitats» i «Recomanacions», caldrà tornar a revisar el nivell de compliment.

Metodologia

Aquesta Auditoria es realitza respecte als 14 dominis, 35 objectius de control i 114 controls de la ISO/IEC 27002:2013, i que ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

La valoració la realitzarem segons la següent taula, basada en el Model de Maduresa de la Capacitat (CMM - *Capability Maturity Model*):

Efectivitat	CMM	Significat	Descripció
0%	L0	Inexistent	Manca completa de qualsevol procés recognoscible. No s'ha reconegut que existeix un problema a resoldre
10%	L1	Inicial / Ad hoc	Estat inicial on l'èxit de les activitats del procés es basa, la majoria de vegades, en l'esforç personal. Els processos són inexistents o localitzats en àrees concretes. No existeixen plantilles definides a nivell corporatiu
50%	L2	Reproduïble, però intuïtiu	Els processos similars es duen a terme de manera similar per persones amb la mateixa tasca. Es normalitzen les tasques en base a l'experiència al mètode. No hi ha comunicació o entrenament formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada persona
90%	L3	Procés definit	L'organització sencera participa en el procés Els processos estan implantats, documentats i comunicats mitjançant entrenament
95%	L4	Gestionat i mesurable	Poden seguir-se amb indicadors numèrics i estadístics l'evolució del procés. Es disposa de tecnologia per automatitzar el fluix de treball. Es disposa d'eines per a millorar la qualitat i la eficiència
100%	L5	Optimitzat	Els processos es troben sota millora constant. En base a criteris quantitatius es determinen les desviacions i s'optimitzen els processos

Aquesta auditoria s'ha realitzat seguint les indicacions del Pla d'Auditoria establert, repartint les tasques en tres etapes:

1. *Preparació / Planificació de l'auditoria*; Durant aquesta etapa es demana tota la documentació i registres rellevants per a l'Auditoria. Un cop recopilada aquesta informació, es revisa la seva idoneïtat i vigència, així com que es trobi alineada amb les bones pràctiques especificades per la ISO.
2. *Execució de l'auditoria*; Aquesta etapa aglutina el conjunt de tasques que proporcionen la informació necessària per a determinar el grau de compliment.
   a) Realització d'entrevistes amb responsables i personal.
   b) Verificació de controls tècnics (implantació i funcionament).

c) Realització de visites per examinar aspectes de seguretat física.

3. Conclusions de l'auditoria; Durant aquesta etapa, s'analitza la informació recollida en les diferents proves i entrevistes de les etapes anteriors. Aquest anàlisi ha de determinar el nivell de maduresa i compliment respecte a la ISO/IEC 27002:2013, localitzant les fortaleses i les «No Conformitats».

Finalment s'elabora un informe per proporcionar la informació rellevant, així com els diferents troballes realitzades.

Avaluació de la maduresa

L'objectiu d'aquesta fase del projecte és avaluar la maduresa de la seguretat, pel que fa als diferents dominis de control plantejats per la ISO/IEC 27002:2013.

Per realitzar el mesurament del grau de maduresa s'ha utilitzat el model CMM (Capability Maturity Model), igual que a la fase d'anàlisis diferencial, on s'estableixen una sèrie de nivells i percentatges que permeten identificar el progrés realitzat en cada un dels controls auditats.

Norma	Dominis	CMM 2019	Efectivitat	CMM 2022	Efectivitat
5	Polítiques de Seguretat	L3	90%	L5	100%
8	Gestió d'actius	L2	50%	L3	90%
9	Control d'accés	L2	50%	L4	95%
11	Seguretat física i ambiental	L2	50%	L2	50%
12	Seguretat en la operativa	L3	90%	L5	100%
13	Seguretat en les telecomunicacions	L2	50%	L2	50%
14	Adquisició, desenvolupament o manteniment dels sistemes d'informació	L2	50%	L5	100%
	Compliment General		**61%**		**84%**

A l'Annexe XVI – Informe d'auditoria pot trobar-se el detall pressuposant que s'han implantat tots els projectes definits en l'apartat Propostes de projectes.

Resultats

Com a resultat de l'anàlisi de cada un dels controls de la ISO/IEC 27002:2013 de referència s'han trobat un total de 4 «No Conformitats» que hauran de ser corregides.

Aquestes «No Conformitats» es troben en els següents controls de la norma:

- 8.3 Mitjans de manipulació
- 9.1 Els requisits de negoci de control d'accés
- 11.2 Seguretat dels equips
- 13.2 Intercanvi d'informació amb parts externes

Àrea	5. Polítiques de la Seguretat de la Informació	Conclusió	Conforme
Control ISO/IEC 27002:2013: 5.1 Direcció de gestió de seguretat de la informació			

Àrea	8. Gestió d'actius	Conclusió	Conforme
Control ISO/IEC 27002:2013: 8.1 Responsabilitat sobre els actius			

Àrea	8. Gestió d'actius	Conclusió	Conforme
Control ISO/IEC 27002:2013: 8.2 Classificació de la Informació			

Àrea	8. Gestió d'actius	Conclusió	No Conforme
Control ISO/IEC 27002:2013: 8.3 Mitjans de manipulació			

Àrea	9. Control d'accés	Conclusió	No Conforme
Control ISO/IEC 27002:2013: 9.1 Els requisits de negoci de control d'accés			

Àrea	9. Control d'accés	Conclusió	Conforme
Control ISO/IEC 27002:2013: 9.2 Gestió d'accés dels usuaris			

Àrea	9. Control d'accés	Conclusió	Conforme
Control ISO/IEC 27002:2013: 9.3 Responsabilitat dels usuaris			

Àrea	9. Control d'accés	Conclusió	Conforme
Control ISO/IEC 27002:2013: 9.4 Control d'accés a sistemes i aplicacions			

Àrea	11. La seguretat física i ambiental	Conclusió	Conforme
Control ISO/IEC 27002:2013: 11.1 Les àrees segures			

Àrea	11. La seguretat física i ambiental	Conclusió	No Conforme
Control ISO/IEC 27002:2013: 11.2 Seguretat dels equips			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.1 Procediments i responsabilitats operacionals			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.2 Protecció contra el malware			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.3 Còpia de seguretat			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.4 Registre i supervisió			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.5 Control de programari operacional			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.6 Gestió tècnica de la vulnerabilitat			

Àrea	12. Seguretat en la Operativa	Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.7 Sistemes d'informació consideracions d'auditoria			

Àrea	13. Seguretat en les comunicacions	Conclusió	Conforme
Control ISO/IEC 27002:2013: 13.1 de gestió de seguretat de xarxa			

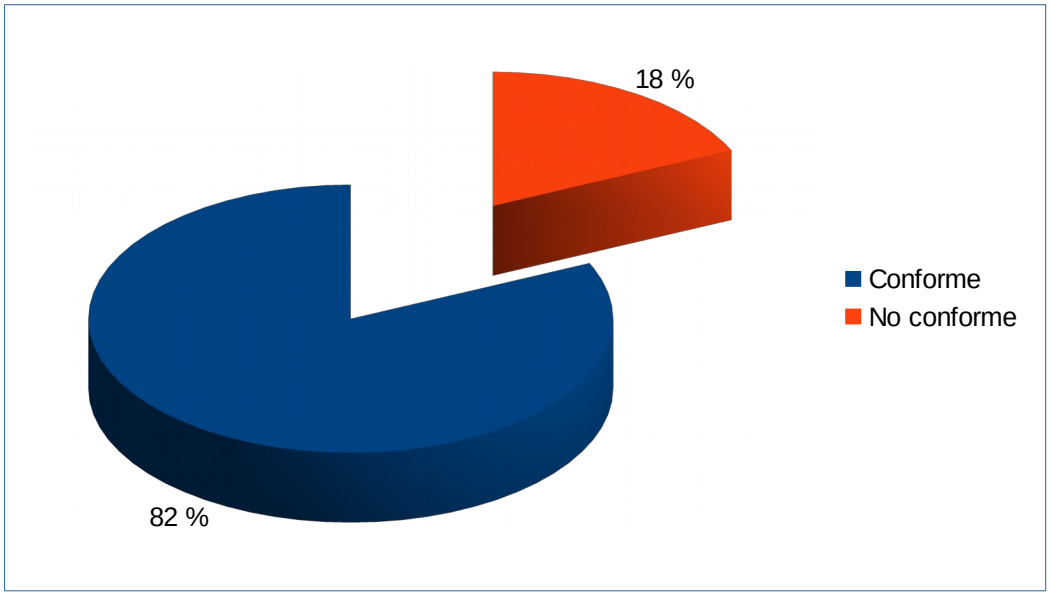
Àrea	13. Seguretat en les comunicacions	Conclusió	No Conforme
Control ISO/IEC 27002:2013: 13.2 Intercanvi d'informació amb parts externes			

Àrea	14. Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme
Control ISO/IEC 27002:2013: 14.1 Requeriments de seguretat dels sistemes d'informació			

Àrea	14. Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme
Control ISO/IEC 27002:2013: 14.2 Seguretat en els processos de desenvolupament i suport			

Àrea	14. Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme
Control ISO/IEC 27002:2013: 14.3 Dades de prova			

Norma	Dominis		Conforme	No conforme
5	Polítiques de la Seguretat de la Informació	5. Polítiques de la Seguretat de la Informació	1	0
8	Gestió d'actius	8. Gestió d'actius	2	1
9	Control d'accés	9. Control d'accés	3	1
11	La seguretat física i ambiental	11. La seguretat física i ambiental	1	1
12	Seguretat en la Operativa	12. Seguretat en la Operativa	7	0
13	Seguretat en les comunicacions	13. Seguretat en les comunicacions	1	1
14	Sistema d'adquisició, desenvolupament i manteniment	14. Sistema d'adquisició, desenvolupament i manteniment	3	0
TOTAL			18	4
			81,82 %	18,18 %



Conclusions

Durant el desenvolupament de tot aquest projecte s'han establert les bases que permetran la implementació d'un Sistema de Gestió de la Seguretat de la Informació (SGSI).

Els nivells de maduresa, tant del SGSI com el de l'Anàlisi de Riscos són inicials i requereixen evolucionar per acollir amb més detall els actius, els riscos i l'optimització de les mesures de seguretat existents o futures.

Els progressos aconseguits en la implantació del SGSI són:

- ✔ Precisar l'estat de la Seguretat de la Informació actual en relació als diferents aspectes de la Norma i establir l'abast i objectius.
- ✔ Establir una base documental i determinar les responsabilitats de cada un dels components de l'estructura organitzativa de seguretat, de manera que s'asseguri la realització de totes les tasques necessàries proporcionant revisió i millora.
- ✔ Identificar i inventariar els actius crítics de l'Organització, determinar la magnitud de les amenaces i, en darrer terme, concretar els riscos als que estan exposats els diferents elements dels Sistemes d'Informació de l'Organització.
- ✔ A partir dels riscos trobats, s'han seleccionat i prioritzat un seguit de projectes i mesures que permetran millorar la seguretat de l'Organització.
- ✔ Aquest SGSI s'ha plantejat com un procés de millora contínua en constant actualització i renovació seguint el model PDCA (plan-do-check-act).

Annexes

Annexe I – Anàlisi diferencia ISO/IEC 27002:2013

Anàlisi diferencial en referència als objectius de control de la ISO/IEC 27002:2013. A continuació detallem el llistat amb els als 113 controls o mesures preventives, organitzats en 14 àrees i 35 objectius de control.

AUDITORIA EN SEGURIDAD DE LA INFORMACIÓN

Herramienta de Evaluacion y Diagnostico bajo la Norma ISO/IEC 27002:2013

CRITERIOS DE EVALUACIÓN	
No realizado	0 %
Realizado informalmente	20 %
Planificado	40 %
Bien definido	60 %
Cuantitativamente controlado	80 %
Mejora continua	100 %

Norma	Seccion	Cumplimiento	
5	POLITICAS DE SEGURIDAD	80 %	
5,1	Directrices de la Dirección en seguridad de la información	80 %	
5.1.1	Conjunto de políticas para la seguridad de la información	Cuantitativamente controlado	80 %
5.1.2	Revisión de las políticas para la seguridad de la información	Cuantitativamente controlado	80 %
8	GESTION DE ACTIVOS	44 %	
8,1	Responsabilidad sobre los Activos	65 %	
8.1.1	Inventario de activos.	Cuantitativamente controlado	80 %
8.1.2	Propiedad de los activos.	Cuantitativamente controlado	80 %
8.1.3	Uso aceptable de los activos.	Realizado informalmente	20 %
8.1.4	Devolución de activos.	Cuantitativamente controlado	80 %
8,2	Clasificacion de la Informacion	0 %	
8.2.1	Directrices de clasificación.	No realizado	0 %
8.2.2	Etiquetado y manipulado de la información.	No realizado	0 %
8,3	Manejo de los soportes de almacenamiento	67 %	
8.3.1	Gestión de soportes extraíbles.	Bien definido	60 %
8.3.2	Eliminación de soportes.	Bien definido	60 %
8.3.3	Soportes físicos en tránsito	Cuantitativamente controlado	80 %
9	CONTROL DE ACCESO	65 %	
9,1	Requisitos de negocio para el control de accesos	80 %	
9.1.1	Política de control de accesos.	Cuantitativamente controlado	80 %
9.1.2	Control de acceso a las redes y servicios asociados.	Cuantitativamente controlado	80 %
9,2	Gestión de acceso de usuario.	48 %	
9.2.1	Gestión de altas/bajas en el registro de usuarios.	Bien definido	60 %
9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Bien definido	60 %
9.2.3	Gestión de los derechos de acceso con privilegios especiales.	Cuantitativamente controlado	80 %
9.2.5	Revisión de los derechos de acceso de los usuarios.	Realizado informalmente	20 %
9.2.6	Retirada o adaptación de los derechos de acceso	Realizado informalmente	20 %
9,4	Control de acceso a sistemas y aplicaciones	68 %	
9.4.1	Restricción del acceso a la información.	Cuantitativamente controlado	80 %
9.4.2	Procedimientos seguros de inicio de sesión.	Mejora continua	100 %
9.4.3	Gestión de contraseñas de usuario.	Mejora continua	100 %
9.4.4	Uso de herramientas de administración de sistemas.	Planificado	40 %
9.4.5	Control de acceso al código fuente de los programas	Realizado informalmente	20 %
11	SEGURIDAD FISICA Y AMBIENTAL	62 %	
11,1	Areas Seguras	63 %	
11.1.1	Perímetro de seguridad física.	Cuantitativamente controlado	80 %
11.1.2	Controles físicos de entrada.	Cuantitativamente controlado	80 %
11.1.3	Seguridad de oficinas, despachos y recursos.	Cuantitativamente controlado	80 %
11.1.4	Protección contra las amenazas externas y ambientales.	Bien definido	60 %
11.1.5	El trabajo en áreas seguras.	Bien definido	60 %
11.1.6	Áreas de acceso público, carga y descarga	Realizado informalmente	20 %
11,2	Seguridad de los Equipos	60 %	
11.2.1	Emplazamiento y protección de equipos.	Cuantitativamente controlado	80 %
11.2.2	Instalaciones de suministro.	Bien definido	60 %
11.2.3	Seguridad del cableado.	Cuantitativamente controlado	80 %
11.2.4	Mantenimiento de los equipos.	Bien definido	60 %
11.2.5	Salida de activos fuera de las dependencias de la empresa.	Planificado	40 %
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Cuantitativamente controlado	80 %
11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	Cuantitativamente controlado	80 %
11.2.8	Equipo informático de usuario desatendido.	No realizado	0 %
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Bien definido	60 %
12	SEGURIDAD EN LA OPERATIVA	80 %	
12,2	Protección contra código malicioso	100 %	
12.2.1	Controles contra el código malicioso.	Mejora continua	100 %
12,3	Copias de seguridad	60 %	
12.3.1	Copias de seguridad de la información	Bien definido	60 %
13	SEGURIDAD EN LAS TELECOMUNICACIONES	48 %	
13,1	Gestión de la seguridad en las redes.	60 %	
13.1.1	Controles de red.	Planificado	40 %
13.1.2	Mecanismos de seguridad asociados a servicios en red.	Bien definido	60 %
13.1.3	Segregación de redes.	Cuantitativamente controlado	80 %
13,2	Intercambio de información con partes externas.	35 %	
13.2.1	Políticas y procedimientos de intercambio de información.	Realizado informalmente	20 %
13.2.2	Acuerdos de intercambio.	Planificado	40 %
13.2.3	Mensajería electrónica.	Planificado	40 %
13.2.4	Acuerdos de confidencialidad y secreto	Planificado	40 %
14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	40 %	
14,2	Seguridad en los procesos de desarrollo y soporte	40 %	
14.2.1	Política de desarrollo seguro de software.	Realizado informalmente	20 %
14.2.6	Seguridad en entornos de desarrollo.	Bien definido	60 %
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Realizado informalmente	20 %
14.2.9	Pruebas de aceptación	Bien definido	60 %

Annexe II – Política de Seguretat

Política de Seguretat

Data publicació	Nom	Signatura
17/03/2019	Responsable de Seguretat	TI Aprovació autor
18/03/2019	Responsable IT	TI Aprovació

Històric de canvis

Versió	Data publicació	Editor	Estat	Comentaris
01.00	13/03/2019	CISO	Inicial	Versió inicial
01.01	16/03/2019	CISO	Final	Versió final

Index

Resum de la política

SCRIPTIX és una consultora multinacional que ofereix solucions de negoci, estratègia, desenvolupament i manteniment d'aplicacions tecnologies i outsourcing.

Els professionals, la informació i el coneixement són els actius principals de de la companyia. També cal considerar com actius crítics els centres de treball e instal·lacions, i als nostres col·laboradors i proveïdors atès que són el suport a les nostres activitats de negoci.

Les premisses fonamentals de la Política de Seguretat de la Informació Corporativa de SCRIPTIX són:

- ✔ La protecció i seguretat de les persones i dels nostres actius clau, i la garantia de continuïtat de les nostres operacions de negoci.
- ✔ El compliment de la legislació local en els països en els que opera, les regulacions sectorials que li apliquen, i els requeriments dels nostres clients en matèria de seguretat.

Abast

Aquesta política serà d'aplicació a totes les empreses que pertanyen al grup SCRIPTIX.

En tot el document, qualsevol referència a «SCRIPTIX» o a la «Companyia», es referirà al àmbit descrit anteriorment.

Sempre que no s'esmenti el contrari de forma explícita, estaran subjectes en aquesta política;

- Tots els processos de negoci i el suport al negoci de SCRIPTIX
- Tot el personal que presta servei en SCRIPTIX, incloent directius, empleats i col·laboradors externs.
- Qualsevol informació en el àmbit de SCRIPTIX i sistemes d'informació o suport en el que es trobi. Per exemple, en format electrònic, com a document imprès o, inclús, informació no registrada en altres mitjans com la veu i els coneixements de les persones.
- Totes les instal·lacions propietat de SCRIPTIX, o sota el seu control, en la que SCRIPTIX desenvolupi alguna activitat.

Organització de la Seguretat Corporativa

Àrees de Seguretat Corporativa

És l'àrea encarregada de dirigir la gestió de la Seguretat Corporativa en tot SCRIPTIX. Aquesta àrea presta servei directament a SCRIPTIX. Per això, forma part de l'àrea de Suport a Negoci (BSA – Business Support Area en anglès).

Les seves principals funcions són:

- Definir la estratègia de Seguretat Corporativa, alineada amb els seus Objectius de Negoci.
- Establir i mantenir la Política de Seguretat Corporativa que donin suport a l'esmentada estratègia.
- Coordinar la col·laboració amb el Grup SMURF en matèria de Seguretat Corporativa.
- Crear una cultura de la seguretat a través de la definició, desenvolupament i gestió d'un programa de formació i conscienciació
- Establir els controls tècnics corporatius (objectius de control, controls i mètriques).
- Proporcionar suport per identificar els requeriments de seguretat en les noves iniciatives i aplicacions internes de SCRIPTIX, i per a la implantació de controls a través d'assessorament expert.
- Donar resposta davant incidents de seguretat.
- Donar suport a auditories externes referent a la seguretat corporativa.
- Planificar i coordinar la realització d'auditories tècniques de seguretat.
- Informar regularment del estat de la seguretat corporativa a l'alta direcció de SCRIPTIX.

L'àrea de Seguretat Corporativa està dirigida per un Chief Information Security Officer (CISO). Les responsabilitats del CISO són les següents:

- Liderar l'àrea de Seguretat Corporativa de SCRIPTIX.
- Supervisar les activitats relacionades amb la seguretat corporativa, d'acord amb l'establert en la política de seguretat corporativa de SCRIPTIX.

- Liderar el Comitè de Seguretat Corporativa de SCRIPTIX.

Addicionalment, el CISO és nombrat com a responsable de les mesures de seguretat per a la protecció de dades personals en tota la Companyia. Com a conseqüència recauen sobre el CISO les següents responsabilitats:

- Conscienciació pel que fa a les mesures de seguretat per a la protecció de les dades personals:
  - Actuar com a punt de contacte únic per a la gestió de queixes i peticions d'assessorament.
  - Planificar accions de formació i conscienciació pel que fa a les mesures de seguretat per a la protecció de dades personals.

Elaborar les guies i normes de seguretat, per a entendre i gestionar adequadament les necessitats particulars de cada negoci de SCRIPTIX i la realitat de cada país en el que es disposen de centres de treball, l'àrea de Seguretat Corporativa es recolzarà en els responsables de seguretat específics:

- En cada país, es designarà un Local Information Security Officer (LISO).
- En cada Initiative, es designarà un Business Information Security Officer (BISO).

L'àrea de Seguretat Corporativa no delegarà cap responsabilitat sobre la Seguretat de la Informació en la figura de LISO i BISO.

L'àrea de Seguretat Corporativa es recolzarà en BISOs i LISOs per:

- Proporcionar un punt de contacte en matèria de seguretat, que serveixi d'enllaç amb l'àrea de Seguretat Corporativa.
- Detectar canvis o noves activitats que haurien de ser conegudes per Seguretat Corporativa i així poder aplicar les mesures de seguretat adequades.
- Assegurar la implementació de les mesures de seguretat en el seu àmbit i realitzar el corresponent seguiment d'aquestes.

Àrees que implementen la Seguretat Corporativa

La responsabilitat sobre l'execució de les mesures i controls definits per l'Àrea de Seguretat Corporativa està distribuït en tot l'organigrama de SCRIPTIX.

L'àrea de Seguretat Corporativa coordinarà amb tots ells la implantació i execució de les mesures definides en la Política de Seguretat Corporativa.

Comitè de Seguretat Corporativa

El Comitè ha d'assegurar que el punt de vista de tota la Organització es te en compte en les decisions respecte a la Seguretat Corporativa, i facilitat la implementació de l'establert en la Política de Seguretat Corporativa de SCRIPTIX en tota la Organització.

Per a aconseguir-ho, està liderat per l'Àrea de Seguretat Corporativa (CISO) i constituït pels màxims responsables de totes les àrees en l'abast de la Seguretat Corporativa. Les seves principals parts interessades interns:

- BSA (Business Support Area)
  - Chief Risk Officer
  - Corporate Law, Compliance & Risk
  - IT Chief Information Officer
- Personal
- Business
  - CEOs regionals
  - Production & Delivery
  - Centres
  - BPO
  - Initiatives
- Auditoria Interna

El Comitè celebrarà reunions ordinàries, convocades anualment, i reunions de extraordinàries a petició del CISO, quant sigui necessari. Les reunions extraordinàries podran requerir únicament la presència de un conjunt limitat de membres de Comitè que es vegin afectats pels temes a discutir en la reunió, tot i que les conclusions es distribuiran a tots els membres.

Els membres del Comitè hauran de discutir i avaluar els següents aspectes:

- Creació i revisió de les polítiques de seguretat.

- Aspectes de seguretat que hagin de ser tractats de manera prioritària.
- Desplegament unificat de les mesures de seguretat en tot SCRIPTIX.
- Plans de formació i conscienciació sobre seguretat a nivell corporatiu.
- Estat dels incidents greus de seguretat de la informació.
- Accions disciplinàries/legals després d'un incident de seguretat greu.
- Els resultats de les auditories de seguretat.
- La implementació d'un Pla de Continuïtat de Negoci i els resultats de les seves proves.
- Canvis en SCRIPTIX amb impacte en la seguretat.

Cos normatiu de la seguretat en SCRIPTIX

Els aspectes concrets i detalls de la implementació en l'establert en aquesta Política es definiran a procediments corporatius específics, sota responsabilitat de les àrees que tenen com a objectiu la implementació de la Seguretat Corporativa.

Excepcions

Queden establertes les següents excepcions a l'establert en aquesta política:

i. En cas d'emergència, catàstrofe o qualsevol altre esdeveniment que afecti o posi en risc vides humanes.

ii. Si així es requerit per alguna llei o regulació, o sota ordre judicial. En aquests casos haurà de quedar documentat l'abast de l'excepció.

iii. En el supòsit d'impossibilitat tecnològica. La excepció només podrà ser temporal, i haurà de ser aprovada en el Comitè de Seguretat Corporatiu juntament amb un Pla d'Acció que elimina l'excepció en un temps raonable.

iv. En la prestació de serveis a clients prevaldran sempre les polítiques especifiques que s'haguessin acordat amb el client.

Tota excepció a aquesta Política en qualsevol altre cas diferent dels exposats suposarà una violació de la mateixa, i haurà de ser denunciada pel CISO l'abans possible davant el Comitè de Seguretat Corporativa.

Informació

La informació és un actiu clau per a la Organització. Per aquest motiu, tots els empleats i col·laboradors de SCRIPTIX han de protegir la informació que es manega segons les necessitats específiques dels seus propietaris respecte la seva confidencialitat, integritat i disponibilitat; evitant posar-la en risc a l'utilitzar-la.

Addicionalment, cal protegir amb especial atenció la informació que contingui dades de caràcter personal i tota aquella subjecte a drets de propietat intel·lectual.

Rols i responsabilitats rellevants

- **Origen de la informació**. És la persona o entitat que posseeix i te complet dret sobre la informació, i que permet a SCRIPTIX utilitzar-la amb un propòsit concret i sota unes condicions determinades.
- **Propietari de la informació**. És un empleat de SCRIPTIX, identificat pel seu carreg organitzatiu, i que es responsabilitza davant l'*origen de la informació*.

- **Usuari de la informació**. És una persona o persones a las que el responsable de la informació permet accedir-hi. La informació només es podrà modificar segons ho especifiqui el *propietari de la informació*.

Classificació de la informació segons la seva confidencialitat

Es defineix la següent classificació de la informació segons el grau de confidencialitat, entesa com la necessitat de control de qui només qui disposa d'autorització per part del propietari de la informació te accés a ella:

- **[Confidencial]**: Correspon a la informació amb requeriments de confidencialitat molt alt. Només es divulgarà dintre de l'abast fixat pel propietari de la informació.
- **[Restringit]**: Correspon a la informació amb requeriments de confidencialitat alt.
- **[Ús intern]**: Correspon a la informació amb requeriments de confidencialitat baix.
- **[Públic]**: No te requeriments de confidencialitat. Qualsevol persona pot accedir a la informació.

Controls de Seguretat Corporativa

Adquisició / recollida de la informació

Tota la informació tindrà assignat un propietari.

El propietari de la informació determinarà la classificació de la informació segons l'indicat en aquesta Política de Seguretat.

Si la informació conté:

- Informació de clients
- Informació d'altres empreses o
- Secrets comercials de SCRIPTIX,

es considerarà sempre com a [Confidencial].

Si la informació conté dades de caràcter personal especialment sensible, tal com religió, raça, condició o orientació sexual o inclinacions polítiques es considerarà sempre com a [Confidencial].

En funció de la classificació de la informació, el propietari de la informació:

- Definirà a qui es permet accedir a la informació.

- Gargaritzarà que, juntament amb la informació, s'especifica clarament la seva classificació, a qui es permet divulgació, qui és el propietari i a quina empresa pertany.

El propietari de la informació ha d'especificar com pot emmagatzemar-se la informació i de què manera, d'acord a la classificació de la informació i la legislació / regulació aplicable.

El propietari de la informació podrà fixar el període màxim de conservació de la informació, d'acord la legislació / regulació aplicable. Després d'aquest període la informació haurà de ser eliminada.

Quant sigui necessari recollir dades de caràcter personal per al seu ús per part de SCRIPTIX, s'ha d'explicar el motiu, com serà processada, qui tindrà accés i on cal dirigir-se per a gestionar qualsevol aspecte relacionat amb les seves dades.

Si la informació conté dades de caràcter personal, el propietari de la informació ha de garantir que tots els empleats i col·laboradors externs amb accés a la informació són informats del propòsit pel qual es va recollir la informació i el seu ús autoritzat.

Si es genera nova informació mitjançant la combinació de informació amb diferent classificació, se li assignarà la classificació més restrictiva de les combinades.

Ús i distribució de la informació

La informació amb dades de caràcter personal només pot ser utilitzada per al propòsit notificat. Si fos necessari fer un ús diferent després d'haver-los recollit, s'haurà de descriure de manera clara el nou propòsit i notificar-ho a les persones afectades.

Si la informació ha de ser tractada mitjançant sistemes informàtics, aquests hauran de comptar amb les mesures de seguretat per a controlar l'accés i la modificació no autoritzada o accidental de la informació. L'abast de les mesures de seguretat es determinaran mitjançant un anàlisi de riscos.

Els usuaris de la informació hauran:

- D'acatar les normes de tractament de la informació d'acord amb la seva classificació i posar especial atenció en el tractament de les dades personals.
- Respectar l'abast de l'accés permès pel propietari de la informació.
- Evitar reproduir la informació sense autorització.
- No deixar informació accessible, sota cap suport independentment de la seva classificació.
- Evitar que la informació classificada pugui ser observada per persones no incloses en els criteris d'accés.

- Evitar fer comentaris sobre informació classificada atès que podrien ser escoltats per persones no incloses en l'abast d'accés permès.

En qualsevol cas, independentment de la classificació, no es permès la realització de canvis en la informació quant aquesta contingui l'advertència «*Es prohibeix l'alteració o modificació d'aquesta informació*».

Només el propietari de la informació podrà canviar la seva classificació i l'abast de l'accés permès.

En cas de ser necessari la distribució d'informació classificada com a [Confidencial], cal adoptar les mesures necessàries per evitar accessos no autoritzats;

- Xifrat del contingut en el cas d'haver de distribuir la informació mitjançant una xarxa externa.
- Sol·licitar confirmació de recepció quant la informació sigui transmesa de manera física mitjançant correu (intern o extern) o algun altre mitjà que no garanteixi que l'entrega es realitza al destinatari desitjat.

Si per requeriments fos necessari divulgar informació fora de l'abast d'accés permès, caldrà sol·licitar autorització prèvia al propietari de la informació.

Emmagatzematge

Els suports utilitzats per emmagatzemar informació s'hauran de protegir d'acord la classificació de la informació que contingui i l'abast d'accés permès.

En cap cas, la informació pot emmagatzemar-se en dispositius i sistemes personal de caràcter privat (p.e: equips personals, discos durs portàtils o pen-drives personals, emmagatzematge en en núvol propietat de l'usuari, etc.).

Destrucció de la informació

Un cop finalitzar el període de conservació fixat pel seu propietari, o quant deixi de ser necessària, la informació classificada ha de ser destruïda ràpidament mitjançant el mètode conforme al tipus d'informació basat en la confidencialitat:

- Informació impresa: es destruirà el paper per mitjà de qualsevol procediment que eviti la recuperació de la informació. Si el document estigués arxivat, el propietari de la informació haurà de sol·licitar la seva destrucció al àrea responsable de l'Arxiu.
- Informació en suport electrònic: el propietari de la informació sol·licitarà l'esborrat segur o la destrucció completa del suport que la contingui, sense existir possibilitat de recuperació.

Empleats

La seguretat dels actius claus de SCRIPTIX te la seva base fonamental en tots els seus empleats.

Tots els empleats de SCRIPTIX han de conèixer, comprendre, comprometre's i complir amb l'establert en la Política de Seguretat Corporativa.

Rols i responsabilitats rellevants

- **Empleat**: Manté una relació laboral directa amb SCRIPTIX, ja sigui personal d'staff , gerents, directors o socis.
- **Chief Compliance Officer**: Lidera les accions relacionades amb el compliment normatiu i assessora als empleats en aquesta matèria.

Controls de Seguretat Corporativa

Procés de contractació

Tot empleat de SCRIPTIX haurà de signar una declaració en el moment de la seva contractació en la que es compromet a:

- Respectar l'establert en la Política de Seguretat Corporativa, legislació i regulacions en les que SCRIPTIX estigui implicada per la seva ubicació o activitat durant la seva relació laboral amb SCRIPTIX.
- Retornar tots els suports de informació i sistemes informàtics que SCRIPTIX li hagi proporcionat i no conservar informació propietat de SCRIPTIX en cap suport a la finalització del contracte laboral. Mantenir la confidencialitat i respectar els drets de propietat intel·lectual de tota la informació de la que tingui coneixement.

Formació i conscienciació

L'àrea de Seguretat Corporativa prepararà els continguts i materials necessaris per impartir programes de formació i conscienciació sobre seguretat de la informació, dirigits a:

- Noves incorporacions, amb l'objectiu de conscienciar sobre la necessitat de tractar la informació de manera segura.
- Tots els empleats, amb l'objectiu de que comprenguin els objectius de seguretat de la informació i com aplicar la política de seguretat en el seu dia a dia.
- Personal directiu, per a garantir que aquest col·lectiu sigui conscient, comprengui el seu rol i les seves responsabilitats de cara al manteniment i millora de SCRIPTIX com a entorn segur.

SCRIPTIX celebrarà sessions de formació i conscienciació sobre seguretat de la informació de manera planificada a tots els empleats i a col·lectius específics segons es consideri necessari. Addicionalment es mantindran registres d'aquestes sessions.

Els gerents, directors i socis hauran de servir com a guia i model d'aplicació de la política de seguretat per a la resta d'empleats – especialment, per aquells sota la seva gestió i supervisió – a través de formació, assessorament presencial i altres mitjans per assegurar el compliment de la política i les normes de seguretat.

Fi de la relació laboral

El procés de finalització de la relació laboral entre un empleat i SCRIPTIX ha de contemplar:

- La sol·licitud de bloqueig de l'accés de l'usuari a tots els sistemes i xarxes als que tingués accés, i la revocació de tots els permisos d'accés.
- La devolució de tots els actius, sistemes informàtics i suports d'emmagatzematge que se li hagués proporcionat.
- La signatura d'un document per part de l'empleat en el que declara haver esborrat qualsevol informació de la que pugues disposar com a conseqüència de la seva relació laboral amb SCRIPTIX i que estigui emmagatzemada en qualsevol dispositiu no propietat de SCRIPTIX.
- La recollida de la seva targeta d'empleat i revocació dels permisos d'accés físic a qualsevol instal·lació de SCRIPTIX.

SCRIPTIX haurà de conservar en l'expedient de l'empleat un registre que totes aquestes accions s'han realitzat, juntament amb la declaració signada d'esborrat d'informació en dispositius no propietat de la companyia.

Accés Físic

Rols i responsabilitats rellevants

- Àrea de Seguretat Corporativa. Defineix la política de seguretat física aplicable i realitza un seguiment del seu desplegament en totes les ubicacions de la companyia.
- Àrea de Facilities Local. Implanta i gestiona les mesures de seguretat física que s'identifiquin com a necessàries en les ubicacions físiques sota la responsabilitat de SCRIPTIX.

Zones de seguretat

S'identifiquen com a zones de seguretat a les distintes seccions dintre de les instal·lacions propietat de SCRIPTIX o sota la seva responsabilitat, en les que s'adopten mesures específiques de protecció i contro d'accés físic en funció de l'activitat que es realitza.

Les zones de seguretat es classificaran com:

- **Pública**: Seran aquelles zones annexes a instal·lacions d'ús exclusiu de SCRIPTIX, be siguin d'ús compartit amb altres empreses bé sigui d'ús public.
- **Interna**: Són aquelles zones en las que es realitza la majoria de la feina per part del personal de SCRIPTIX
- **Restringida**: Són les zones en les que es realitza treballs específics d'alta sensibilitat per la informació que es tracta en elles.
- **Especialment protegides**: Són les zones que requereixen la més alta protecció i mesures de seguretat molt específiques pel tipus d'informació o actius inclouen.

Factors vàlids d'identificació per a l'accés físic

- **Document d'identitat**: Un document expedit per una autoritat governamental d'àmbit nacional, regional o local que identifiqui inequívocament a la persona mitjançant el seu nom complet i una fotografia.
- **Credencial d'accés físic**: Una targeta controlada per SCRIPTIX que serveixi als empleats com a credencial d'accés físic a les instal·lacions de la companyia.

- **Credencials de visitant**: Una targeta controlada per SCRIPTIX que serveixi al personal visitant com a credencial d'accés físic a les instal·lacions de la companyia. Aquesta targeta sempre tindrà una validesa temporal.

Controls de seguretat Corporativa

Mesures de seguretat per zones

Les zones de seguretat de tipus «*Publica*» contaran amb les següents mesures de seguretat: No requereixen cap mesura específica.

Les zones de seguretat de tipus «*Restringida*» tindran implementades les següents mesures de seguretat:

- El seu perímetre estarà limitat per elements físics de tal manera que l'entrada o sortida només sigui possible a través dels punts d'accés habilitats.
- El perímetre haurà de dificultar la visibilitat des de l'exterior a de l'interior de la zona restringida.

En aquells casos que així es consideri, podran instal·lar-se càmeres de CCTV que, al menys, registrin l'entrada a la zona fora de l'horari laboral. Les imatges emmagatzemades tindran una profunditat d'una setmana.

Les zones de seguretat de tipus «*Especialment protegides*» contaran amb les següents mesures de seguretat:

- El perímetre estarà delimitat per elements físics de tal forma que l'accés només sigui possible a través dels punts d'accés establerts.
- Preferiblement no existiran finestres de cap tipus. Si no fos possible, hauran de disposar d'un sistema que eviti la visibilitat des de l'exterior.
- Existiran punts d'accés autoritzats únicament des de les zones de tipus «*Interna*» o «*Restringida*».
- Hauran de disposar de càmeres de CCTV que registrin l'activitat completa de la zona en tot moment. L'històric de les imatges emmagatzemades serà d'una setmana.
- Podran desplegar-se mesures de seguretat addicionals específiques com a resultat de un anàlisis de riscos.

Com a norma general, tota persona autoritzada haurà de portar visible la seva credencial d'accés físic en l'interior del perímetre de les zones classificades com a no «*Publiques*»

L'àrea de Seguretat Corporativa revisarà que les zones de seguretat disposen de les mesures de seguretat corresponents a la seva classificació i impulsarà la implantació de mesures adequades a cada zona.

Cicle de vida de factors d'autentificació

Cada àrea de Facilities Local identificarà les zones de seguretat en les seves instal·lacions, implantarà i gestionarà el control d'entrada i sortida entre les seves zones segons la seva classificació.

L'àrea de Facilities Local disposarà d'un inventari actualitzat amb totes les zones de seguretat i instal·lacions, el seu ús i les necessitats de negoci.

Es designarà un responsable del control d'accés per a cada zona de seguretat. Les peticions demanant permís d'accés físic s'enviaran al responsable del centre de control d'accés de la zona de seguretat per a la seva aprovació.

Si es fa ús d'un sistema automatitzat per a l'emissió de credencials i alta / baixa de permisos d'accés físic, el seu ús quedarà limitat a un conjunt de persones autoritzades.

Visitants

Les visites no podran accedir a zones classificades sense anar acompanyats per un empleat de SCRIPTIX.

L'entrega d'una credencial de visita, en control d'entrada haurà de:

- Identificar a la persona mitjançant un document d'identitat
- Registrar en el control d'accés d'entrada la seva identitat, data i hora de la visita i persona a la que ve a visitar.

Un cop finalitzada la visita, la persona visitada acompanyarà als visitants a la sortida i s'assegurarà de que es torni la credencial d'accés.

A l'inici de la jornada laboral, el control d'entrada haurà de comprovar si s'han tornat totes les credencials de visitant que hagin expirat, i haurà de registrar la desaparició de targetes mitjançant incidència en el sistema corporatiu de gestió d'incidències.

Col·laboradors externs

A petició d'un gerent, director o soci, es podrà assignar una valides superior a un dia a la credencial de visitant emesa per a un col·laborador extern ocasional, amb un màxim d'un mes.

En el cas de col·laboradors externs on la duració de col·laboració sigui superior a un mes, se li podrà assignar una credencial d'accés físic d'extern.

Accés Lògic

Rols i responsabilitats rellevants

- **Sistema**: Es considera sistema qualsevol aplicació, sistema operatiu de servidor o element de xarxa de comunicacions.
- **Identificació**: Una cadena de caràcters associada de manera única a un usuari (persona o procés) en un sistema i que s'utilitza per a identificar l'ús o accés que un usuari fa.
- **Autentificació simple**: Per a validar que un usuari és legitim posseïdor d'una identificació, es sol·licitarà que demostri la seva identitat mitjançant:
  - Conèixer un secret compartit entre l'usuari i el sistema (p.e: una contrasenya)
  - Posseir un objecte físic que el sistema associa de manera única amb un usuari (p.e: un token de seguretat)
  - Disposar d'una característica física única (p.e: empremta dactilar) registrada amb anterioritat en el sistema.
- **Autentificació de doble factor**: Per a disposar d'un major grau de confiança en el procés de validació, es podrà sol·licitar que es demostri la identitat mitjançant la comunicació de 2 tipus d'autentificació simple diferents.

Controls de Seguretat Corporativa

Identificació i autentificació

Es disposarà d'un repositori corporatiu únic d'identificadors d'usuari així com de les contrasenyes associades.

Es disposarà de procediments de gestió d'identificadors d'usuari i els seus mecanismes d'autentificació associats.

El sistema d'autentificació serà escollit segons els risc:

- Com a norma general, s'utilitzarà la autentificació simple mitjançant l'ús d'un secret compartit.
- Es preferiran sistemes de doble factor d'autenticació quant es desitgi mitigar riscos concrets (p.e: suplantació d'identitat, repudi, etc.)
- Es podrà permetre l'accés a la informació o ús de serveis sense comprovació d'identitat de l'usuari quant es permeti la consulta d'informació pública.

Els sistemes que utilitzin autentificació biomètrica hauran d'emmagatzemar de manera xifrada. Addicionalment hauran de controla l'accés a aquesta informació tenint en compte que es considerada informació personal.

Contrasenyes

Es proporcionarà els sistemes necessaris per a que un usuari pugui canviar la contrasenya sota demanda.

El sistema de canvi de contrasenya implementarà restriccions en l'elecció de la contrasenya segons es consideri a nivell corporatiu per a garantir la robustesa mínima del password.

Quant una contrasenya es reinicii, s'haurà:

- Generar una contrasenya d'un sol ús i que l'usuari haurà de canviar la primera vegada que la faci servir
- Permetre a l'usuari que escolleixi la seva contrasenya directament i sense intervenció de cap altra persona.

Una contrasenya no s'ha d'emmagatzemar de manera fàcilment accessible.

Com a norma general, la contrasenya s'hauria de canviar de manera periòdica i sempre que existeixi la sospita que pugui ser coneguda per algú més que el propietari.

Cicle de vida dels comptes d'usuari i permisos

Abans de crear una compte d'usuari o donar permisos d'accés, l'administrador del sistema haurà d'assegurar que la persona te autorització per accedir i utilitzar la informació amb els privilegis demanats.

Al concedir permisos d'accés, s'ha d'informar a la persona interessada de l'abast de l'ús no autoritzat, de les polítiques, normes i procediments que ha de respectar.

L'administrador del sistema podrà revocar els permisos o bloquejar l'accés al sistema, en el cas que es detecti qualsevol ús inadequat. Addicionalment es registrarà l'incident de seguretat en el sistema de gestió d'incidències.

Els permisos d'accés hauran de ser eliminats, i en cas de necessitat el compte haurà de ser bloquejat si:

- Ho sol·licita el propietari de la informació.
- Finalitza la necessitat de negoci.
- L'empleat no accedeix durant un temps prolongat.
- Canvien les funcions del propietari del compte i ja no requereix de l'accés.
- Finalitza la relació laboral del propietari del compte amb SCRIPTIX.

Dispositius de l'usuari

Rols i responsabilitats rellevants

- **SCRIPTIX IT**. Estableix acords amb proveïdors de dispositius i programari per al seu ús a nivell corporatiu.
- **IT Local**. Adquireix i gestiona els dispositius d'usuari que utilitzarà el personal dintre del seu àmbit local, seguint els criteris i pautes marcades per SCRIPTIX IT.
- **Chief Compliance Officer**. Lidera les accions relacionades amb el compliment normatiu i assessora als empleats en aquesta matèria.

Controls de Seguretat Corporativa

Requeriments de seguretat de un dispositiu d'usuari

Tot dispositiu d'usuari ha de disposar de les mesures de seguretat adequades a la informació que manega i als riscos als que està exposat. Com a mínim:

- Els PC (Personal Computer) d'escriptori i portàtils hauran:

  - Disposar de bloqueig de pantalla per inactivitat que requereixi un factor d'autentificació per al seu desbloqueig.
  - Disposar de la protecció anti-malware aprovada a nivell corporatiu.
- Els portàtils hauran de xifrar totes les dades de l'usuari emmagatzemades en el dispositiu.
- Les tablets i smartphones hauran de disposar de:
  - Bloqueig de pantalla per inactivitat que requereixi un factor d'autentificació per al seu desbloqueig.
  - D'un sistema que permeti a SCRIPTIX esborrar el seu contingut de manera remota.

La protecció anti-malware:

- Escanejarà periòdicament l'equip per cercar malware.
- Revisarà pro-activament qualsevol fitxer procedent de l'exterior (p.e: suports físics, Internet, etc.)
- Haurà d'estar permanentment actiu i actualitzat.
- No podrà ser deshabilitat.

Tot dispositiu d'usuari haurà de disposar de tots els parxes de seguretat publicats pels diferents proveïdors, a excepció que aquestes actualitzacions provoquin alguna incompatibilitat o dificultin greument l'ús del programari o de l'equip.

Cicle de vida d'un dispositiu d'usuari

Haurà d'existir un inventari corporatiu on quedin identificats tots els dispositius d'usuari, i que registri:

- Un identificador únic
- A quin Centre de Treball pertanyen
- Si estan assignats a un empleat o extern i a qui s'ha entregat
- Si s'han entregat a un extern, què empleat de SCRIPTIX es responsabilitza

Els responsables de l'inventari de dispositius de IT Local hauran de registrar tots els dispositius d'usuari en l'inventari des de el moment de la seva compra.

Els responsables de l'inventari de IT Local hauran d'assegurar que tot dispositiu no assignat a un empleat o extern està emmagatzemat en un contenidor tancat al que només ells podran accedir.

Abans d'entregar un dispositiu d'usuari, els responsables de l'inventari de dispositius d'usuari de IT Local hauran d'assegurar-se que l'empleat signa una declaració en la que es compromet a:

- Custodia del dispositiu i protegir-lo de qualsevol dany
- Utilitzar el dispositiu estrictament per activitats de SCRIPTIX i no per a fins particulars
- Utilitzar-lo segons l'establert en aquesta política.
- Retornar-lo al responsable de l'inventari de IT Local quant així ho requereixi SCRIPTIX

Específicament, es prohibeix l'ús de:

- Màquines virtuals que no tinguin una imatge de sistema operatiu securitzat per SCRIPTIX IT
- dispositius en els que s'hagi eliminat els mecanismes de seguretat del fabricant

Tota persona que tingui un dispositiu d'usuari amb informació de SCRIPTIX haurà de prendre les mesures necessàries per evitar la pèrdua o robatori del dispositiu. En cas de pèrdua o robatori, s'haurà d'informar immediatament mitjançant incidència en el sistema corporatiu de gestió d'incidències.

Tot programari instal·lat en un dispositiu d'usuari que requereixi llicència d'ús:

- Ha d'haver estat aprovada per SCRIPTIX per al seu ús professional
- SCRIPTIX ha de disposar de les llicències vàlides que permetin l'ús que es realitzarà del programari.

Està prohibit l'ús o la instal·lació de programari que pugui suposar un risc per a l'ús professional del dispositiu. Específicament, està prohibida la instal·lació o el ús d'aplicacions no corporatives d'intercanvi de fitxers.

Preferentment, es protegirà mitjançant xifrat tota la informació classificada emmagatzemada en un dispositiu portàtil d'emmagatzematge.

La informació amb dades de caràcter personal emmagatzemada en un dispositiu portàtil d'emmagatzematge haurà de protegir-se sempre mitjançant xifrat si es transporta el dispositiu fora de la zona de seguretat de SCRIPTIX.

La informació classificada emmagatzemada en un dispositiu portàtil d'emmagatzematge ha e ser esborrada del dispositiu immediatament en el moment que deixi de ser necessària.

SCRIPTIX podrà monitorar o revisar l'ús d'un dispositiu d'usuari per a detectar usos no autoritzats.

Quant es decideixi que un dispositiu d'usuari deixarà d'utilitzar-se en la companyia, s'haurà d'assegurar que s'eliminen del dispositiu totes les dades que contingui mitjançant un sistema que impedeixi la seva posterior recuperació.

Servidors i software base

Rols i responsabilitats rellevants

- **Àrea de Seguretat Corporativa**. Proporciona suport expert per a la implementació dels controls de seguretat, en línia amb l'indicat en aquesta Política i realitzar les revisions per a comprovar la seva efectivitat i detectar línies de millora.
- **Responsable del Sistema**. Persona o grup de persones encarregades de la administració de un sistema i de controlar el seu adequat ús.

Controls de Seguretat Corporativa

Tot sistema haurà de tenir un responsable assignat que identificarà si és necessària la seva classificació, s'encarregarà de la seva administració i controlarà l'ús adequat.

SCRIPTIX mantindrà un inventari corporatiu de sistemes, de forma que disposi d'un registre actualitzat de tots els seus sistemes amb les característiques dels servidors físics, el programari base i la seva versió, la seva classificació, el seu responsable i aplicació o aplicacions a las que dona servei.

Securització

El responsable del sistema assegurarà que el seu software base està securitzat segons s'especifiqui en el procediment de securització aplicable. En tot cas, en el software base s'haurà:

- Ajustar la configuració per a complir en l'establert respecte l'accés lògic en aquesta política.
- Eliminar, bloquejar o deshabilitat qualsevol programari innecessari.
- Eliminar, si és possible, tots els usuaris existents per defecte que no siguin necessaris, i canviar totes les contrasenyes per defecte dels usuaris que romanguin.
- Comprovar que no existeixen funcionalitat i serveis que no siguin necessaris.
- Deshabilitar o bloquejar els ports de comunicacions que rebin peticions.
- Instal·lar un sistema anti-malware segons correspongui al software base. Aquest sistema anti-malware haurà de:
  - Estar sempre actiu i actualitzat.
  - Realitzar escanejos regularment
  - Evitar, detectar, eliminar o recuperar el sistema davant atacs de malware.

Xarxes de Comunicacions

En SCRIPTIX s'utilitzen xarxes de comunicacions per a l'intercanvi d'informació tant internament com externament (amb clients) i Internet per a obtenir informació pública.

Per això es controla la connectivitat en la xarxa, per evitar accessos no autoritzats a la informació de la companyia i dels clients, per a prevenir usos indeguts de recursos i evitar danys a la capacitat operativa de la companyia i dels seus clients.

Rols i responsabilitats rellevants

- **SCRIPTIX IT**. Es responsabilitza de la creació, administració, separació i interconnexió de es xarxes, mantenint un inventari corporatiu d'aquestes, monitorització del seu funcionament i estar actualitzats de les mesures de seguretat desplegades en aquestes.
- **Responsable de la Xarxa**. Persona o grup de persones encarregades de controla l´ús adequat de la xarxa.

Controls de Seguretat Corporativa

SCRIPTIX IT designarà un responsable de la xarxa que es responsabilitzarà de controlar el seu adequat ús.

SCRIPTIX IT ha de mantenir:

- Un inventari de les xarxes de la companyia.
- Un mapa de xarxes amb els elements existents en la xarxa i la connectivitat entre xarxes internes i externes.

Les xarxes s'hauran de dividir en sub-xarxes tenint en compte el seu propòsit i nivell de seguretat que requereixin en funció de l'ús o de la informació que es trobi en els sistemes connectats.

Es mantindrà un registre de canvis en la configuració i en la topologia de xarxes i sub-xarxes per a possibles investigacions de seguretat.

Connexió entre xarxes

Al connectar xarxes internes, el responsable de la xarxa haurà de fer-ho sempre ajustant-se a les condicions de ambdós xarxes, i haurà d'instal·lar mecanismes de identificació, autentificació, control d'accés, etc. en funció del tipus de informació.

La connexió d'una xarxa interna amb una externa:

- Requerirà autorització de SCRIPTIX IT
- Mai serà directa, sinó que s'inclourà una DMZ (Zona Desmilitaritzada) entre ambdós xarxes i en el que no es podrà realitzar processos de dades de negoci i els recursos emmagatzemats seran temporals.
- S'ha d'implementar una separació lògica entre la xarxa interna i la DMZ, i mesures de seguretat per evitar l'accés no autoritzat des de l'exterior.

Control d'accés a les xarxes

Independentment de la connectivitat entre sub-xarxes, no es podrà connectar una sub-xarxa de un propòsit determinat un sistema que serveix per a un propòsit diferent.

Els següents sistemes hauran d'estar en sub-xarxes separades:

- Dispositius d'usuari.
- Servidors que suportin processos de negoci o gestió interna de SCRIPTIX.
- Servidors que presten servei a clients.
- Servidors de desenvolupament.
- Telefonia IP i videoconferència.

L'accés d'un usuari des de una xarxa externa a una xarxa interna haurà de validar la connexió mitjançant el doble factor d'autenticació i mai es permetrà l'accés a recursos que l'usuari no tindria accés sota connexió directa.

Com a norma general, l'accés a la xarxa mitjançant tecnologia Wireless només està permès per a les xarxes d'usuari de SCRIPTIX. Aquests accessos requeriran verificar la identitat de l'usuari mitjançant ID de usuari i contrasenya.

Ús de les xarxes

Abans de proporcionar accés a una xarxa, el responsable de la xarxa haurà d'assegurar-se que l'usuari coneix les normes, guies i procediments operatius específics.

Els usuaris han de fer un ús responsable de la xarxa, acord la política de seguretat i les normes, guies i procediments operatius específics, i no utilitzar-la per a fins personals perjudicant les activitats de negoci ni accedir a informació d'altres usuaris de la xarxa.

No és permès l'ús de la xarxa per a usos contraris a la legislació vigent.

S'ha de disposar d'un sistema de monitorització que permeti detectar un intent o un accés / ús no autoritzat.

El responsable de la xarxa ha de reportar qualsevol accés o ús no autoritzat que detecti l'abans possible mitjançant l'apertura d'un incident de seguretat en el sistema corporatiu de gestió d'incidències.

Gestió d'Incidents de Seguretat

La política de seguretat corporativa estableix l'estratègia, objectius de control i controls per a protegir els actius clau de la companyia. Un incompliment d'aquesta política suposa l'exposició a riscos.

Rols i responsabilitats rellevants

- **Àrea de Seguretat Corporativa**. Revisa periòdicament els mecanismes de monitorització, dirigeix la gestió d'incidents de seguretat i realitza un seguiment de les mesures implantades derivades d'un incident.
- **Comitè de Seguretat Corporativa**. Avalua la possibilitat de prendre accions legals o disciplinàries després de la resolució d'un incident greu.

Controls de Seguretat Corporativa

Monitorització

S'implantaran tots els sistemes de monitorització que siguin necessaris amb l'objectiu de detectar els següents incidents de seguretat:

- Infraccions legals o o de regularització.
- Atacs a sistemes d'informació (accessos no autoritzats, suplantació, etc.).
- Existència de malware en els sistemes d'informació.

- Ús de sistemes personals i que dificulten l'execució del negoci.
- Violació de la política de seguretat, normes internes i altres actes indeguts.

Es limitarà l'abast de la monitorització al mínim necessari, i els mitjans empleats seran els mínims imprescindibles per assolir l'objectiu de manera adequada.

La monitorització es durà a terme garantit el respecte per la privacitat dels empleats i col·laboradors externs.

Els sistemes de monitorització emmagatzemaran registre de la monitorització per a posteriors investigacions en cas d'incident de seguretat.

Detecció i registre d'un incident de seguretat

Qualsevol empleat de la companyia o col·laborador extern que detecti la existència d'un incident de seguretat o tingui indicis que pogués produir-se, haurà de notificar-lo l'abans possible mitjançant el sistema corporatiu de gestió d'incidents.

Un cop registrada la incidència, s'escalarà fins la seva resolució seguint el procediment corporatiu de Gestió d'Incidents de Seguretat.

Després de la resolució d'un incident greu, o en el cas que un incident lleu es repeteixi de manera recurrent, l'àrea de seguretat corporativa haurà de:

- Identificar la causa de l'incident.
- Analitzar les mesures que s'haurien de prendre per a evitar la seva recurrència.
- Assegurar la implementació d'aquestes mesures.

Continuïtat del Negoci

Rols i responsabilitats rellevants

- **Àrea de Seguretat Corporativa**. Proposa la estratègia global de Continuïtat de Negoci, redacta els plans associats, coordina l'adquisició de recursos e implanta els procediment de preparació necessaris, dissenya i coordina l'execució de proves del PCN, i l'actualitza quant és necessari.
- **Comitè de Seguretat Corporativa**. Aprova la documentació i els recursos identificats per a cada escenari de contingència, l'abast de les proves i el seu informe de resultats.

Controls de Seguretat Corporativa

Plantejament

Per a cada escenari de contingència aprovat, l'àrea de Seguretat Corporativa coordinarà:

- La redacció del PCN (Pla de Continuïtat de Negoci), incloent:
  - Pla de Gestió de l'Incident.
  - Pla de Comunicació amb empleats, agents externs i mitjans de comunicació pública.
  - Pla de Recuperació de l'Incident, incloent els procediments operatius i la identificació i documentació dels recursos necessaris.
- L'assignació o adopció dels recursos necessaris per a la recuperació en cas de contingència.
- Procediment de suport necessaris.

Proves

Es provarà de manera periòdica els plans dissenyats per als escenaris de contingència. L'enfoc serà de proves parcials o completes.

L'Àrea de Seguretat Corporativa proposarà al Comitè de Seguretat Corporativa l'abast de les proves a realitzar per a la seva aprovació.

L'àrea de Seguretat Corporativa dissenyarà les proves a realitzar, en coordinarà l'execució i elaborarà un informe de la prova que haurà de ser aprovat pel Comitè de Seguretat Corporativa. Per a cada prova, s'haurà d'identificar i registrar:

- Incidències i deficiències detectades.
- Accions correctores.
- Accions de millora.

Annexe III – Procediment d'auditories internes

Procediment d'auditoria interna SCRIPTIX

Data publicació	Nom	Signatura
17/03/2019	Responsable de Seguretat	TI Aprovació autor
18/03/2019	Responsable IT	TI Aprovació

Històric de canvis

Versió	Data publicació	Editor	Estat	Comentaris
01.00	13/03/2019	CISO	Inicial	Versió inicial
01.01	16/03/2019	CISO	Final	Versió final

Índex

Índex de taules

Índex de fugures

Introducció

En un Sistema de Gestió de la Seguretat de la Informació basat en la norma ISO/IEC 27001 es fa necessari dur a terme auditories internes cada cert temps per poder comprovar que l'estat del SGSI sigui el correcte. El principal objectiu de que es realitzin auditories internes de manera periòdica és poder determinar si els objectius, els controls, els processos i els procediments del SGSI es troben:

- Conformes al requeriments que estableix l'estàndard internacional ISO/IEC 27001, a més de la legislació i els reglaments d'aplicació.
- Concorde els requisits establerts en seguretat de la informació.
- Eficaçment implementats.
- Comportant-se de manera esperada.

El programa d'auditoria s'ha de planificar en funció del nivell d'importància dels processos i les àrees que seran auditada, a més ha de comptar amb els resultat obtinguts d'auditories prèvies. S'han de definir els criteris utilitzats durant l'auditoria, l'abast, la freqüència o els mètodes utilitzats. Els auditors escollits per a dur a terme l'auditoria han de garantir que es realitza de forma objectiva i imparcial, per això els auditors no haurien d'auditar el seu propi treball.

S'ha de comptar amb un procediment documentat en el que s'especifiquin les responsabilitats, els requisits i la direcció de les auditories, addicionalment s'ha d'emetre un informe amb els resultats obtinguts.

Les responsabilitats pel que fa a les auditories internes han d'estar perfectament establertes, és a dir, s'ha de conèixer quines són les persones encarregades de planificar-les, els requeriments amb el que compten, la manera d'informar sobre els resultats, el lloc on han de guardar-se els registres, etc.

La alta direcció de l'organització és la responsable de que l'àrea auditada dugui a terme les accions necessàries per eliminar les no conformitats que s'hagin detectat durant l'auditoria i presentar els motius que van causar la no conformitat. Durant el seguiment de les activitats realitzades s'ha d'incloure una verificació de les accions que s'han dut a terme, així com un informe que indiqui la verificació dels resultats obtinguts.

Objectius

L'objectiu del procediment d'Auditoria Interna és especificar els requeriments i processos que s'han de dur a terme juntament amb els responsables de cada requeriment / procés, per tal de definir el pla d'auditoria de seguretat de la informació.

Així, doncs, l'objectiu de l'auditoria inclourà els següents punts:

- Determinar el grau de conformitat del sistema de gestió SCRIPTIX, o part d'aquest, amb els criteris d'auditoria.
- Avaluar la capacitat dels sistemes de gestió per a assegurar el compliment amb requisits legals o contractuals.
- Avaluar l'eficàcia del sistema de gestió per a aconseguir els objectius especificats.
- Identificar àrees potencials de millora del sistema de gestió.

La realització periòdica d'auditories internes de seguretat permetrà saber l'estat de seguretat els sistemes d'informació. Com a beneficis d'aquestes auditories cal destacar:

- Permetre reduir els impactes un cop identificats els riscos i vulnerabilitats.
- Ofereix major garanties i nivells de seguretat per al negoci.
- Millora la imatge externa de l'empresa.
- Ajuda a saber què mesures concretes de seguretat cal implementar.
- Augmenta la seguretat de la companyia, salvaguardant la confidencialitat i la integritat de la informació que es gestiona.

Abast

L' abast d'aquest procediment d'auditoria és el mateix que s'ha definit en l'abast del Sistema de Gestió de la Seguretat de la Informació (SGSI) sota les normes ISO/IEC 27001:2013.

Procediment

L'aplicació de l'Auditoria es farà en seguint les següents fases:

1. Preparació / Planificació de l'auditoria
2. Execució de l'auditoria
3. Conclusions de l'auditoria
4. Seguiment de l'auditoria

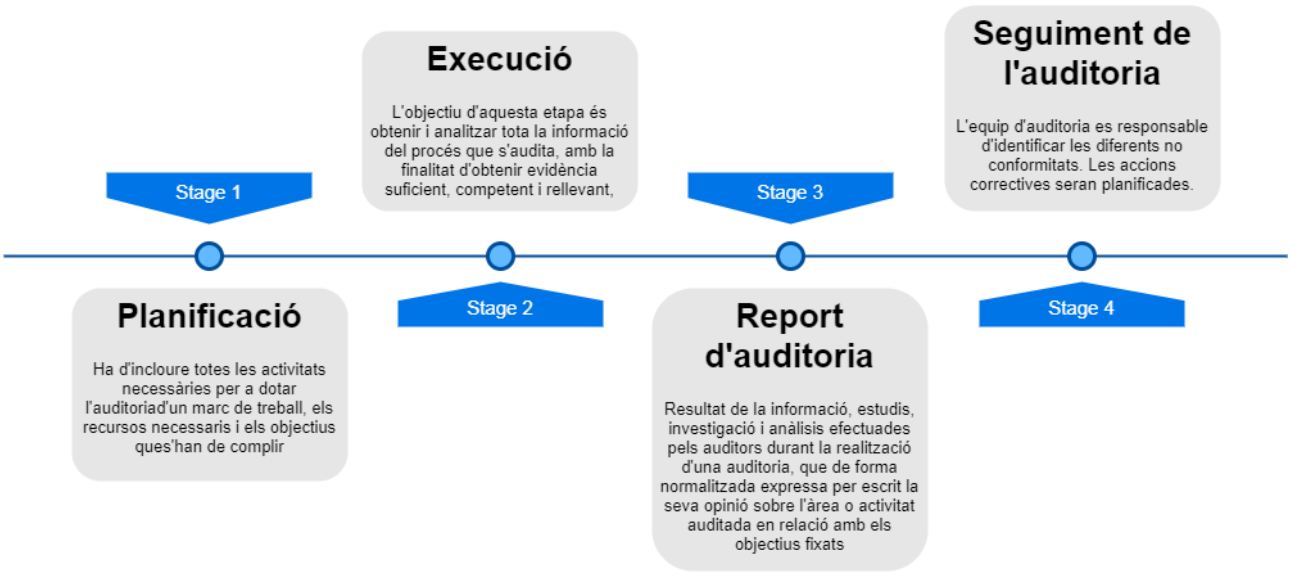


Figura 16: Procediment d'auditoria

Preparació / Planificació de l'auditoria

La persona encarregada de dur a terme l'auditoria, l'auditor, conforme les dades previstes en el Pla d'Auditories, ha de comunicar per mitjà del programa d'auditories als diferents departament de l'organització la data en que tindrà lloc aquesta.

Execució de l'auditoria

L'auditoria es basa en quatre aspectes bàsics dintre de cada un dels departaments de l'organització, els quals són:

- La forma dels documents, és a dir, s'ha de tenir en compte l'estructura del document, l'actualització, codificació, etc.
- El contingut dels documents: la eficàcia i la eficàcia de les mesures descrites en els documents.
- Verificar que els documents compleixin amb els requisits exigits per l'estàndard internacional ISO/IEC 27001.
- Que s'apliqui realment el que s'ha descrits en els documents.

Les comprovacions es duran a terme durant les reunions que es realitzaran entre l'auditor i les persones que integraran el departament auditat. Durant les reunions, l'auditor requerirà les proves necessàries que demostrin el compliment de l'indicat en els procediments que afecten al departament auditat.

Conclusions de l'auditoria

Un cop realitzada l'auditoria, l'auditor encarregat de realitzar-la haurà de complimentar l'Informe d'Auditoria. Mitjançant aquest informe s'estableixen les no conformitats detectades per a posteriorment procedir a obrir la no conformitat oportuna i so es necessari, realitzar l'apertura de les Accions correctives o preventives que es derivin de l'auditoria.

Les no conformitats i les accions correctives o preventives que s'obrin s'hauran de registrar i es farà entrega d'una còpia a cada responsable dels departaments afectats.

Seguiment de l'auditoria

Si durant l'auditoria s'han detectat desviacions, l'auditor serà el responsable de realitzar les comprovacions necessàries per assegurar que s'estan aplicant les accions proposades dintre del marc temporal estimat per a cada una d'elles.

Serà l'auditor intern qui determinarà l'aprovació o la no aprovació de les accions que s'han dut a terme en cada una de les desviacions detectades durant l'auditoria, i quedaran reflectides en l'apartat de tancament d'aquestes. Si no s'aprova, s'hauran d'indicar els motius pels que s'ha arribat a aquesta conclusió en el corresponent apartat, i l'auditor juntament amb el reposable de corregir la desviació han de proposar una nova mesura, que bé pots ser una mesura correctiva o preventiva.

Si per algun motiu persisteixen les desviacions, l'auditor intern ha d'informar a l'alta direcció.

S'originarà l'apertura d'Accions Correctores Preventives sempre que, l'Auditor percebi que es reiteren les desviacions i aquestes afecten greument al bon funcionament del Sistema de Gestió de Seguretat de la Informació.

A continuació s'adjunta el detall de l'estructura de la plantilla de no conformitats.

Àrea	*Descripció de l'àrea / sistema / procés auditat*	Conclusió	(*1)

Control ISO: Nom
Descripció del control de la ISO/IEC 27002:2013

Treball realitzat
Descripció detallat del treball realitzat

Evidències
*És detallen les evidencies recollides, les quals donen suport al treball realitzat i les observacions efectuades utilitzant la següent nomenclatura EV_XXX, on **EV** es la abreviatura del'evidència **XXX** és el número de l'evidencia dintre l'informe*

Recomanacions
S'adjunta les recomanacions sobre les observacions del punt anterior

Recomanacions
S'adjunta les recomanacions sobre les observacions del punt anterior

Estat	(*2)
Responsable	(*3)
Termini	(*4)

Tabla 11: Plantilla de no conformitats

	Descripció		
(*1)	Conforme (fons verd)	No conforme (fons vermell)	No aplica (fons blanc)
(*2)	Pendent	En curs	N/A (no hi ha recomanacions
(*3)	Àrea o personal responsable	N/A (no hi ha recomanacions)	
(*4)	1 mes / 3 mesos / 6 mesos / + 6 mesos / N/A (no hi ha recomanacions)		

Resultats

L'informe d'auditoria ha d'incloure la següent informació:

- Data de l'auditoria.
- Nom de/ls auditor/s.
- Abast de l'auditoria; àrea, departament, sistema o procés auditat.
- Conformitat del SGSI versió 2013 amb la norma.
- No conformitats detectades i accions correctives / preventives de cada una d'elles.
- Si l'auditoria no és de certificació pot, addicionalment, contenir recomanacions de millora.

Independència dels auditors

Les auditories han de realitzar-se per auditors independents del personal que tinguin algun tipus de responsabilitat directa respecte l'activitat que es troben auditant, pel que l'auditor:

- No poden ser el responsable de un departament del que depèn el procés auditat.
- No podrà formar part de un departament dependent del procés auditat.

Annexe IV – Gestió d'indicadors de Seguretat

Gestió d'indicadors de Seguretat SCRIPTIX

Data publicació	Nom	Signatura
14/03/2019	Responsable de Riscos	TI Aprovació autor
20/03/2019	Responsable de Seguretat	TI Aprovació autor

Històric de canvis

Versió	Data publicació	Editor	Estat	Comentaris
01.00	13/03/2019	Responsable de Riscos	Publicat	Versió inicial

La creació d'indicadors està orientada a la mesura de l'efectivitat, eficiència i eficàcia dels components implementats i gestió definits en el model d'operació del marc de seguretat de la informació, indicadors que serviran com a input per a la millora continua permetent adoptar decisions de millora.

Els objectius d'aquests processos de mesura pel que fa a la seguretat de la informació son:

- Avaluar la efectivitat de la implementació dels controls de seguretat.
- Avaluar la eficiència del Model de Seguretat de la Informació dintre de la companyia.
- Proveir d'estats de seguretat que serveixin de guia en les revisions del Model de Seguretat de la Informació, facilitant millores en la seguretat de la informació i noves entrades a auditar.
- Comunicar valors de seguretat a la companyia.
- Servir com a input al Pla d'Anàlisi i Tractament dels Riscos.

A continuació es detallen cada un dels indicadors ja implementats en SCRIPTIX, seguint els vuit components bàsics esmentats.

Control ISO amb el què està relacionat	
5 – Política de Seguretat	
Objetiu de l'indicador	**Definició**
Revisió del document "Poítiques de Seguretat de la Informació" elaborat per la direcció de l'organització	El contingut de les polítiques es basa en el context en el que opera una organització i solen ser considerades en relació amb els objectius de la organització, les estratègies adoptades per assolir els objectius, la estructura i els processos adoptats per l'organització, els objectius generals i específics relacionats amb el tema de la política i requeriments de les polítiques procedents de nivells més superiors (legals d'obligat compliment, del sector al que pertany l'organització, de la pròpia organització de nivells superiors o més amplis, ...) relacionades
Responsable	**Freqüència**
Responsaable de Seguretat	Anual
Fórmula de mesurament	**Descripció dels valors**
0 = No es compleix 1 = Es compleix	La companyia ha definit una política general de seguretat de la informació
Valor objectiu de l'indicador	
1	

Control ISO amb el què està relacionat	
8 – Gestió d'actius	
Objectiu de l'indicador	**Definició**
L'objectiu de l'indicador és que l'organització tingui coneixement precís dels actius que poseeix.	Els actius de la informació han de ser classificats d'acord la sensibilitat i criticitat de la informació que contenen o bé d'acord a la funcionalitat que compleixen i rotulats en funció d'aquest criteri.
Responsable	**Freqüència**
Responsable IT Local	Semestral
Fórmula de mesurament	**Descripció dels valors**
0 = No es compleix 1 = Es compleix 2 = Es compleix parcialment	La companyia disposa d'un inventari d'actius i la persona responsable dels actius
Valor objectiu de l'indicador	
1	

Control ISO amb el què està relacionat	
9 – Control d'Accés	
Objectiu de l'indicador	**Definició**
Controlar l'accés per mitjà d'un sistema de restriccions i excepcions a la informació com a base de tot sistema de seguretat informàtica	Per impedir l'accés no autoritzat als sistemes d'informació s'haurien d'implementar procediments formals per a controlar l'assignació de drets d'accés als sistemes d'informació, base de dades i serveis d'informació, i aquests han d'estar clarament documentats, comunicats i controlats pel que fa al seu compliment
Responsable	**Freqüència**
Facilities Local	Semestral
Fórmula de mesurament	**Descripció dels valors**
0 = No es compleix 1 = Es compleix 2 = Es compleix parcialment	La companyia disposa d'un procediment per al control d'accés a la xarxa i als sistemes d'informació. Es valida el seu compliment
Valor objectiu de l'indicador	
1	

Control ISO amb el què està relacionat	
11 – Seguretat física i ambiental	
Objectiu de l'indicador	**Definició**
Minimitzar els riscos de danys i interferències a la informació i a es operacions de l'organització	L'establiment del perímetre de seguretat i àrees protegides facilita la implementació de controls de protecció de les instal·lacions de processament d'informació crítica o sensible, contra accessos físics no autoritzats. El control de factors ambientals d'origen intern i/o extern permeten garantir el correcte funcionament dels equips de processament i minimitzar les interrupcions de servei
Responsable	**Freqüència**
Facilities Local	Anual
Fórmula de mesurament	**Descripció dels valors**
A.0 = No es compleix A.1 = Es compleix A.2 = Es compleix parcialment B.0 = No es compleix B.1 = Es compleix B.2 = Es compleix parcialment	**(A)** La companyia disposa de mesures físiques per a impedir l'accés no autoritzat. Addicionalment es disposa d'un procediment per al registre de tota persona aliena a l'empresa. **(B)** Es disposa de sistemes de refrigeració a tots els CPD. Addicionalment es disposa de connexió de subministre elèctric i evitar així que qualsevol tall elèctric generi indisponibilitat dels sistemes d'informació
Valor objectiu de l'indicador	
A.1 / B.1	

Control ISO amb el què està relacionat	
12 – Seguretat en la operativa	
Objectiu de l'indicador	**Definició**
Controlar l'existència dels procediment d'operació i desenvolupament ui manteniment actualitzats	Assegurar la operació correcta i segura dels mitjans de processament de la informació mitjançant el desenvolupament dels procediments operatius apropiats. S'han d'establir les responsabilitats i procediments per a la gestió i operació de tots els medis de processament de la informació. S'hauria d'implementar la segregació de tasques, sempre que sigui possible, per a reduir el disc per un mal ús deliberat o per negligència
Responsable	**Freqüència**
Business Development	Anual
Fórmula de mesurament	**Descripció dels valors**
A.0 = No es compleix A.1 = Es compleix A.2 = Es compleix parcialment B.0 = No es compleix B.1 = Es compleix B.2 = Es compleix parcialment D.0 = No es compleix D.1 = Es compleix D.2 = Es compleix parcialment	(**A**) Disposar dels procediments operatius per a cada mitja de processament (**B**) Inventari de responsables i responsabilitats i procediments per a la gestió i operació dels medis de processament (**D**) Inventari de tasques segregades i responsable de cada tasca
Valor objectiu de l'indicador	
A.1 / B.1 / D.1	

Control ISO amb el què està relacionat	
13 – Seguretat de les telecomunicacions	
Objectiu de l'indicador	**Definició**
Assegurar la protecció de la informació que es comunica mitjançant xarxes telemàtiques i la protecció de la infraestructura de suport	La gestió segura de les xarxes requereix de la cura del fluix de dades, implicacions legals, monitoreig i protecció. La informació confidencial que passa a través de les xarxes publiques solen requerir controls addicionals de protecció. L'intercanvi de informació per part de les organitzacions hauria de basar-se en una política formal d'intercanvi i en línia dels acords d'intercanvi
Responsable	**Freqüència**
Responsable de Seguretat / Chief Compliance Officer	Anual
Fórmula de mesurament	**Descripció dels valors**
A.0 = No es compleix A.1 = Es compleix A.2 = Es compleix parcialment B.0 = No es compleix B.1 = Es compleix B.2 = Es compleix parcialment	(**A**) Revisió de la implantació de IDS (Intrusion Detection System) i de les polítiques de detecció. (**B**) Revisió de la política d'intercanvi de dades amb altres organitzacions tant privades com publiques (estaments oficials)
Valor objectiu de l'indicador	
A.1 / B.1	

Control ISO amb el què està relacionat	
14 – Adquisició, desenvolupament i manteniment dels sistemes	
Objectiu de l'indicador	**Definició**
Assegurar la inclusió de controls de seguretat i validació de dades en l'adquisició i desenvolupament de sistemes d'informació	Definir i documentar les normes i procediments que s'aplicaran durant el cicle de vida de les aplicacions i en la infraestructura base en la que es recolzen Definir els mètodes de protecció de la informació crítica o sensible Aplica a tots els sistemes informàtics, tant de desenvolupament propis com de tercers, i a tots els Sistemes Operatius i/o Sofware que integren qualsevol dels ambients administrats per les organitzacions on resideixen els desenvolupaments esmentats
Responsable	**Freqüència**
Business Development	Anual
Fórmula de mesurament	**Descripció dels valors**
A.0 = No es compleix A.1 = Es compleix A.2 = Es compleix parcialment B.0 = No es compleix B.1 = Es compleix B.2 = Es compleix parcialment	(**A**) Disposa d'un procediment per al desenvolupament de programari que tingui en compte aspectes com la qualitat del codi i seguretat (**B**) isposar del procediment per a la distribució del codi pels diferents ambients fins arribar a l'entorn de Producció
Valor objectiu de l'indicador	
A.1 / B.1	

Annexe V – Declaració d'aplicabilitat

Declaració d'Aplicabilitat del SGSI SCRIPTIX

Data publicació	Nom	Signatura
17/03/2019	Responsable de Seguretat	TI Aprovació autor
18/03/2019	Responsable Riscos	TI Aprovació revisor
20/03/2019	Responsable IT	TI Aprovació

Històric de canvis

Versió	Data publicació	Editor	Estat	Comentaris
01.00	Pendent	CISO	Inicial	Versió inicial

Índex

Introducció

L'objectiu del present document és indicar quins controls de la ISO/IEC 27001:2013 són d'aplicació a SCRIPTIX.

El present document servirà de marc de referència per a l'auditoria de certificació ISO/IEC 27001, on es comprovaran tots els controls implementats.

Abast

L'abast del present document d'Aplicabilitat és el mateix que es troba definit en l'apartat ABAST del Sistema de Gestió de Seguretat de la Informació (SGSI).

Declaració d'aplicabilitat

A continuació es detallen els 114 controls, 35 objectius i 14 dominis de la ISO/IEC 27002:2013 que són aplicables al SGSI.

Controls	Aplicabilitat	Implementació
5. POLÍTIQUES DE SEGURETAT DE LA INFORMACIÓ		
5.1 Directrius de la direcció en seguretat de la informació		
5.1.1 Conjunt de polítiques per a la seguretat de la informació	Aplica	Control necessari per a la norma ISO. Política de seguretat de SCRIPTIX
5.1.2 Revisió de les polítiques per a la seguretat de la informació	Aplica	Iteració de la revisió / aprovació
6. ASPECTES ORGANITZATIUS DE LA SEGURETAT DE LA INFORMACIÓ		
6.1 Directrius de la direcció en seguretat de la informació		
6.1.1 Assignació de responsabilitats per a la seguretat de la informació	Aplica	Definit en el document de Política de Seguretat
6.1.2 Segregació de tasques	Aplica	En fase de millora. S'està definint el nou circuit
6.1.3 Contacte amb les autoritats	Aplica	En fase de millora.
6.1.4 Contacte amb grups d'interès especial	No aplica	No es manté contacte amb grups i posts de seguretat especialitzats i associacions professionals
6.1.5 Seguretat de la informació en la gestió de projectes	Aplica	Pendent d'integració amb projectes.

6.2 Directrius de la direcció en seguretat de la informació		
6.2.1 Política d'usos de dispositius per a mobilitat	Aplica	En fase de millora.
6.2.2 Teletreball	Aplica	Definit el procediment. Pendent d'implementació
7. SEGURETAT LLIGADA ALS RECURSOS HUMANS		
7.1 Abans de la contractació		
7.1.1 Investigació d'antecedents	Aplica	No implementat
7.1.2 Terminis i condicions de la contractació	Aplica	Definit en el document de Política de Seguretat. En fase de millora
7.2 Durant la contractació		
7.2.1 Responsabilitats de gestió	Aplica	Definit en el document de Política de Seguretat. En fase de millora
7.2.2 Conscienciació, educació i capacitació en seguretat de la informació	Aplica	Definit en el document de Política de Seguretat. En fase de millora
7.2.3 Procés disciplinari	Aplica	Definit el procediment. Pendent d'implementació
7.3 Baixa o canvi de lloc de treball		
11.2 Seguretat dels equips		
11.2.1 Ubicació i protecció dels equips	Aplica	Pendent de definir
11.2.2 Instal·lacions de subministrament	Aplica	Pendent de definir
11.2.3 Seguretat del cablejat	Aplica	Definit en el document de Política de Seguretat. En fase de millora
11.2.4 Manteniment dels equips	Aplica	Implementat «de facto». Pendent de definir el procediment
11.2.5 Sortida d'actius fora de les dependències de la companyia	Aplica	Implementat «de facto». Pendent de definir el procediment
11.2.6 Seguretat dels equips i actius fora de les instal·lacions de la companyia	Aplica	Definit en el document de Política de Seguretat. En fase de millora
11.2.7 Reutilització o retirada segura de dispositius d'emmagatzematge	Aplica	Definit en el document de Política de Seguretat. En fase de millora
11.2.8 Equip informàtic d'usuari desatès	Aplica	Definit en el document de Política de Seguretat. En fase de millora
11.2.9 Política de lloc de treball buidat i bloqueig de pantalla	Aplica	Pendent de definir
12. SEGURETAT EN LA OPERATIVA		
12.1 Responsabilitats i procediments d'operació		
12.1.1 Documentació de procediments d'operació	Aplica	Pendent de definir
12.1.2 Gestió de canvis	Aplica	Definit el procediment. Pendent d'implementació
12.1.3 Gestió de capacitats	Aplica	Pendent de definir
12.1.4 Separació d'entorn de desenvolupament, proves i producció	Aplica	Definit el procediment. Pendent d'implementació
12.2 Protecció contra codi maliciós		
12.2.1 Controls contra el codi maliciós	Aplica	Definit en el document de Política de Seguretat. Aplicació anti-malware McAfee corporatiu
12.3 Còpies de seguretat		
12.3.1 Còpies de seguretat de la informació	Aplica	Definit en el document de Política de Seguretat. En fase de millora
12.4 Requeriments de l'activitat i supervisió		
12.4.1 Registre i gestió d'events de seguretat	Aplica	Definit en el document de Política de Seguretat. Implementat
12.4.2 Protecció dels registres d'informació	Aplica	Definit en el document de Política de Seguretat. En fase de millora
12.4.3 Registre d'activitats de l'administrador i operador del sistema	Aplica	Definit en el document de Política de Seguretat. En fase de millora
12.4.4 Sincronització de rellotges	Aplica	Pendent de definir
12.5 Control del software en explotació		
12.5.1 Instal·lació del software en sistemes en producció	Aplica	Pendent de definir
12.6 Gestió de la vulnerabilitat tècnica		
12.6.1 Gestió de les vulnerabilitats tècniques	Aplica	Definit en el document de Política de Seguretat. En fase de millora
12.6.2 Restriccions en les instal·lacions de software	Aplica	Definit en el document de Política de Seguretat. En fase de millora
12.7 Consideracions de les auditories dels sistemes d'informació		
12.7.1 Controls d'auditoria dels sistemes d'informació	Aplica	Definit el procediment. Pendent d'implementació. En fase de millora
13. SEGURETAT EN LES TELECOMUNICACIONS		
13.1 Gestió de la seguretat en les xarxes		
13.1.1 Controls de xarxa	Aplica	Implementat. En fase de millora
13.1.2 Mecanismes de seguretat associats als serveis de xarxa	Aplica	Implementat implantant controls de xarxa i sistemes IDS. En fase de millora
13.1.3 Segregació de xarxes	Aplica	Implantat. En fase de millora
13.2 Intercanvi d'informació amb terceres parts		
13.2.1 Polítiques i procediments d'intercanvi d'informació	Aplica	Implantat. En fase de millora
13.2.2 Acords d'intercanvi	Aplica	Implantat. En fase de millora
13.2.3 Missatgeria electrònica	Aplica	Implantat. En fase de millora
13.2.4 Acords de confidencialitat i secret	Aplica	Implantat. Definit en el PCN.
14. ADQUISICIÓ, DESENVOLUPAMENT I MANTENIMENT DELS SISTEMES D'INFORMACIÓ		
14.1 Requeriments de seguretat dels sistemes d'informació		
14.1.1 Anàlisi i especificacions dels requeriments de seguretat	Aplica	Implementat. En fase de millora
14.1.2 Seguretat de les comunicacions en serveis accessibles per xarxes publiques	Aplica	Implantat. En fase de millora
14.1.3 Protecció de les transmissions per xarxes telemàtiques	Aplica	Implantat. En fase de millora
14.2 Seguretat en els processos de desenvolupament i suport		
14.2.1 Política de desenvolupament segur de programari	Aplica	Definit el procediment. Pendent d'implementació
14.2.2 Procediments de control de canvis en els sistemes	Aplica	Pendent de definir
14.2.3 Revisió tècnica de les aplicacions després de efectuar canvis en el sistema operatiu	Aplica	Pendent de definir
14.2.4 Restriccions als canvis en paquets de software	No aplica	
14.2.5 Ús de principis d'enginyeria en protecció de sistemes	No aplica	
14.2.6 Seguretat en entorns de desenvolupament	Aplica	Pendent de definir
14.2.7 Externalització del desenvolupament de programari	No aplica	
14.2.8 Proves de funcionalitat durant el desenvolupament de programari	Aplica	Definit el procediment de cicle de programari
14.2.9 Proves d'acceptació	Aplica	Definit el procediment de cicle de programari
14.3 Dades de prova		
14.3.1 Protecció de les dades utilitzades en les proves	Aplica	Pendent de definir

15. RELACIÓ AMB SUBMINISTRADORS		
15.1 Seguretat de la informació en les relacions amb subministradors		
15.1.1 Política de seguretat de la informació per subministradors	Aplica	Definit el procediment. En fase d'implementació
15.1.2 Tractament del risc dintre dels acords dels subministradors	Aplica	Definit el procediment. En fase d'implementació
15.1.3 Cadena de subministraments en tecnologies de la informació i les comunicacions	Aplica	Definit el procediment. En fase d'implementació
15.2 Gestió de la prestació de servei pels subministradors		
15.2.1 Supervisió i revisió dels serveis prestats per tercers	Aplica	Pendent de definir
15.2.2 Gestió del canvi en els serveis prestats per tercers	Aplica	Pendent de definir
16. GESTIÓ D'INCIDENTS EN LA SEGURETAT DE LA INFORMACIÓ		
16.1 Gestió d'incidents de seguretat en la informació i millores		
16.1.1 Responsabilitats i procediments	Aplica	Definit procediment de Rols i Responsabilitats. En fase de millora
16.1.2 Notificació dels events de seguretat de la informació	Aplica	Definit el procediment. Implantat. En fase de millora
16.1.3 Notificació de punts dèbils de seguretat	Aplica	Definit el procediment. Implantat. En fase de millora
16.1.4 Valoració dels events de seguretat de la informació i presa de decisions	Aplica	Definit el procediment. Implantat. En fase de millora
16.1.5 Resposta als incidents de seguretat	Aplica	Definit el procediment. Implantat. En fase de millora
16.1.6 Aprenentatge dels incidents de seguretat de la informació	Aplica	Definit el procediment. Implantat. En fase de millora
16.1.7 Recopilació d'evidències	Aplica	Definit el procediment. Implantat. En fase de millora
17. GESTIÓ D'INCIDENTS EN LA SEGURETAT DE LA INFORMACIÓ		
17.1 Continuïtat de la seguretat de la informació		
17.1.1 Planificació de la continuïtat de la seguretat de la informació	Aplica	Definit procediment de PCN
17.1.2 Implantació de la continuïtat de la seguretat de la informació	Aplica	Definit procediment de PCN
17.1.3 Verificació, revisió i avaluació de la continuïtat de la seguretat de la informació	Aplica	Definit procediment de PCN
17.2 Redundàncies		
17.2.1 Disponibilitat de les instal·lacions per al processament de la informació	Aplica	Definit procediment de PCN
18. COMPLIMENT		
18.1 Compliment dels requisits legals i contractuals		
18.1.1 Identificació de la legislació aplicable	Aplica	Procediment definit. En fase de millora
18.1.2 Drets de propietat intel·lectual (DPI)	Aplica	Procediment definit. En fase de millora
18.1.3 Protecció dels registres de l'organització	Aplica	Procediment definit. En fase de millora
18.1.4 Protecció de dades i privacitat de la informació personal	Aplica	Procediment definit. En fase de millora
18.1.5 Regulació dels controls criptogràfics	Aplica	Procediment definit. En fase de millora
18.2 Revisions de la seguretat de la informació		
18.2.1 Revisió independent de la seguretat de la informació	Aplica	Definit procediment d'Auditories Externes
18.2.2 Compliment de les polítiques i normes de seguretat	Aplica	Definit el procediment. En fase de millora
18.2.3 Comprovació del compliment	Aplica	Definit el procediment. En fase de millora

Annexe VI – Metodologia d'anàlisi de riscos

Procediment d'anàlisi de riscos SCRIPTIX

Data publicació	Nom	Signatura
14/03/2019	Responsable de Riscos	TI Aprovació autor
20/03/2019	Responsable de Seguretat	TI Aprovació autor
21/03/2019	Responsable IT	TI Aprovació

Històric de canvis

Versió	Data publicació	Editor	Estat	Comentaris
01.00	13/03/2019	Responsable de Riscos	Publicat	Versió inicial

Índex

Índex de taules

Índex de fugures

Objectiu

L'objectiu del procediment es establir la metodologia i tasques per realitzar l'Anàlisi i Gestió de Riscos de SCRIPTIX.

Mitjançant l'Anàlisi i Gestió de Riscos es podran identificar els riscos als que està exposada l'organització i poder actuar aplicant les mesures de seguretat necessàries per a mitigar, delegar o acceptar els riscos. Addicionalment mitjançant aquest procediment podrà elaborar-se els plans de contingència de l'organització.

Abast

L' abast d'aquest procediment d'auditoria és el mateix que hi ha definit en l'abast del SGSI.

Rols i responsabilitats

Comitè de direcció

Les funcions en matèria de seguretat de la informació del comitè de direcció de la companyia són les esmentades a continuació:

- Fer de la seguretat de la informació un punt de l'agenda del comitè de direcció de la companyia.
- Nomenar els membres del comitè de seguretat de la informació i donar-hi suport, dotar-lo dels recursos necessaris i establir-hi les directrius de treball.
- Aprovar la política, les normes i responsabilitats generals en matèria de seguretat de la informació.
- Determinar el llindar de risc acceptable en matèria de seguretat.
- Analitzar els possibles riscos derivats de canvis en les funcions o en el funcionament de la companyia i adoptar les mesures de seguretat més adequades.

- Aprovar el pla de seguretat de la informació, que recull els principals projectes i iniciatives en matèria de seguretat.
- Fer el seguiment del quadre de comandament de la seguretat de la informació.

Les decisions preses pel comitè de direcció en matèria de seguretat de la informació han de quedar recollides en acta.

Comitè de seguretat de la informació

Les decisions en matèria de seguretat de la informació les pren de manera consensuada un grup format per diferents responsables dins de la companyia.

Les funcions en matèria de seguretat de la informació del comitè de seguretat de la informació són les següents:

- Implantar les directrius del comitè de direcció.
- Assignar rols i funcions en matèria de seguretat.
- Presentar a aprovació al comitè de direcció les polítiques, normes i responsabilitats en matèria de seguretat de la informació.
- Validar el mapa de riscos i les accions de mitigació que ha proposat el responsable de seguretat de la informació.
- Validar el pla de seguretat de la informació o pla director de seguretat de la informació i presentar-lo a aprovació al comitè de direcció. Supervisar-ne la implantació i fer-ne el seguiment.
- Supervisar i aprovar el desenvolupament i manteniment del pla de continuïtat de negoci.
- Vetllar perquè es compleixi la legislació que sigui aplicable en matèria de seguretat.
- Promoure la conscienciació i formació d'usuaris i liderar la comunicació necessària.
- Revisar les incidències més destacades.
- Aprovar i revisar periòdicament el quadre de comandament de la seguretat de la informació i de l'evolució de l'SGSI.

Responsable de seguretat de la informació

La designació d'un responsable de seguretat de la informació (RSI) és l'única via per a avançar de manera organitzada i gradual en seguretat de la informació, ja que garanteix que hi ha algú per a qui la seguretat de la informació és una prioritat.

Les funcions en matèria de seguretat de la informació dels RSI són coordinar les accions orientades a garantir la seguretat de la informació en qualsevol de les formes que té (digital, òptica, paper, etc.) i en tot el cicle de vida d'aquesta informació (creació, manteniment, distribució, emmagatzematge i destrucció), per a protegir-la en termes de confidencialitat, privadesa, integritat, disponibilitat, autenticitat i traçabilitat.

Tot plegat es concreta en els punts següents:

- Implantar les directrius del comitè de seguretat de la informació de la companyia.
- Elaborar, promoure i mantenir una política de seguretat de la informació, i proposar anualment objectius en matèria de seguretat de la informació.
- Desenvolupar i mantenir el document d'Organització de la seguretat de la informació en col·laboració amb l'àrea d'organització o recursos humans, en el qual es recull qui assumeix cadascuna de les responsabilitats en seguretat i també una descripció detallada de funcions i dependències.
- Actuar com a punt focal en matèria de seguretat de la informació dins de la companyia, cosa que inclou la coordinació amb altres unitats i funcions (seguretat física, prevenció, emergències, relacions amb la premsa, etc.), a fi de gestionar la seguretat de la informació de manera global.
- Revisar periòdicament l'estat de la seguretat en qüestions organitzatives, tècniques o metodològiques. Aquesta revisió ha de permetre proposar o actualitzar el pla de seguretat de la informació i incorporar-hi totes les accions preventives, correctives i de millora que s'han anat detectant. Una vegada el CSI ha aprovat aquest pla i el pressupost, l'RSI ha de gestionar el pressupost assignat i la contractació de recursos quan sigui necessari.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Definir l'arquitectura de seguretat dels sistemes d'informació, monitorar la seguretat en l'àmbit tecnològic (gestió de traces, vulnerabilitats, canvis, etc.), fer el seguiment de les incidències de seguretat i escalar-les al CSI si correspon.
- Elaborar i mantenir un pla de conscienciació i formació en seguretat de la informació del personal, en col·laboració amb la unitat responsable de formació de la companyia.
- Fer el seguiment de les incidències de seguretat, revisar-les i escalar-les al CSI si correspon.

- Coordinar la implantació d'eines i controls de seguretat de la informació i definir el quadre de comandament de la seguretat. L'RSI ha d'analitzar i mantenir actualitzat aquest quadre de comandament i presentar-lo al CSI amb la periodicitat que s'estableixi.

Responsable de riscos

- Vetllar pel compliment legal (RD 3/2010, GDPR, Esquema nacional de seguretat, Basilea, SOX, etc.) i coordinar les actuacions necessàries amb les unitats responsables.
- Controlar la gestió de riscos de nous projectes i vetllar pel desenvolupament segur d'aplicacions.
- Desenvolupar, amb el suport de les unitats corresponents, el marc normatiu de seguretat i controlar-ne el compliment.
- Coordinar accions amb les àrees de negoci per a elaborar i gestionar un pla de continuïtat de negoci de la companyia, basat en l'anàlisi de risc i la criticitat dels processos de negoci, i la determinació de l'impacte en cas de materialització del risc.
- Promoure i coordinar entre les àrees de negoci l'anàlisi de riscos dels processos més crítics i la informació més sensible, i proposar accions per a millorar i mitigar el risc, d'acord amb el llindar acceptable que ha definit el comitè de direcció. Elevar el mapa de riscos i el pla de seguretat de la informació al comitè de seguretat de la informació (CSI).

Resta d'àrees

Cada àrea dins de la companyia ha de col·laborar amb l'RSI a desplegar la seguretat en el seu àmbit d'actuació i a aconseguir treballar i fer treballar l'organització de manera segura. Així, doncs, també s'han d'identificar funcions de seguretat en els àmbits d'auditoria, assegurances, formació, organització, etc.

Termes i definicions

Terme	Definició
Confidencialitat	És la propietat que impedeix la divulgació d'informació a persones o sistemes no autoritzats. Assegura l'accés a la informació únicament a aquelles persones que comptin amb la deguda autorització. Per exemple, en una transacció per internet (compra on-line) les dades personals tramesses (número de targeta, nom, adreça postal o electrònica, etc.) des de el comprador al venedor viatgen encriptades mitjançant el protocol HTTPS. Si per algun motiu aquestes dades fossin capturades per un tercer, en cap cas es veuria afectada la confidencialitat atès que al viatjar les dades de manera encriptada, la informació no és interpretable.
Integritat	És la propietat que busca mantenir les dades lliures de modificacions no autoritzades. La integritat és el mantenir amb exactitud la informació tal qual va ser generada, sense ser manipulada o alterada per persones o processos no autoritzats. Per exemple, l'accés al sistema de nòmines d'una empresa ha d'estar protegit mitjançant protocols d'autorització (qui accedeix, i que pot fer). Si una persona no autoritzada accedeix al sistema de nòmines, aquesta pot canviar (suposem que a l'alça) la seva nòmina. En aquest moment la integritat de la informació ha estat compromesa.
Disponibilitat	És la característica, qualitat o condició de la informació de trobar-se a la disposició dels qui han d'accedir a ella, ja siguin persones, processos o aplicacions. Per exemple i atès que la UOC és una plataforma on-line, ha d'establir els mecanismes per a que la web estigui disponible de manera continuada per a que els estudiants que ho desitgin puguin accedir quant ho desitgin. Si una persona malintencionada realitzés un atac DoS (Deny of Service – Denegació de Servei) la web de la UOC deixaria d'estar disponible i en conseqüència els estudiants no podrien accedir-hi. En aquest cas la disponibilitat de la web de la UOC s'hauria vist compromesa.
Autenticitat	És la propietat que permet identificar el generador de la informació. Per exemple en rebre un missatge d'algú, estar segur que és d'aquest algú el que ho ha manat, i no una tercera persona fent-se passar per l'altra (suplantació d'identitat)
No-repudi	proporciona protecció contra la interrupció, per part d'alguna de les entitats implicades en la comunicació, d'haver participat en tota o part de la comunicació. El servei de Seguretat de No repudi o irrenunciabilitat està estandarditzat en l'ISO-7498-2
Traçabilitat	És possible reproduir un històric o seqüència d'accions sobre un determinat procés i determinar qui ha estat l'autor de cada acció
Informació	Es refereix a tota comunicació o representació de coneixement com dades, en qualsevol forma, amb inclusió de formes textuals, numèriques, gràfiques, cartogràfiques, narratives o audiovisuals, i en qualsevol mitjà, ja sigui magnètic, en paper, en pantalles d'ordinadors, audiovisual o un altre.
Sistema d'Informació	Es refereix a un conjunt independent de recursos d'informació organitzats per a la recopilació, processament, manteniment, transmissió i difusió d'informació segons determinats procediments, tant automatitzats com manuals.
Tecnologia de la Informació	Es refereix al maquinari i programari operats pel Organisme o per un tercer que processi informació en el seu nom, per dur a terme una funció pròpia, sense tenir en compte la tecnologia utilitzada, ja es tracti de computació de dades, telecomunicacions o un altre tipus.
Comitè de Seguretat de la Informació	El Comitè de Seguretat de la Informació, és un cos integrat per representants de totes les àrees substantives de l'Organisme, destinat a garantir el suport manifest de les autoritats a les iniciatives de seguretat.
Responsable de Seguretat Informàtica	És la persona que compleix la funció de supervisar el compliment de la present Política i d'assessorar en matèria de seguretat de la informació als integrants de l'Organisme que així ho requereixin.

Tabla 12: Termes i definicions

Metodologia d’anàlisis de riscos

La metodologia emprada en aquest estudi és l’anomenada «Margarit». Aquesta metodologia la va elaborar el Ministeri d'Administracions Públiques (MAP) amb la finalitat d'ajudar totes les administracions públiques de l'Estat espanyol a millorar diversos aspectes.

Aquesta metodologia té com a característica fonamental que els riscos que es plantegen per a una organització s'expressen en valors econòmics directament, cosa que té un avantatge i un inconvenient:

- L'aspecte positiu d'aquesta metodologia és que el resultat s'expressa en valors econòmics. Això fa que les decisions que s'han de prendre i que ha de validar la direcció estan fonamentades i són fàcilment defensables.
- En canvi, el fet d'haver de traduir de manera directa totes les valoracions en valors econòmics fa que l'aplicació d'aquesta metodologia sigui realment costosa.

Hi ha dos grans tasques a realitzar;

- **Anàlisis dels riscos**; que permet determinar què te l’organització i estimar que podria passar.
- **Tractament dels riscos**; que permet organitzar la defensa de manera conscienciosa i prudent.

Ambdós activitats, anàlisi i tractament, es combinen en el procés denominat ***Gestió de Riscos***.

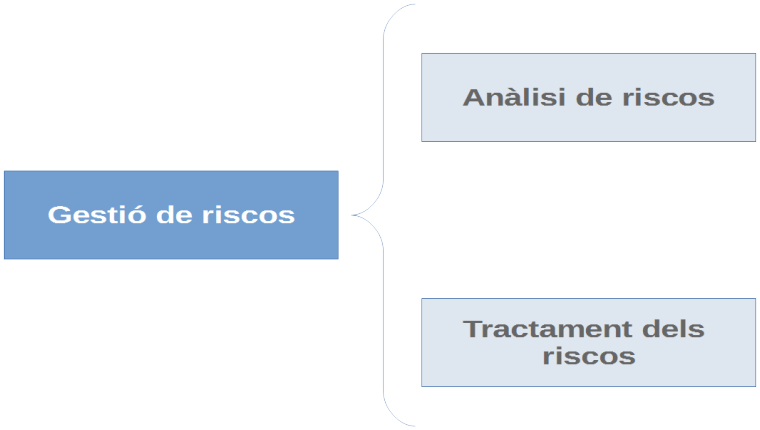


Figura 17: Gestió de Riscos

En l'Anàlisi de Riscos considera els següents elements:

- **Actius**: Per *actiu* s'entén tot element que necessita l'organització per a fer les activitats de negoci que li són pròpies.
- **Amenaces**: Són totes les situacions que poden arribar a passar en una organització i que poden danyar els actius, i provocar, doncs, que aquests actius no funcionin correctament o que no es puguin utilitzar de la manera correcta per a dur a terme l'activitat de negoci de l'organització.
- **Vulnerabilitats**: Les v*ulnerabilitats* les diferents debilitats que presenten els actius identificats anteriorment i que són aprofitats per les amenaces per a provocar un dany.
- **Impacte**: S'entén com a i*mpacte* les conseqüències que es produeixen en l'organització quan una amenaça aprofita una vulnerabilitat per a danyar un actiu.

Fases de Margerit

Aquesta metodologia, com s'ha comentat, té una eina –encara que no és imprescindible– que permet l'aplicació de Magerit d'una manera directa.

Magerit segueix un procés fins a arribar a elaborar i identificar tots els riscos d'una organització.

Les fases són les següents:

- Presa de dades i processos d'Informació.
- Establiment dels paràmetres.
- Anàlisi d'actius.
- Anàlisi d'amenaces.
- Establiment de les vulnerabilitats.
- Valoració d'impactes.
- Anàlisi de riscos intrínsecs.
- Influència dels controls de seguretat.
- Anàlisi dels riscos efectius.

- Gestió dels riscos.

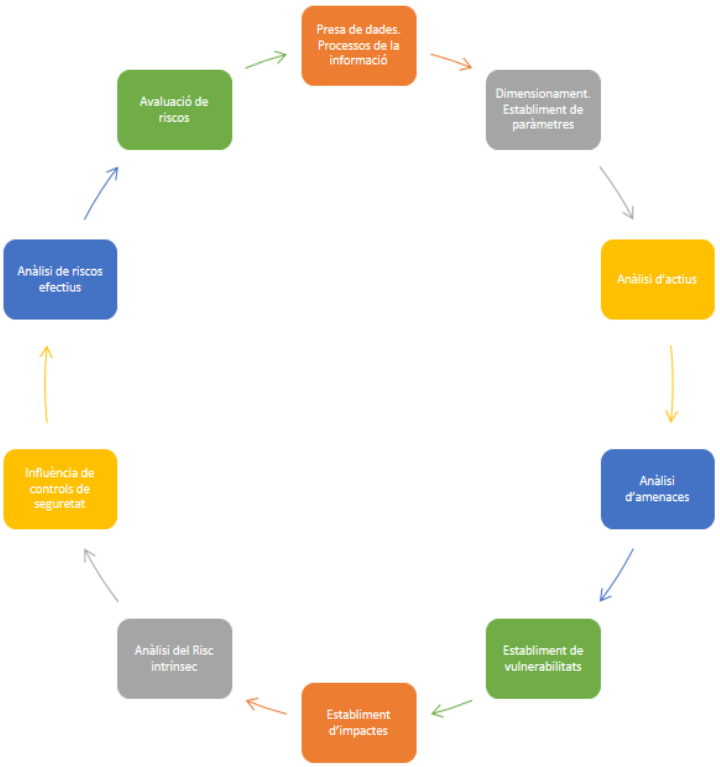


Figura 18: Fases Margerit

Presa de dades i processos d'informació

En aquesta primera fase –la més important de tota la metodologia–, s'ha de definir l'abast que s'ha d'estudiar o analitzar, ja que, depenent d'aquest abast, el procés és més o menys costós. Com més abast, més gran és el nombre de riscos analitzables.

Un altre factor que s'ha de tenir en compte és que, en aquesta primera fase, s'han d'analitzar els processos que duu a terme l'organització, ja que els riscos que s'han d'estudiar són els que poden interferir en els processos crítics. No s'ha de passar per alt que l'objectiu de tota seguretat és sempre garantir que els processos propis de l'organització es puguin fer de la millor manera possible.

Hi ha amenaces que no provocaran interferències en les activitats de l'organització i que no s'han d'analitzar, ja que protegir-se contra aquestes amenaces no té sentit, perquè no l'afectaran mai.

En aquesta primera fase també cal tenir present un factor importantíssim: la granularitat; *La granularitat té a veure amb la definició de les unitats que es pretén analitzar. Vol dir que s'ha de determinar el nivell de detall a què es vol arribar. Com més detall (baix nivell), més elements s'han d'analitzar i més costós és l'anàlisi de riscos*.

Establiment de paràmetres

La segona fase és la més important en la metodologia Magerit. Consisteix a establir paràmetres que s'utilitzaran durant tot el procés d'anàlisi de riscos.

Els paràmetres que s'identifiquin en aquesta fase s'han d'utilitzar durant tot el procés d'anàlisi de riscos i que si això no es compleix els resultats que s'obtindran no es podran comparar, de manera que el resultat no mostrarà els riscos reals d'una organització.

Els paràmetres que s'han d'identificar són els següents:

Valor dels actius

Aquest paràmetre té l'objectiu d'assignar una valoració econòmica a tots els actius d'una organització que es pretenen analitzar. Els actius que s'han d'analitzar són els que requereix l'organització per a dur a terme els processos que són propis de l'organització.

Per a dur a terme la valoració s'han d'establir diferents grups d'actius segons el valor que tenen. A cadascun d'aquests rangs s'hi assigna un valor estimat que és el que s'utilitzarà per a tots els actius la valoració econòmica dels quals es correspongui amb aquest rang de valors.

A l'hora d'assignar una valoració a cada actiu s'ha de tenir en consideració el següent:

- El ***valor de reposició*** és el valor que té per a l'organització reposar aquest actiu en cas que es perdi o que no es pugui utilitzar.

- El ***valor de configuració*** és el temps que es necessita des que s'adquireix el nou actiu fins que es configura o es posa a punt perquè es pugui utilitzar per a la funció que desenvolupava l'anterior actiu.
- El ***valor d'ús*** de l'actiu és el valor que perd l'organització durant el temps que no pot utilitzar aquest actiu per a la funció que desenvolupa.
- El ***valor de pèrdua d'oportunitat*** és el valor que perd potencialment l'organització pel fet de no poder disposar d'aquest actiu durant un temps.

Vulnerabilitat

Les vulnerabilitats s'entenen com una freqüència d'ocurrència d'una amenaça; és a dir, la freqüència amb què una organització pot tenir una amenaça en concret.

Aquesta freqüència d'ocurrència, o vulnerabilitat, també es plasma en una escala de valors (no es recomana més de cinc nivells) que s'han d'utilitzar per a tot l'estudi.

Una vegada hem determinat l'escala de valors que utilitzarem durant l'anàlisi de riscos, cal traduir aquestes vulnerabilitats a nombres, per a treballar-hi. Aquesta valoració numèrica es fa amb estimacions anuals, és a dir, assignant un nombre de vegades per any:

$$Vulnerabilitat = Freqüència\,estimada\,/\,dies\,any$$

Impacte

S'entén per impacte el tant per cent del valor de l'actiu que es perd en cas que hi hagi una incidència sobre aquest actiu. Per a fer aquesta anàlisi a priori, també s'ha de fer una estimació per rang d'impactes; és a dir, cal pensar en els diferents nivells d'impacte que es vol utilitzar, i a partir d'aquí assignar el percentatge de valor que s'estima que es pot perdre en cada cas.

Efectivitat del control de seguretat

Aquest paràmetre consisteix a veure la influència que tindran les mesures de protecció davant els riscos que detectem, és a dir, a pensar en la manera com ens poden reduir el risc detectat les diferents mesures de seguretat que implantem.

A l'hora de reduir un risc, cal tenir en compte que les mesures de seguretat tenen dues maneres d'actuar-hi en contra: o bé redueixen la vulnerabilitat (la freqüència d'ocurrència), o bé redueixen l'impacte que provoca aquest risc.

Valoració d'actius		
Descripció	Abreviatura	Valor
Molt alt	DT	300.000,00 €
Alt	A	150.000,00 €
Mitjà	M	75.000,00 €
Baix	B	30.000,00 €
Molt baix	MB	10.000,00 €
Despreciable	D	5.000,00 €

Tabla 13: Valoració d'actius

Freqüència		
Descripció	Abreviatura	Valor
Extremadament freqüent	EF	1
Molt freqüent	MF	0,07123288
Freqüent	F	0,01643836
Poc Freqüent	PF	0,0109589
Molt poc freqüent	MPF	0,00547945
Menyspreable	D	0,00273973
Dies: 365		

Tabla 14: Freqüència

Impacte		
Descripció	Abreviatura	Valor
Critico	C	90,00 %
Alt	A	75,00 %
Mitjà	M	50,00 %
Baix	B	20,00 %

Tabla 15: Impacte

Anàlisi d'Actius

Aquesta fase de l'estudi consisteix a identificar els actius que té l'organització i que necessita per a dur a terme les seves activitats. En aquesta fase és molt important haver deixat identificat clarament l'abast de l'anàlisi de riscos, ja que solament s'ha d'analitzar els actius que hi ha dins d'aquest abast.

Quan es parla d'actius analitzables cal pensar en els tipus d'actius següents:

- *Actius físics*. Són tots els actius de tipus maquinari que s'utilitzen en l'organització: ordinadors, servidors, portàtils, PDA, telèfons mòbils, impressores, etc.
- *Actius lògics*. Són tots els elements de programari que s'utilitzen: sistemes operatius, aplicacions pròpies, paquets tancats de mercat, processos batch, etc.
- *Actius de personal*. Són les persones, des del punt de vista de rols o perfils que intervenen en el desenvolupament de les activitats de l'organització: responsable de seguretat, administrador de la xarxa, personal d'administració, secretaris, usuaris, etc.
- *Actius d'entorn i infraestructura*. Són tots els elements que té l'organització i que necessita perquè la resta funcioni correctament. Són, per exemple, els sistemes d'aire condicionat o el cablejat de dades i de cor- rent elèctric.
- *Actius intangibles*. Són els elements que no té directament l'organització però que són importants per a ella, com ara la imatge corporativa, la credibilitat, la confiança dels clients, o el saber fer o know how.

Anàlisi d'amenaces

Les amenaces són les situacions que es poden arribar a donar en una organització i que desembocarien en un problema de seguretat.

La classificació de les amenaces que poden afectar a l'organització es classifiquen en quatre grans grups:

- **Accidents**. Són les situacions no provocades voluntàriament que sovint no es poden evitar, sinó que passen per efectes naturals. Dins d'aquesta categoria d'accidents n'hi ha de diferents tipus, com ara:

- Accident físic (inundació, incendi, terratrèmol, explosió, etc.).
- Avaria.
- Interrupció dels serveis essencials (talls en el subministrament elèctric, en les telecomunicacions, etc.).
- Accidents mecànics o electromagnètics (xoc, caiguda, radiació, etc.).

- **Errors**. Són les situacions que són comeses de manera involuntària pel desenvolupament mateix de les activitats diàries de l'organització, sia per desconeixement o per distracció del personal de l'organització o de tercers que són contractats per l'organització mateixa. Entre aquestes situacions esmentem les següents:
  - Errors en la utilització dels sistemes, provocats per un mal ús.
  - Errors en el disseny conceptual de les aplicacions.
  - Errors en el desenvolupament de les aplicacions.
  - Errors d'actualització o aplicació de pegats als sistemes o aplicacions.
  - Errors en el monitoratge.
  - Errors de compatibilitat entre aplicacions.
  - Errors inesperats (virus, cavalls de Troia, etc.).
- **Amenaces intencionals presencials**. Són les provocades pel personal ma- teix de l'organització de manera voluntària quan fan accions que saben que provoquen un dany, tant des del punt de vista físic com del lògic. Entre aquestes amenaces esmentem les següents:
  - Accés físic no autoritzat, sia amb destrucció de la informació o amb subministració.
  - Accés lògic no autoritzat, intercepció passiva de la informació o subtracció o alteració de la informació en trànsit.
  - Indisponibilitat de recursos, tant si són humans (baixes, vacances, abandonament, malaltia, etc.) com tècnics (bloqueig de sistema, per exemple).
  - Filtració de dades a terceres organitzacions, tant si són dades personals (LOPD) com tècniques.
- **Amenaces intencionals remotes**. Amenaces provocades per terceres per- sones, és a dir, per persones alienes a l'organització i que aconsegueixen danyar-la. Entre aquestes amenaces esmentem les següents:
  - Accés lògic no autoritzat. Accés d'un tercer no autoritzat, que explota una vulnerabilitat del sistema per utilitzar-la en benefici propi.

- Suplantació de l'origen. Intercepció d'una comunicació escoltant o fal- sejant les dades intercanviades.
- Cucs. Virus que utilitzen les capacitats de servidors i clients per a pro- pagar-se per Internet.
- Denegació de servei, sigui contra l'amplada de banda (consumir tota l'amplada de banda de la màquina que es vol atacar) o contra els recursos del sistema (consumir tota la memòria i els recursos de la màquina utilitzada per a oferir un servei).

Establiment de les vulnerabilitats

En Magerit, malgrat que no és necessari fer una llista de les vulnerabilitats, sí que ho és tenir-les en compte per a estimar la freqüència d'ocurrència d'una determinada amenaça sobre un actiu.

Valoració d'impactes

Els impactes es defineixen com les conseqüències que provoca en l'organització el fet que una certa amenaça, aprofitant una determinada vulnerabilitat, afecti un actiu.

A l'hora d'analitzar els impactes s'han de tenir en consideració els aspectes següents:

- El resultat de l'agressió d'una amenaça sobre un actiu.
- L'efecte sobre cada actiu per a agrupar els impactes en cadena segons la relació d'actius.
- El valor econòmic representatiu de les pèrdues produïdes en cada actiu.
- Les pèrdues quantitatives o qualitatives.

Anàlisi de riscos intrínsecs

A partir d'aquest punt, i amb els valors que hàgim identificat per a cada situació, ja es pot fer l'estudi dels riscos actuals a què està sotmesa una organització.

Per a aquest estudi, únicament és necessari fer una multiplicació dels valors que hem indicat fins ara:

$$Risc = Valoració\ de\ l'\ actiu \times Vulnerabilitat \times Impapcte$$

Influència dels controls de seguretat

Una vegada tenim identificats els riscos actuals a què està exposada l'organització, s'entra en la fase de gestió de riscos, que consisteix a mirar d'escollir la millor solució de seguretat que ens permeti reduir-los.

Per a fer-ho, hi ha dos tipus fonamentals de controls de seguretat:

- **Preventius**. Són les mesures de seguretat que redueixen les vulnerabilitats (la freqüència d'ocurrència).
  $$Nova\ vulnerabilitat = Vulnerabilitat \times Percentatge\ disminució\ de\ vulnerabilitat$$
- **Correctius**. Són les mesures de seguretat que redueixen l'impacte de les amenaces.
  $$Nova\ impacte = Impacte \times Percentatge\ disminució\ d'\ impacte$$

Anàlisi de riscos efectius

És el resultat d'estudiar com es reduirien els riscos amb cadascuna de les me- sures de protecció (controls de seguretat) que hem identificat; és a dir, s'ha de calcular el risc definitiu, que dóna com a resultat el risc efectiu que tindrà l'organització per a cadascuna de les amenaces identificades:

- Risc intrínsec
  $$Valor\ Actiu \times Vulnerabilitat \times Impacte$$

- Risc efectiu
  $Valor\ Efectiu \times Vulnerabilitat \times Impacte$

Gestió de riscos

Aquesta última fase consisteix en la presa de decisions de l'organització sobre les mesures de seguretat que ha d'escollir entre la llista de controls de seguretat que li permeten reduir els riscos.

A l'hora de gestionar els riscos, s'han d'escollir les mesures de seguretat que permetin reduir els riscos intrínsecs de l'organització fins a situar-los per sota del llindar de riscos amb un cost més petit per a l'organització.

Els riscos en una organització, es poden prendre tres decisions:

- Reduir-los.
- Transferir-los.
- Acceptar-los.

A l'hora de gestionar riscos s'ha d'elaborar un pla d'acció, que ha de contenir la informació següent:

- **Establir prioritats**. Consisteix a designar els riscos que s'han de reduir en primer lloc perquè són els més elevats per a l'organització.
- **Plantejar l'anàlisi de cost-benefici**. Consisteix a estudiar, per a cadascuna de les mesures que es poden implantar, quin cost comporta a l'organització i en quin percentatge redueix els riscos detectats.
- **Seleccionar controls definitius**. Una vegada analitzat el cost-benefici de tots els controls, cal seleccionar definitivament els que ha d'implantar l'organització per a reduir els riscos fins a situar-los per sota del seu llindar de risc.
- **Assignar responsabilitats**. Consisteix a assignar els responsables dins de l'organització de dur a terme la implantació dels controls. És important tenir identificades aquestes persones ja que, si no, hi ha el perill que les decisions que es prenguin no s'acabin implantant.
- **Implantar controls**. Consisteix a implantar els controls de seguretat desig- nats. Cal tenir en compte que els controls que s'implanten no han de ser forçosament tècnics, sinó que poden ser controls organitzatius o procedimentals.

Annexe VII – Valoració econòmica dels actius

Codi	Actiu	Valor Quantitatiu		Valor Quantitatiu/u
AH-1	CPD Principal	4	Alta	175.000,00 €
AH-2	CPD Secundari	4	Alta	175.000,00 €
AH-3	Switchs	1	Molt Baixa	250,00 €
AH-4	Routers	1	Molt Baixa	1.250,00 €
AH-5	Punt d'accés Wifi	1	Molt Baixa	160,00 €
AH-6	Unitat de cinta	1	Molt Baixa	1.250,00 €
AH-7	Portàtils (empleats)	2	Baixa	1.450,00 €
AH-8	Smartphones Android	1	Molt Baixa	350,00 €
AH-9	Smartphones Appel	1	Molt Baixa	1.280,00 €
AH-10	Unitats d'Emmagatzematge	1	Molt Baixa	2.800,00 €
AA-1	Windows Server 2016	2	Baixa	450,00 €
AA-2	Programari VMWare	1	Molt Baixa	275,00 €
AA-3	Base de dades MySQL	1	Molt Baixa	120,00 €
AA-4	Base de dades Oracle	3	Mitjana	11.250,00 €
AA-5	Base de dades Informix	1	Molt Baixa	1.250,00 €
AA-6	Firewall (programari lliure)	1	Molt Baixa	60,00 €
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	4	Alta	75.000,00 €
AA-8	Windows 7 (SO portàtils)	1	Molt Baixa	320,00 €
AA-9	Windows 10 (SO portàtils)	1	Molt Baixa	470,00 €
AS-1	Contracte seguretat física	2	Baixa	12.000,00 €
AS-2	Contracte de lloguer oficines	3	Mitjana	55.000,00 €
AS-3	Contracte recursos Sistemes Informàtics	2	Baixa	15.000,00 €
AS-4	Pàgina web de la organització	2	Baixa	235,00 €
AS-5	Contracte servei de neteja	1	Molt Baixa	8.500,00 €
AX-1	Comunicacions CPD Secundari	3	Mitjana	13.000,00 €
AX-2	Comunicacions línia mòbil i 3G/4G	1	Molt Baixa	2.500,00 €
AX-3	Comunicacions llocs de treball amb CPD principal	2	Baixa	340,00 €
AX-4	Comunicacions Internet	1	Molt Baixa	450,00 €
AX-5	Comunicacions Unitats d'Emmagatzematge núvol	2	Baixa	1.200,00 €
AP-1	Directius de la companyia	4	Alta	15.000,00 €
AP-2	Comandaments intermedis de la companyia	4	Alta	11.000,00 €
AP-3	Administradors de xarxa	2	Baixa	2.200,00 €
AP-4	Administradors base de dades (DBA)	2	Baixa	2.350,00 €
AP-5	Personal d'estructura	1	Molt Baixa	1.200,00 €
AP-6	Personal d'staff	1	Molt Baixa	1.100,00 €
AD-1	Backups	1	Molt Baixa	250,00 €
AD-2	Informació de clients	4	Alta	125.000,00 €
AD-3	Informació de proveïdors	3	Mitjana	75.000,00 €
AD-4	Informació d'empleats	4	Alta	190.000,00 €
AD-5	Inventari d'actius	2	Baixa	10.000,00 €
AE-1	Sistema refrigeració CPDs	3	Mitjana	7.500,00 €
AE-2	Equips de destrucció de paper	1	Molt Baixa	1.500,00 €
AE-3	Sistema d'alarmes	1	Molt Baixa	3.800,00 €
AE-4	Armaris ignífugs	1	Molt Baixa	4.500,00 €
AI-1	Edifici corporatiu	5	Molt Alta	2.340.000,00 €
AI-2	Seus corporatives	5	Molt Alta	270.000,00 €
AI-3	Llocs de treball	5	Molt Alta	850,00 €

Tabla 16: Valoració econòmica dels actius

Annexe VIII – Valoració dimensions de seguretat dels actius

Indicador	Categoria Actiu	Codi	Actiu	Dimensions seguretat	
AH	Hardware	AH-1	CPD Principal	10	Dany molt greu
		AH-2	CPD Secundari	10	Dany molt greu
		AH-3	Switchs	1-3	Dany menor
		AH-4	Routers	1-3	Dany menor
		AH-5	Punt d'accés Wifi	0	Dany irrellevant
		AH-6	Unitat de cinta	0	Dany irrellevant
		AH-7	Portàtils (empleats)	4-6	Dany important
		AH-8	Smartphones Android	1-3	Dany menor
		AH-9	Smartphones Appel	1-3	Dany menor
		AH-10	Unitats d'Emmagatzematge	4-6	Dany important
AA	Aplicació i Software	AA-1	Windows Server 2016	4-6	Dany important
		AA-2	Programari VMWare	4-6	Dany important
		AA-3	Base de dades MySQL	1-3	Dany menor
		AA-4	Base de dades Oracle	1-3	Dany menor
		AA-5	Base de dades Informix	1-3	Dany menor
		AA-6	Firewall (programari lliure)	4-6	Dany important
		AA-7	ERP SAP (Gestió RRHH, compres, facturació)	10	Dany molt greu
		AA-8	Windows 7 (SO portàtils)	4-6	Dany important
		AA-9	Windows 10 (SO portàtils)	4-6	Dany important
AS	Serveis	AS-1	Contracte seguretat física	4-6	Dany important
		AS-2	Contracte de lloguer oficines	1-3	Dany menor
		AS-3	Contracte recursos Sistemes Informàtics	4-6	Dany important
		AS-4	Pàgina web de la organització	4-6	Dany important
		AS-5	Contracte servei de neteja	1-3	Dany menor
AX	Xarxa	AX-1	Comunicacions CPD Secundari	7-9	Dany greu
		AX-2	Comunicacions línia mòbil i 3G/4G	4-6	Dany important
		AX-3	Comunicacions llocs de treball amb CPD principal	7-9	Dany greu
		AX-4	Comunicacions Internet	1-3	Dany menor
		AX-5	Comunicacions Unitats d'Emmagatzematge núvol	1-3	Dany menor
AP	Personal	AP-1	Directius de la companyia	7-9	Dany greu
		AP-2	Comandaments intermedis de la companyia	7-9	Dany greu
		AP-3	Administradors de xarxa	7-9	Dany greu
		AP-4	Administradors base de dades (DBA)	7-9	Dany greu
		AP-5	Personal d'estructura	7-9	Dany greu
		AP-6	Personal d'staff	7-9	Dany greu
AD	Dades	AD-1	Backups	7-9	Dany greu
		AD-2	Informació de clients	7-9	Dany greu
		AD-3	Informació de proveïdors	7-9	Dany greu
		AD-4	Informació d'empleats	10	Dany molt greu
		AD-5	Inventari d'actius	1-3	Dany menor
AE	Equipament Auxiliar	AE-1	Sistema refrigeració CPDs	7-9	Dany greu
		AE-2	Equips de destrucció de paper	1-3	Dany menor
		AE-3	Sistema d'alarmes	4-6	Dany important
		AE-4	Armaris ignífugs	4-6	Dany important
AI	Instal·lacions	AI-1	Edifici corporatiu	10	Dany molt greu
		AI-2	Seus corporatives	10	Dany molt greu
		AI-3	Llocs de treball	7-9	Dany greu

Tabla 17: Valoració dimensió seguretat actius

Annexe IX – Anàlisi d'amenaces

Tipus amenaça	Codi	Amenaça	Actiu afectat							
			AH	AA	AS	AX	AP	AD	AE	AI
Accidents	AM-1	Inundació								X
	AM-2	Incendi	X		X				X	X
	AM-3	Terratrèmol								
	AM-4	Explosió								
	AM-5	Avaria	X	X		X		X	X	
	AM-6	Interrupció dels serveis essencials	X			X			X	X
	AM-7	Accidents mecànics o electromagnètics	X				X	X	X	
Errors	AM-8	Errors en la utilització dels sistemes, provocats per un mal ús	X	X		X		X	X	
	AM-9	Errors en el disseny conceptual de les aplicacions		X				X		
	AM-10	Errors en el desenvolupament de les aplicacions		X				X		
	AM-11	Errors d'actualització o aplicació de pegats als sistemes o aplicacions	X	X		X				
	AM-12	Errors en el monitoratge	X	X		X		X	X	X
	AM-13	Errors de compatibilitat entre aplicacions	X	X						
	AM-14	Errors inesperats (virus, cavalls de Troia, etc.)		X				X		
Amenaces intencionals presencials	AM-15	Accés físic no autoritzat, sia amb destrucció de la informació o amb subministració				X		X		X
	AM-16	Accés lògic no autoritzat, intercepció passiva de la informació o subtracció o alteració de la informació en trànsit				X		X		
	AM-17	Indisponibilitat de recursos, tant si són humans (baixes, vacances, abandonament, malaltia, etc.) com tècnics	X	X	X	X	X	X	X	
	AM-18	Filtració de dades a terceres organitzacions, tant si són dades personals (LOPD) com tècniques					X	X		
Amenaces intencionals remotes	AM-19	Accés lògic no autoritzat. Accés d'un tercer no autoritzat, que explota una vulnerabilitat del sistema per utilitzar-la en benefici propi	X	X		X		X		
	AM-20	Suplantació de l'origen. Intercepció d'una comunicació escoltant o falsejant les dades intercanviades	X			X	X			
	AM-21	Cucs. Virus que utilitzen les capacitats de servidors i clients per a pro- pagar-se per Internet		X		X				
	AM-22	Denegació de servei, sigui contra l'amplada de banda o contra els recursos del sistema	X			X				

Tabla 18: Amenaces per actiu

Annexe X – Anàlisis d'actius i dimensions de seguretat

Accidents		Inundació		Incendi		Terratrèmol		Explosió		Avaria		Interrupció dels serveis essencials		Accidents mecànics o electromagnètics	
Codi	Actiu	AM-1		AM-2		AM-3		AM-4		AM-5		AM-6		AM-7	
AH-1	CPD Principal	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AH-2	CPD Secundari	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AH-3	Switchs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AH-4	Routers	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AH-5	Punt d'accés Wifi	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	PF	0,0109589	D	0,00273973
AH-6	Unitat de cinta	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	PF	0,0109589	MPF	0,00547945	D	0,00273973
AH-7	Portàtils (empleats)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	PF	0,0109589	MPF	0,00547945	PF	0,0109589
AH-8	Smartphones Android	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	PF	0,0109589	PF	0,0109589	PF	0,0109589
AH-9	Smartphones Appel	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	PF	0,0109589	PF	0,0109589	PF	0,0109589
AH-10	Unitats d'Emmagatzematge	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	F	0,01643836	MPF	0,00547945	D	0,00273973
AA-1	Windows Server 2016	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-2	Programari VMWare	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-3	Base de dades MySQL	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-4	Base de dades Oracle	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-5	Base de dades Informix	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-6	Firewall (programari lliure)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AA-8	Windows 7 (SO portàtils)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-9	Windows 10 (SO portàtils)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-1	Contracte seguretat física	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-2	Contracte de lloguer oficines	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-3	Contracte recursos Sistemes Informàtics	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-4	Pàgina web de la organització	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-5	Contracte servei de neteja	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AX-1	Comunicacions CPD Secundari	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973	D	0,00273973
AX-2	Comunicacions línia mòbil i 3G/4G	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	PF	0,0109589	D	0,00273973
AX-3	Comunicacions llocs de treball amb CPD principal	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AX-4	Comunicacions Internet	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AP-1	Directius de la companyia	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-2	Comandaments intermedis de la companyia	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-3	Administradors de xarxa	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-4	Administradors base de dades (DBA)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-5	Personal d'estructura	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-6	Personal d'staff	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-1	Backups	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-2	Informació de clients	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-3	Informació de proveïdors	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-4	Informació d'empleats	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-5	Inventari d'actius	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-1	Sistema refrigeració CPDs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AE-2	Equips de destrucció de paper	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945
AE-3	Sistema d'alarmes	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-4	Armaris ignífugs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-1	Edifici corporatiu	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-2	Seus corporatives	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-3	Llocs de treball	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973

Tabla 19: Dimensió seguretat - Accidents

Errors		Errors en la utilització dels sistemes, provocats per un mal ús		Errors en el disseny conceptual de les aplicacions		Errors en el desenvolupament de les aplicacions		Errors d'actualització o aplicació de pegats als sistemes o aplicacions		Errors en el monitoratge		Errors de compatibilitat entre aplicacions		Errors inesperats (virus, cavalls de Troia, etc.)	
Codi	Actiu	AM-8		AM-9		AM-10		AM-11		AM-12		AM-13		AM-14	
AH-1	CPD Principal	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945
AH-2	CPD Secundari	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945
AH-3	Switchs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-4	Routers	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-5	Punt d'accés Wifi	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-6	Unitat de cinta	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-7	Portàtils (empleats)	PF	0,0109589	D	0,00273973	D	0,00273973	PF	0,0109589	MPF	0,00547945	PF	0,0109589	PF	0,0109589
AH-8	Smartphones Android	PF	0,0109589	PF	0,0109589	D	0,00273973	PF	0,0109589	D	0,00273973	MPF	0,00547945	D	0,00273973
AH-9	Smartphones Appel	PF	0,0109589	PF	0,0109589	D	0,00273973	PF	0,0109589	D	0,00273973	MPF	0,00547945	D	0,00273973
AH-10	Unitats d'Emmagatzematge	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-1	Windows Server 2016	D	0,00273973	D	0,00273973	D	0,00273973	F	0,01643836	D	0,00273973	D	0,00273973	PF	0,0109589
AA-2	Programari VMWare	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AA-3	Base de dades MySQL	MPF	0,00547945	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973	D	0,00273973	D	0,00273973
AA-4	Base de dades Oracle	PF	0,0109589	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AA-5	Base de dades Informix	PF	0,0109589	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AA-6	Firewall (programari lliure)	F	0,01643836	MPF	0,00547945	MPF	0,00547945	PF	0,0109589	D	0,00273973	D	0,00273973	D	0,00273973
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	PF	0,0109589	D	0,00273973	MPF	0,00547945	PF	0,0109589	D	0,00273973	MPF	0,00547945	D	0,00273973
AA-8	Windows 7 (SO portàtils)	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973	MPF	0,00547945	MPF	0,00547945
AA-9	Windows 10 (SO portàtils)	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973	MPF	0,00547945	MPF	0,00547945
AS-1	Contracte seguretat física	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-2	Contracte de lloguer oficines	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-3	Contracte recursos Sistemes Informàtics	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-4	Pàgina web de la organització	D	0,00273973	D	0,00273973	MPF	0,00547945	MPF	0,00547945	MPF	0,00547945	D	0,00273973	D	0,00273973
AS-5	Contracte servei de neteja	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AX-1	Comunicacions CPD Secundari	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973
AX-2	Comunicacions línia mòbil i 3G/4G	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AX-3	Comunicacions llocs de treball amb CPD principal	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973
AX-4	Comunicacions Internet	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-1	Directius de la companyia	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-2	Comandaments intermedis de la companyia	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-3	Administradors de xarxa	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-4	Administradors base de dades (DBA)	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-5	Personal d'estructura	PF	0,0109589	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-6	Personal d'staff	PF	0,0109589	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-1	Backups	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-2	Informació de clients	MPF	0,00547945	MPF	0,00547945	PF	0,0109589	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AD-3	Informació de proveïdors	MPF	0,00547945	MPF	0,00547945	PF	0,0109589	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AD-4	Informació d'empleats	MPF	0,00547945	MPF	0,00547945	PF	0,0109589	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AD-5	Inventari d'actius	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-1	Sistema refrigeració CPDs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-2	Equips de destrucció de paper	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-3	Sistema d'alarmes	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-4	Armaris ignífugs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-1	Edifici corporatiu	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-2	Seus corporatives	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-3	Llocs de treball	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973

Tabla 20: Dimensió seguretat - Errors

Amenaces intencionals presencials		Accés físic no autoritzat, amb destrucció de la informació o amb subministració		Accés lògic no autoritzat		Indisponibilitat de recursos, tant si són humans com tècnics		Filtració de dades a terceres organitzacions	
Codi	Actiu	AM-15		AM-16		AM-17		AM-18	
AH-1	CPD Principal	D	0,00273973	MPF	0,00547945	D	0,00273973	D	0,00273973
AH-2	CPD Secundari	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AH-3	Switchs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-4	Routers	D	0,00273973	PF	0,0109589	MPF	0,00547945	D	0,00273973
AH-5	Punt d'accés Wifi	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973
AH-6	Unitat de cinta	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-7	Portàtils (empleats)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-8	Smartphones Android	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-9	Smartphones Appel	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-10	Unitats d'Emmagatzematge	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-1	Windows Server 2016	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AA-2	Programari VMWare	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-3	Base de dades MySQL	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-4	Base de dades Oracle	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AA-5	Base de dades Informix	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AA-6	Firewall (programari lliure)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	D	0,00273973	D	0,00273973	F	0,01643836	D	0,00273973
AA-8	Windows 7 (SO portàtils)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-9	Windows 10 (SO portàtils)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-1	Contracte seguretat física	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-2	Contracte de lloguer oficines	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-3	Contracte recursos Sistemes Informàtics	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945
AS-4	Pàgina web de la organització	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AS-5	Contracte servei de neteja	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945
AX-1	Comunicacions CPD Secundari	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AX-2	Comunicacions línia mòbil i 3G/4G	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AX-3	Comunicacions llocs de treball amb CPD principal	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AX-4	Comunicacions Internet	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	D	0,00273973	MPF	0,00547945	MPF	0,00547945	D	0,00273973
AP-1	Directius de la companyia	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AP-2	Comandaments intermedis de la companyia	D	0,00273973	D	0,00273973	PF	0,0109589	MPF	0,00547945
AP-3	Administradors de xarxa	D	0,00273973	D	0,00273973	PF	0,0109589	MPF	0,00547945
AP-4	Administradors base de dades (DBA)	D	0,00273973	D	0,00273973	PF	0,0109589	MPF	0,00547945
AP-5	Personal d'estructura	D	0,00273973	D	0,00273973	PF	0,0109589	PF	0,0109589
AP-6	Personal d'staff	D	0,00273973	D	0,00273973	F	0,01643836	PF	0,0109589
AD-1	Backups	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AD-2	Informació de clients	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-3	Informació de proveïdors	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-4	Informació d'empleats	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-5	Inventari d'actius	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-1	Sistema refrigeració CPDs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-2	Equips de destrucció de paper	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AE-3	Sistema d'alarmes	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AE-4	Armaris ignífugs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-1	Edifici corporatiu	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-2	Seus corporatives	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-3	Llocs de treball	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973

Tabla 21: Dimensió seguretat - Amenaces intencionals presencials

Amenaces intencionals remotes		Accés lògic no autoritzat. Accés d'un tercer no autoritzat		Suplantació de l'origen		Cucs. Virus que utilitzen les capacitats de servidors i clients per a pro- pagar-se per Internet		Denegació de servei, sigui contra l'amplada de banda o contra els recursos del sistema	
Codi	Actiu	AM-19		AM-20		AM-21		AM-22	
AH-1	CPD Principal	MPF	0,00547945	D	0,00273973	MPF	0,00547945	D	0,00273973
AH-2	CPD Secundari	MPF	0,00547945	D	0,00273973	MPF	0,00547945	D	0,00273973
AH-3	Switchs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-4	Routers	MPF	0,00547945	MPF	0,00547945	D	0,00273973	MPF	0,00547945
AH-5	Punt d'accés Wifi	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-6	Unitat de cinta	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AH-7	Portàtils (empleats)	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973
AH-8	Smartphones Android	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AH-9	Smartphones Appel	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AH-10	Unitats d'Emmagatzematge	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-1	Windows Server 2016	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AA-2	Programari VMWare	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-3	Base de dades MySQL	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-4	Base de dades Oracle	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-5	Base de dades Informix	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-6	Firewall (programari lliure)	D	0,00273973	D	0,00273973	D	0,00273973	MPF	0,00547945
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AA-8	Windows 7 (SO portàtils)	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973
AA-9	Windows 10 (SO portàtils)	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973
AS-1	Contracte seguretat física	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-2	Contracte de lloguer oficines	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-3	Contracte recursos Sistemes Informàtics	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-4	Pàgina web de la organització	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AS-5	Contracte servei de neteja	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AX-1	Comunicacions CPD Secundari	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AX-2	Comunicacions línia mòbil i 3G/4G	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AX-3	Comunicacions llocs de treball amb CPD principal	MPF	0,00547945	D	0,00273973	D	0,00273973	D	0,00273973
AX-4	Comunicacions Internet	PF	0,0109589	MPF	0,00547945	D	0,00273973	MPF	0,00547945
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	PF	0,0109589	MPF	0,00547945	D	0,00273973	MPF	0,00547945
AP-1	Directius de la companyia	D	0,00273973	D	0,00273973	MPF	0,00547945	D	0,00273973
AP-2	Comandaments intermedis de la companyia	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-3	Administradors de xarxa	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-4	Administradors base de dades (DBA)	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AP-5	Personal d'estructura	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973
AP-6	Personal d'staff	D	0,00273973	D	0,00273973	PF	0,0109589	D	0,00273973
AD-1	Backups	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-2	Informació de clients	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-3	Informació de proveïdors	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-4	Informació d'empleats	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AD-5	Inventari d'actius	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-1	Sistema refrigeració CPDs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-2	Equips de destrucció de paper	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-3	Sistema d'alarmes	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AE-4	Armaris ignífugs	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-1	Edifici corporatiu	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-2	Seus corporatives	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973
AI-3	Llocs de treball	D	0,00273973	D	0,00273973	D	0,00273973	D	0,00273973

Tabla 22: Dimensió seguretat - Amenaces intencionals remotes

Annexe XI – Anàlisi d'impacte versus Impacte Potencial

Indicador	Categoria Actiu	Codi	Actiu	Quantitat	Impacte Qualitatiu	Impacte	Impacte Potencial
AH	Hardware	*AH-1*	CPD Principal	1	C	0,90	157.500,00 €
		AH-2	CPD Secundari	1	C	0,90	157.500,00 €
		AH-3	Switchs	35	B	0,20	1.750,00 €
		AH-4	Routers	7	A	0,75	6.562,50 €
		AH-5	Punt d'accés Wifi	43	B	0,20	1.376,00 €
		AH-6	Unitat de cinta	3	B	0,20	750,00 €
		AH-7	Portàtils (empleats)	18.000	B	0,20	5.220.000,00 €
		AH-8	Smartphones Android	8.000	B	0,20	560.000,00 €
		AH-9	Smartphones Appel	2.500	M	0,50	1.600.000,00 €
		AH-10	Unitats d'Emmagatzematge	12	M	0,50	16.800,00 €
AA	Aplicació i Software	*AA-1*	Windows Server 2016	4	A	0,75	1.350,00 €
		AA-2	Programari VMWare	12	M	0,50	1.650,00 €
		AA-3	Base de dades MySQL	25	M	0,50	1.500,00 €
		AA-4	Base de dades Oracle	12	A	0,75	101.250,00 €
		AA-5	Base de dades Informix	8	M	0,50	5.000,00 €
		AA-6	Firewall (programari lliure)	8	C	0,90	432,00 €
		AA-7	ERP SAP (Gestió RRHH, compres, facturació)	2	C	0,90	135.000,00 €
		AA-8	Windows 7 (SO portàtils)	12.000	M	0,50	1.920.000,00 €
		AA-9	Windows 10 (SO portàtils)	9.000	M	0,50	2.115.000,00 €
AS	Serveis	*AS-1*	Contracte seguretat física	1	B	0,20	2.400,00 €
		AS-2	Contracte de lloguer oficines	1	B	0,20	11.000,00 €
		AS-3	Contracte recursos Sistemes Informàtics	1	B	0,20	3.000,00 €
		AS-4	Pàgina web de la organització	1	M	0,50	117,50 €
		AS-5	Contracte servei de neteja	1	B	0,20	1.700,00 €
AX	Xarxa	*AX-1*	Comunicacions CPD Secundari	2	A	0,75	19.500,00 €
		AX-2	Comunicacions línia mòbil i 3G/4G	1.630	B	0,20	815.000,00 €
		AX-3	Comunicacions llocs de treball amb CPD principal	21.000	M	0,50	120.750.000,00 €
		AX-4	Comunicacions Internet	3	M	0,50	675,00 €
		AX-5	Comunicacions Unitats d'Emmagatzematge núvol	3	M	0,50	1.800,00 €
AP	Personal	*AP-1*	Directius de la companyia	68	C	0,90	918.000,00 €
		AP-2	Comandaments intermedis de la companyia	350	A	0,75	2.887.500,00 €
		AP-3	Administradors de xarxa	7	A	0,75	11.550,00 €
		AP-4	Administradors base de dades (DBA)	4	A	0,75	7.050,00 €
		AP-5	Personal d'estructura	18.870	M	0,50	11.322.000,00 €
		AP-6	Personal d'staff	1.700	B	0,20	374.000,00 €
AD	Dades	*AD-1*	Backups	3	A	0,75	562,50 €
		AD-2	Informació de clients	1	C	0,90	112.500,00 €
		AD-3	Informació de proveïdors	1	C	0,90	67.500,00 €
		AD-4	Informació d'empleats	1	C	0,90	171.000,00 €
		AD-5	Inventari d'actius	1	A	0,75	7.500,00 €
AE	Equipament Auxiliar	*AE-1*	Sistema refrigeració CPDs	4	A	0,75	22.500,00 €
		AE-2	Equips de destrucció de paper	159	M	0,50	119.250,00 €
		AE-3	Sistema d'alarmes	32	M	0,50	60.800,00 €
		AE-4	Armaris ignífugs	63	M	0,50	141.750,00 €
AI	Instal·lacions	*AI-1*	Edifici corporatiu	1	C	0,90	2.106.000,00 €
		AI-2	Seus corporatives	17	C	0,90	4.131.000,00 €
		AI-3	Llocs de treball	21.000	M	0,50	8.925.000,00 €

Tabla 23: Impacte Potencial

Annexe XII – Anàlisi del risc intrínsec

Accidents		Inundació	Incendi	Terratrèmol	Explosió	Avaria	Interrupció dels serveis essencials	Accidents mecànics o electromagnètics
Codi	Actiu	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec
AH-1	CPD Principal	431,51 €	431,51 €	431,51 €	431,51 €	863,01 €	863,01 €	431,51 €
AH-2	CPD Secundari	431,51 €	431,51 €	431,51 €	431,51 €	863,01 €	863,01 €	431,51 €
AH-3	Switchs	4,79 €	4,79 €	4,79 €	4,79 €	9,59 €	9,59 €	4,79 €
AH-4	Routers	17,98 €	17,98 €	17,98 €	17,98 €	35,96 €	35,96 €	17,98 €
AH-5	Punt d'accés Wifi	3,77 €	3,77 €	3,77 €	3,77 €	7,54 €	15,08 €	3,77 €
AH-6	Unitat de cinta	2,05 €	2,05 €	2,05 €	2,05 €	8,22 €	4,11 €	2,05 €
AH-7	Portàtils (empleats)	14.301,37 €	14.301,37 €	14.301,37 €	14.301,37 €	57.205,48 €	28.602,74 €	57.205,48 €
AH-8	Smartphones Android	1.534,25 €	1.534,25 €	1.534,25 €	1.534,25 €	6.136,99 €	6.136,99 €	6.136,99 €
AH-9	Smartphones Appel	4.383,56 €	4.383,56 €	4.383,56 €	4.383,56 €	17.534,25 €	17.534,25 €	17.534,25 €
AH-10	Unitats d'Emmagatzematge	46,03 €	46,03 €	46,03 €	46,03 €	276,16 €	92,05 €	46,03 €
AA-1	Windows Server 2016	3,70 €	3,70 €	3,70 €	3,70 €	3,70 €	3,70 €	3,70 €
AA-2	Programari VMWare	4,52 €	4,52 €	4,52 €	4,52 €	4,52 €	4,52 €	4,52 €
AA-3	Base de dades MySQL	4,11 €	4,11 €	4,11 €	4,11 €	4,11 €	4,11 €	4,11 €
AA-4	Base de dades Oracle	277,40 €	277,40 €	277,40 €	277,40 €	277,40 €	277,40 €	277,40 €
AA-5	Base de dades Informix	13,70 €	13,70 €	13,70 €	13,70 €	13,70 €	13,70 €	13,70 €
AA-6	Firewall (programari lliure)	1,18 €	1,18 €	1,18 €	1,18 €	1,18 €	1,18 €	1,18 €
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	369,86 €	369,86 €	369,86 €	369,86 €	369,86 €	739,73 €	369,86 €
AA-8	Windows 7 (SO portàtils)	5.260,27 €	5.260,27 €	5.260,27 €	5.260,27 €	5.260,27 €	5.260,27 €	5.260,27 €
AA-9	Windows 10 (SO portàtils)	5.794,52 €	5.794,52 €	5.794,52 €	5.794,52 €	5.794,52 €	5.794,52 €	5.794,52 €
AS-1	Contracte seguretat física	6,58 €	6,58 €	6,58 €	6,58 €	6,58 €	6,58 €	6,58 €
AS-2	Contracte de lloguer oficines	30,14 €	30,14 €	30,14 €	30,14 €	30,14 €	30,14 €	30,14 €
AS-3	Contracte recursos Sistemes Informàtics	8,22 €	8,22 €	8,22 €	8,22 €	8,22 €	8,22 €	8,22 €
AS-4	Pàgina web de la organització	0,32 €	0,32 €	0,32 €	0,32 €	0,32 €	0,32 €	0,32 €
AS-5	Contracte servei de neteja	4,66 €	4,66 €	4,66 €	4,66 €	4,66 €	4,66 €	4,66 €
AX-1	Comunicacions CPD Secundari	53,42 €	53,42 €	53,42 €	53,42 €	213,70 €	53,42 €	53,42 €
AX-2	Comunicacions línia mòbil i 3G/4G	2.232,88 €	2.232,88 €	2.232,88 €	2.232,88 €	4.465,75 €	8.931,51 €	2.232,88 €
AX-3	Comunicacions llocs de treball amb CPD principal	330.821,91 €	330.821,91 €	330.821,91 €	330.821,91 €	330.821,91 €	661.643,83 €	330.821,91 €
AX-4	Comunicacions Internet	1,85 €	1,85 €	1,85 €	1,85 €	1,85 €	3,70 €	1,85 €
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	4,93 €	4,93 €	4,93 €	4,93 €	4,93 €	9,86 €	4,93 €
AP-1	Directius de la companyia	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €
AP-2	Comandaments intermedis de la companyia	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €
AP-3	Administradors de xarxa	31,64 €	31,64 €	31,64 €	31,64 €	31,64 €	31,64 €	31,64 €
AP-4	Administradors base de dades (DBA)	19,32 €	19,32 €	19,32 €	19,32 €	19,32 €	19,32 €	19,32 €
AP-5	Personal d'estructura	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €
AP-6	Personal d'staff	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €
AD-1	Backups	1,54 €	1,54 €	1,54 €	1,54 €	1,54 €	1,54 €	1,54 €
AD-2	Informació de clients	308,22 €	308,22 €	308,22 €	308,22 €	308,22 €	308,22 €	308,22 €
AD-3	Informació de proveïdors	184,93 €	184,93 €	184,93 €	184,93 €	184,93 €	184,93 €	184,93 €
AD-4	Informació d'empleats	468,49 €	468,49 €	468,49 €	468,49 €	468,49 €	468,49 €	468,49 €
AD-5	Inventari d'actius	20,55 €	20,55 €	20,55 €	20,55 €	20,55 €	20,55 €	20,55 €
AE-1	Sistema refrigeració CPDs	61,64 €	61,64 €	61,64 €	61,64 €	123,29 €	123,29 €	61,64 €
AE-2	Equips de destrucció de paper	326,71 €	326,71 €	326,71 €	326,71 €	326,71 €	326,71 €	653,42 €
AE-3	Sistema d'alarmes	166,58 €	166,58 €	166,58 €	166,58 €	166,58 €	166,58 €	166,58 €
AE-4	Armaris ignífugs	388,36 €	388,36 €	388,36 €	388,36 €	388,36 €	388,36 €	388,36 €
AI-1	Edifici corporatiu	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €
AI-2	Seus corporatives	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €
AI-3	Llocs de treball	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €	48.904,11 €	48.904,11 €	24.452,05 €

Tabla 24: Risc Intrínsec - Accidents

Errors		Errors en la utilització dels sistemes, provocats per un mal ús	Errors en el disseny conceptual de les aplicacions	Errors en el desenvolupament de les aplicacions	Errors d'actualització o aplicació de pegats als sistemes o aplicacions	Errors en el monitoratge	Errors de compatibilitat entre aplicacions	Errors inesperats (virus, cavalls de Troia, etc.)
Codi	Actiu	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec
AH-1	CPD Principal	863,01 €	431,51 €	431,51 €	431,51 €	431,51 €	431,51 €	863,01 €
AH-2	CPD Secundari	863,01 €	431,51 €	431,51 €	431,51 €	431,51 €	431,51 €	863,01 €
AH-3	Switchs	4,79 €	4,79 €	4,79 €	4,79 €	4,79 €	4,79 €	4,79 €
AH-4	Routers	17,98 €	17,98 €	17,98 €	17,98 €	17,98 €	17,98 €	17,98 €
AH-5	Punt d'accés Wifi	3,77 €	3,77 €	3,77 €	3,77 €	3,77 €	3,77 €	3,77 €
AH-6	Unitat de cinta	2,05 €	2,05 €	2,05 €	2,05 €	2,05 €	2,05 €	2,05 €
AH-7	Portàtils (empleats)	57.205,48 €	14.301,37 €	14.301,37 €	57.205,48 €	28.602,74 €	57.205,48 €	57.205,48 €
AH-8	Smartphones Android	6.136,99 €	6.136,99 €	1.534,25 €	6.136,99 €	1.534,25 €	3.068,49 €	1.534,25 €
AH-9	Smartphones Appel	17.534,25 €	17.534,25 €	4.383,56 €	17.534,25 €	4.383,56 €	8.767,12 €	4.383,56 €
AH-10	Unitats d'Emmagatzematge	46,03 €	46,03 €	46,03 €	46,03 €	46,03 €	46,03 €	46,03 €
AA-1	Windows Server 2016	3,70 €	3,70 €	3,70 €	22,19 €	3,70 €	3,70 €	14,79 €
AA-2	Programari VMWare	4,52 €	4,52 €	4,52 €	9,04 €	4,52 €	4,52 €	4,52 €
AA-3	Base de dades MySQL	8,22 €	4,11 €	4,11 €	16,44 €	4,11 €	4,11 €	4,11 €
AA-4	Base de dades Oracle	1.109,59 €	277,40 €	277,40 €	554,79 €	277,40 €	277,40 €	277,40 €
AA-5	Base de dades Informix	54,79 €	13,70 €	13,70 €	27,40 €	13,70 €	13,70 €	13,70 €
AA-6	Firewall (programari lliure)	7,10 €	2,37 €	2,37 €	4,73 €	1,18 €	1,18 €	1,18 €
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	1.479,45 €	369,86 €	739,73 €	1.479,45 €	369,86 €	739,73 €	369,86 €
AA-8	Windows 7 (SO portàtils)	5.260,27 €	5.260,27 €	10.520,55 €	10.520,55 €	5.260,27 €	10.520,55 €	10.520,55 €
AA-9	Windows 10 (SO portàtils)	5.794,52 €	5.794,52 €	11.589,04 €	11.589,04 €	5.794,52 €	11.589,04 €	11.589,04 €
AS-1	Contracte seguretat física	6,58 €	6,58 €	6,58 €	6,58 €	6,58 €	6,58 €	6,58 €
AS-2	Contracte de lloguer oficines	30,14 €	30,14 €	30,14 €	30,14 €	30,14 €	30,14 €	30,14 €
AS-3	Contracte recursos Sistemes Informàtics	8,22 €	8,22 €	8,22 €	8,22 €	8,22 €	8,22 €	8,22 €
AS-4	Pàgina web de la organització	0,32 €	0,32 €	0,64 €	0,64 €	0,64 €	0,32 €	0,32 €
AS-5	Contracte servei de neteja	4,66 €	4,66 €	4,66 €	4,66 €	4,66 €	4,66 €	4,66 €
AX-1	Comunicacions CPD Secundari	53,42 €	53,42 €	53,42 €	53,42 €	106,85 €	53,42 €	53,42 €
AX-2	Comunicacions línia mòbil i 3G/4G	2.232,88 €	2.232,88 €	2.232,88 €	2.232,88 €	2.232,88 €	2.232,88 €	2.232,88 €
AX-3	Comunicacions llocs de treball amb CPD principal	330.821,91 €	330.821,91 €	330.821,91 €	330.821,91 €	661.643,83 €	330.821,91 €	330.821,91 €
AX-4	Comunicacions Internet	1,85 €	1,85 €	1,85 €	1,85 €	3,70 €	1,85 €	1,85 €
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	4,93 €	4,93 €	4,93 €	4,93 €	4,93 €	4,93 €	4,93 €
AP-1	Directius de la companyia	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €	2.515,07 €
AP-2	Comandaments intermedis de la companyia	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €
AP-3	Administradors de xarxa	31,64 €	31,64 €	31,64 €	31,64 €	31,64 €	31,64 €	31,64 €
AP-4	Administradors base de dades (DBA)	38,63 €	19,32 €	19,32 €	19,32 €	19,32 €	19,32 €	19,32 €
AP-5	Personal d'estructura	124.076,71 €	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €	31.019,18 €
AP-6	Personal d'staff	4.098,63 €	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €	1.024,66 €
AD-1	Backups	1,54 €	1,54 €	1,54 €	1,54 €	1,54 €	1,54 €	1,54 €
AD-2	Informació de clients	616,44 €	616,44 €	1.232,88 €	616,44 €	308,22 €	308,22 €	308,22 €
AD-3	Informació de proveïdors	369,86 €	369,86 €	739,73 €	369,86 €	184,93 €	184,93 €	184,93 €
AD-4	Informació d'empleats	936,99 €	936,99 €	1.873,97 €	936,99 €	468,49 €	468,49 €	468,49 €
AD-5	Inventari d'actius	20,55 €	20,55 €	20,55 €	20,55 €	20,55 €	20,55 €	20,55 €
AE-1	Sistema refrigeració CPDs	61,64 €	61,64 €	61,64 €	61,64 €	61,64 €	61,64 €	61,64 €
AE-2	Equips de destrucció de paper	653,42 €	326,71 €	326,71 €	326,71 €	326,71 €	326,71 €	326,71 €
AE-3	Sistema d'alarmes	166,58 €	166,58 €	166,58 €	166,58 €	166,58 €	166,58 €	166,58 €
AE-4	Armaris ignífugs	388,36 €	388,36 €	388,36 €	388,36 €	388,36 €	388,36 €	388,36 €
AI-1	Edifici corporatiu	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €
AI-2	Seus corporatives	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €
AI-3	Llocs de treball	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €

Tabla 25: Risc Intrínsec - Errors

Amenaces intencionals presencials		Accés físic no autoritzat, amb destrucció de la informació o amb subministració	Accés lògic no autoritzat	Indisponibilitat de recursos, tant si són humans com tècnics	Filtració de dades a terceres organitzacions
Codi	Actiu	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec
AH-1	CPD Principal	431,51 €	863,01 €	431,51 €	431,51 €
AH-2	CPD Secundari	431,51 €	863,01 €	863,01 €	431,51 €
AH-3	Switchs	4,79 €	4,79 €	4,79 €	4,79 €
AH-4	Routers	17,98 €	71,92 €	35,96 €	17,98 €
AH-5	Punt d'accés Wifi	3,77 €	3,77 €	15,08 €	3,77 €
AH-6	Unitat de cinta	2,05 €	2,05 €	2,05 €	2,05 €
AH-7	Portàtils (empleats)	14.301,37 €	14.301,37 €	14.301,37 €	14.301,37 €
AH-8	Smartphones Android	1.534,25 €	1.534,25 €	1.534,25 €	1.534,25 €
AH-9	Smartphones Appel	4.383,56 €	4.383,56 €	4.383,56 €	4.383,56 €
AH-10	Unitats d'Emmagatzematge	46,03 €	46,03 €	46,03 €	46,03 €
AA-1	Windows Server 2016	3,70 €	3,70 €	7,40 €	3,70 €
AA-2	Programari VMWare	4,52 €	4,52 €	4,52 €	4,52 €
AA-3	Base de dades MySQL	4,11 €	4,11 €	4,11 €	4,11 €
AA-4	Base de dades Oracle	277,40 €	277,40 €	554,79 €	277,40 €
AA-5	Base de dades Informix	13,70 €	13,70 €	27,40 €	13,70 €
AA-6	Firewall (programari lliure)	1,18 €	1,18 €	1,18 €	1,18 €
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	369,86 €	369,86 €	2.219,18 €	369,86 €
AA-8	Windows 7 (SO portàtils)	5.260,27 €	5.260,27 €	5.260,27 €	5.260,27 €
AA-9	Windows 10 (SO portàtils)	5.794,52 €	5.794,52 €	5.794,52 €	5.794,52 €
AS-1	Contracte seguretat física	6,58 €	6,58 €	6,58 €	6,58 €
AS-2	Contracte de lloguer oficines	30,14 €	30,14 €	30,14 €	30,14 €
AS-3	Contracte recursos Sistemes Informàtics	8,22 €	8,22 €	8,22 €	16,44 €
AS-4	Pàgina web de la organització	0,32 €	0,32 €	0,64 €	0,32 €
AS-5	Contracte servei de neteja	4,66 €	4,66 €	4,66 €	9,32 €
AX-1	Comunicacions CPD Secundari	53,42 €	106,85 €	106,85 €	53,42 €
AX-2	Comunicacions línia mòbil i 3G/4G	2.232,88 €	2.232,88 €	4.465,75 €	2.232,88 €
AX-3	Comunicacions llocs de treball amb CPD principal	330.821,91 €	330.821,91 €	330.821,91 €	330.821,91 €
AX-4	Comunicacions Internet	1,85 €	3,70 €	3,70 €	1,85 €
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	4,93 €	9,86 €	9,86 €	4,93 €
AP-1	Directius de la companyia	2.515,07 €	2.515,07 €	5.030,14 €	2.515,07 €
AP-2	Comandaments intermedis de la companyia	7.910,96 €	7.910,96 €	31.643,84 €	15.821,92 €
AP-3	Administradors de xarxa	31,64 €	31,64 €	126,58 €	63,29 €
AP-4	Administradors base de dades (DBA)	19,32 €	19,32 €	77,26 €	38,63 €
AP-5	Personal d'estructura	31.019,18 €	31.019,18 €	124.076,71 €	124.076,71 €
AP-6	Personal d'staff	1.024,66 €	1.024,66 €	6.147,95 €	4.098,63 €
AD-1	Backups	1,54 €	1,54 €	3,08 €	1,54 €
AD-2	Informació de clients	308,22 €	308,22 €	308,22 €	308,22 €
AD-3	Informació de proveïdors	184,93 €	184,93 €	184,93 €	184,93 €
AD-4	Informació d'empleats	468,49 €	468,49 €	468,49 €	468,49 €
AD-5	Inventari d'actius	20,55 €	20,55 €	20,55 €	20,55 €
AE-1	Sistema refrigeració CPDs	61,64 €	61,64 €	61,64 €	61,64 €
AE-2	Equips de destrucció de paper	326,71 €	326,71 €	653,42 €	326,71 €
AE-3	Sistema d'alarmes	166,58 €	166,58 €	333,15 €	166,58 €
AE-4	Armaris ignífugs	388,36 €	388,36 €	388,36 €	388,36 €
AI-1	Edifici corporatiu	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €
AI-2	Seus corporatives	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €
AI-3	Llocs de treball	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €

Tabla 26: Risc Intrínsec - Amenaces intencionals presencials

Amenaces intencionals remotes		Accés lògic no autoritzat. Accés d'un tercer no autoritzat	Suplantació de l'origen	Cucs. Virus que utilitzen les capacitats de servidors i clients per a pro- pagar-se per Internet	Denegació de servei, sigui contra l'amplada de banda o contra els recursos del sistema
Codi	Actiu	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec	Risc Intrínsec
AH-1	CPD Principal	863,01 €	431,51 €	863,01 €	431,51 €
AH-2	CPD Secundari	863,01 €	431,51 €	863,01 €	431,51 €
AH-3	Switchs	4,79 €	4,79 €	4,79 €	4,79 €
AH-4	Routers	35,96 €	35,96 €	17,98 €	35,96 €
AH-5	Punt d'accés Wifi	3,77 €	3,77 €	3,77 €	3,77 €
AH-6	Unitat de cinta	2,05 €	2,05 €	2,05 €	2,05 €
AH-7	Portàtils (empleats)	14.301,37 €	14.301,37 €	57.205,48 €	14.301,37 €
AH-8	Smartphones Android	1.534,25 €	1.534,25 €	3.068,49 €	1.534,25 €
AH-9	Smartphones Appel	4.383,56 €	4.383,56 €	8.767,12 €	4.383,56 €
AH-10	Unitats d'Emmagatzematge	46,03 €	46,03 €	46,03 €	46,03 €
AA-1	Windows Server 2016	3,70 €	3,70 €	7,40 €	3,70 €
AA-2	Programari VMWare	4,52 €	4,52 €	4,52 €	4,52 €
AA-3	Base de dades MySQL	4,11 €	4,11 €	4,11 €	4,11 €
AA-4	Base de dades Oracle	277,40 €	277,40 €	277,40 €	277,40 €
AA-5	Base de dades Informix	13,70 €	13,70 €	13,70 €	13,70 €
AA-6	Firewall (programari lliure)	1,18 €	1,18 €	1,18 €	2,37 €
AA-7	ERP SAP (Gestió RRHH, compres, facturació)	369,86 €	369,86 €	369,86 €	369,86 €
AA-8	Windows 7 (SO portàtils)	5.260,27 €	5.260,27 €	21.041,10 €	5.260,27 €
AA-9	Windows 10 (SO portàtils)	5.794,52 €	5.794,52 €	23.178,08 €	5.794,52 €
AS-1	Contracte seguretat física	6,58 €	6,58 €	6,58 €	6,58 €
AS-2	Contracte de lloguer oficines	30,14 €	30,14 €	30,14 €	30,14 €
AS-3	Contracte recursos Sistemes Informàtics	8,22 €	8,22 €	8,22 €	8,22 €
AS-4	Pàgina web de la organització	0,32 €	0,32 €	0,32 €	0,32 €
AS-5	Contracte servei de neteja	4,66 €	4,66 €	4,66 €	4,66 €
AX-1	Comunicacions CPD Secundari	106,85 €	53,42 €	53,42 €	53,42 €
AX-2	Comunicacions línia mòbil i 3G/4G	2.232,88 €	2.232,88 €	2.232,88 €	2.232,88 €
AX-3	Comunicacions llocs de treball amb CPD principal	661.643,83 €	330.821,91 €	330.821,91 €	330.821,91 €
AX-4	Comunicacions Internet	7,40 €	3,70 €	1,85 €	3,70 €
AX-5	Comunicacions Unitats d'Emmagatzematge núvo	19,73 €	9,86 €	4,93 €	9,86 €
AP-1	Directius de la companyia	2.515,07 €	2.515,07 €	5.030,14 €	2.515,07 €
AP-2	Comandaments intermedis de la companyia	7.910,96 €	7.910,96 €	7.910,96 €	7.910,96 €
AP-3	Administradors de xarxa	31,64 €	31,64 €	31,64 €	31,64 €
AP-4	Administradors base de dades (DBA)	19,32 €	19,32 €	19,32 €	19,32 €
AP-5	Personal d'estructura	31.019,18 €	31.019,18 €	124.076,71 €	31.019,18 €
AP-6	Personal d'staff	1.024,66 €	1.024,66 €	4.098,63 €	1.024,66 €
AD-1	Backups	1,54 €	1,54 €	1,54 €	1,54 €
AD-2	Informació de clients	308,22 €	308,22 €	308,22 €	308,22 €
AD-3	Informació de proveïdors	184,93 €	184,93 €	184,93 €	184,93 €
AD-4	Informació d'empleats	468,49 €	468,49 €	468,49 €	468,49 €
AD-5	Inventari d'actius	20,55 €	20,55 €	20,55 €	20,55 €
AE-1	Sistema refrigeració CPDs	61,64 €	61,64 €	61,64 €	61,64 €
AE-2	Equips de destrucció de paper	326,71 €	326,71 €	326,71 €	326,71 €
AE-3	Sistema d'alarmes	166,58 €	166,58 €	166,58 €	166,58 €
AE-4	Armaris ignífugs	388,36 €	388,36 €	388,36 €	388,36 €
AI-1	Edifici corporatiu	5.769,86 €	5.769,86 €	5.769,86 €	5.769,86 €
AI-2	Seus corporatives	11.317,81 €	11.317,81 €	11.317,81 €	11.317,81 €
AI-3	Llocs de treball	24.452,05 €	24.452,05 €	24.452,05 €	24.452,05 €

Tabla 27: Risc Intrínsec - Amenaces intencionals remotes

Annexe XIII – Projectes a curt termini

El següent quadre mostra la planificació dels projectes proposats.

	Nombre	Duracion	Inicio	Terminado	Predecesores
1	**Projectes curt termini**	**283 days**	**2/09/19 8:00**	**30/09/20 17:00**	
2	SGSI-1-1 Inventari d'actius (CMDB)	26,25 days	2/09/19 8:00	8/10/19 10:00	
3	SGSI-2-1 Implementació d'un ATD (Advanced Threat Detection)	48,75 days	8/10/19 10:00	13/12/19 17:00	2
4	SGSI-3-1 Implementació d'un sistema de traçabilitat	39 days	16/12/19 8:00	6/02/20 17:00	3
5	SGSI-4-1 Programa de conscienciació sobre la seguretat	24,88 days	7/02/20 8:00	12/03/20 16:02	4
6	SGSI-5-1 Implementació d'auditories de compliment normatiu	51,25 days	12/03/20 16:02	25/05/20 9:02	5
7	SGSI-6-1 Procediments i gestió d'auditories internes i externes	38,75 days	25/05/20 9:02	16/07/20 16:02	6
8	SGSI-7-1 Política de gestió de backups	54,12 days	16/07/20 16:02	30/09/20 17:00	7

A continuació es mostren les fitxes amb el detall de cada un dels projectes contemplats en aquest termini.

Projecte	**SGSI-1-1 Inventari d'actius (CMDB)**
Responsables	Responsable de Seguretat
Objectiu	Inventariar els actius de la companyia
Descripció i accions necessaris per a la seva posada en marxa	
L'inventari d'actius de l'organització es realitzarà mitjançant programari CMDB, que és l'acrònim de «configuration management database». Terme que prové del mon ITIL. Un CMDB és un repositori que relaciona tots els «elements de configuració» (en anglès Configuration Items o CI's) de l'organització i les seves relacions. Els «elements de configuració» que es tindran en compte en l'inventari seran els serveis que ofereix el departament d'IT, elements de maquinari necessaris per al desenvolupament de l'activitat de l'organització (màquines, servidors, routers, perifèrics, etc.), persones involucrades, xarxes, software, documentació, proveïdors, etc. La importància de tenir una correcta CMDB ve de que permet disposar de la informació necessària per a la presa de decisions pel que fa a qualsevol canvi en un «element de configuració», l'impacte que pot tenir aquest canvi en els serveis que ofereix el departament de tecnologia, l'impacte sobre la infraestructura (canvi en un servei, la seva ampliació, cancel·lació, etc.).	
Departament/s implicat/s	Departament IT
Planificació del projecte	Del 02/09/2019 al 08/10/2019
Recursos econòmic	12.705,00 €
Controls ISO afectats	8.1 Responsabilitats sobre els actius 8.2 Classificació de la informació
Resultats esperats	Repositori que relaciona tots els «elements de configuració» de l'organització
Riscos que mitiga	Els actius de la informació han de ser classificats d'acord la sensibilitat i criticitat de la informació que contenen o bé d'acord la funcionalitat que compleixen, amb l'objectiu de senyalar con ha de ser tractada i protegida la informació.
Relació amb altres projectes	
Factors crítics d'èxit	Compliment de les especificacions de la ISO/IEC 27002

Projecte	**SGSI-2-1 Implementació d'un ATD (Advanced Threat Detection)**
Responsables	Responsable de Seguretat
Objectiu	Implementar un model per a la detecció d'amenaces tant internes com externes
Descripció i accions necessaris per a la seva posada en marxa	
Avui en dia, les organitzacions necessiten un nou model de protecció contra amenaces en el que l'arquitectura de defensa incorpori una capa que prescindeixi de l'ús de signatures per a neutralitzar la nova generació de cyberatacs. Ara que els atacs desconeguts (zero-day), polimòrfics i d'amenaces persistents avançades són pràcticament desconeguts i s'estan convertint en un medi habitual per a tenir èxits, és necessari disposar de solucions que no utilitzin signatures. La selecció i implantació d'un sistema ATD es realitzarà tenint en compte les següents premisses; • Evitar solucions ATD que només detectin. • Evitar ofertes basades en entorns de prova o sandbox. • Evitar anàlisi de malware des de el núvol. • Evitar dispositius «all in one». Cal disposar de dispositius especialment dissenyats per a la protecció del correu electrònic, web, arxius compartits, etc.	
Departament/s implicat/s	Departament IT Àrea seguretat corporativa
Planificació del projecte	Del 08/10/2019 al 13/12/2019
Recursos econòmic	23.595,00 €
Controls ISO afectats	9.4 Control d'accés a sistemes i aplicacions 12.2 Protecció contra codi maliciós 13.1 Gestió de la seguretat en les xarxes
Resultats esperats	Sistema de gestió d'alertes contra l'accés no autoritzat
Riscos que mitiga	- Evitar l'accés no autoritzat als Sistemes d'Informació - Detecció i alerta de codi maliciós - Protecció de les dades confidencials que circulen per la xarxa evitant d'aquesta manera la seva fuga fora de l'organització de manera no controlada
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB)
Factors crítics d'èxit	Identificació dels punts crítics d'accés a la xarxa i punts vulnerables

Projecte	**SGSI-3-1 Implementació d'un sistema de traçabilitat**
Responsables	Responsable de Seguretat
Objectiu	Implementar un sistema de traçabilitat que ajudi a l'anàlisi de la causa en el cas d'incident de seguretat
Descripció i accions necessaris per a la seva posada en marxa	
Els sistemes de traçabilitat registren l'activitat dels usuaris i dels seus processos (login/logout, origen, temps d'activitat, accions, connexions, ...) en registre d'events o logs. La informació d'aquests registres és essencial per a l'elaboració d'informes de gestió i monitorització. Entre els diferents events que es registraran estan l'inici/fi de sessió, l'accés i modificació de fitxers i directoris, canvi en les configuracions principals, execució de programes, accessos a internet, instal·lació de programari, etc.. Els registres d'activitat dels diferents sistemes i equips són dades a partir de les quals és possible, no tan sols detectar errades de rendiment o mal funcionament, si no també detectar errors e intrusions. Amb aquesta informació alimentarà els sistemes de monitorització per a la generació d'alertes en temps real. La implantació d'un sistema de traçabilitat facilita l'anàlisi forense per al diagnòstic de les causes que originen incidents de seguretat. Per ultim, són necessaris per verificar el compliment de certs requeriments legals o contractuals durant les auditories.	
Departament/s implicat/s	Departament IT Àrea seguretat corporativa
Planificació del projecte	Del 16/12/2019 al 06/02/2020
Recursos econòmic	18.452,50 €
Controls ISO afectats	9.4 Control d'accés a sistemes i aplicacions 12.2 Protecció contra codi maliciós 13.1 Gestió de la seguretat en les xarxes
Resultats esperats	Reporting per a l'anàlisi d'incidents de seguretat
Riscos que mitiga	Determinar la causa de qualsevol incident de seguretat que es produeixi. Analitzar les traces de manera proactiva permetrà detectar qualsevol «bug» de seguretat.
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB)
Factors crítics d'èxit	Definició de les traces i nivell de detall d'aquestes

Projecte	**SGSI-4-1 Programa de conscienciació sobre la seguretat**
Responsables	Responsable de Seguretat
Objectiu	Conscienciació a tots els empleats de la companyia de les mesures de seguretat a tenir en compte en el dia a dia així com dels recursos de formació i consulta disponibles
Descripció i accions necessaris per a la seva posada en marxa	
El programa de conscienciació consisteix en una sèrie de mesures encaminades a realitzar un procés formatiu combinant la distribució de material per a la seva lectura i visualització i addicionalment l'organització de sessions presencials. Aquesta constarà de quatre blocs temàtics o píndoles: la informació, els dispositius de suport, el lloc de treball i els dispositius mòbils. Cada píndola la compondran els següents materials: vídeos interactius, presentacions, documents de text i test d'autoavaluació. Per a fomentar la participació dels empleats el «kit» disposarà de quatre vídeos interactius associats a les píndoles. En aquests vídeos es mostraran consells i bones pràctiques en el lloc de treball i en l'entorn laboral. Representaran escenes quotidianes en una oficina qualsevol. En les escenes hauran icones sobre les quals es podrà fer click per a llegir en més detall els diferents consells. Cada una de les píndoles estarà explicada en un document de text. Aquests documents contindran informació sobre els conceptes, mesures i bones pràctiques mencionades en les presentacions i vídeos interactius. Les presentacions i els documents podran distribuir-se per a una lectura individual o explicar-se en una sessió formativa. Els test d'autoavaluació amb preguntes sobre cada temàtica permetran a l'usuari comprovar el grau de coneixement adquirit així com determinar en nivell d'eficàcia del programa per part de l'organització.	
Departament/s implicat/s	Departament IT Àrea seguretat corporativa
Planificació del projecte	Del 07/02/2020 al 12/03/2020
Recursos econòmic	12.039,50 €
Controls ISO afectats	5.1 Directius de la Direcció en seguretat de la informació 16.1 Gestió dels incidents de seguretat i millores 17.1 Continuïtat de la seguretat de la informació 18.1 Compliment dels requisits legals i contractuals 18.2 Revisions de la seguretat de la informació
Resultats esperats	Conscienciació i aplicació de les píndoles de seguretat per part de tots els empleats de la companyia Reducció dels incidents de seguretat
Riscos que mitiga	Prevenir qualsevol incident de seguretat per causa humana.
Relació amb altres projectes	SGSI-5-1 Implementació d'auditories de compliment normatiu SGSI-6-1 Procediments i gestió d'auditories internes i externes
Factors crítics d'èxit	Kit i píndoles formatives simples i fàcils d'entendre

Projecte	**SGSI-5-1 Implementació d'auditories de compliment normatiu**
Responsables	Responsable de Seguretat
Objectiu	Disposar de protocols per al control del compliment normatiu
Descripció i accions necessaris per a la seva posada en marxa	
L'organització implementarà serveis gestionats de Compliment Normatiu i Legal que permetran demostrar als auditors el compliment de regulacions i normatives d'una manera eficient i proactiva. Aquests serveis hauran d'estar enfocats a accions que combinin les necessitats de seguretat i de l'entorn de IT amb els requisits per al compliment de la legislació a aplicar. Es posarà especial focus en: • LOPD: Llei Orgànica de Protecció de Dades de Caràcter Personal i Reglament de Mesures de Seguretat. • GDPR: Reglament General de Protecció de Dades (Reglament 2016/679). • LSSI/CE: Llei de Serveis de la Societat de la Informació i el Comerç Electrònic (Llei 34/2002 de 11 de juliol). • Canvis regulatius (codi penal, etc) i revisió de línies ètiques. • Normatives pròpies de l'organització o de legislacions específiques. • Manteniment de Documents de Seguretat.	
Departament/s implicat/s	Departament legal Àrea seguretat corporativa
Planificació del projecte	Del 12/03/2020 al 25/05/2020
Recursos econòmic	24.805,00 €
Controls ISO afectats	18.1 Compliment dels requisits legals i contractuals
Resultats esperats	Compliment de les polítiques i normes legals i contractuals
Riscos que mitiga	Evitar sancions econòmiques per incompliment de la normativa legal i contractual. Addicionalment i de manera implícita també s'evita la pèrdua de prestigi.
Relació amb altres projectes	Implementació d'auditories de compliment normatiu
Factors crítics d'èxit	Protocols per al compliment i control del compliment de LOPD, GDPR, LSSI/CE

Projecte	**SGSI-6-1 Procediments i gestió d'auditories internes i externes**
Responsables	Responsable de Seguretat
Objectiu	Disposar d'un procediment per a la gestió d'auditories internes i externes en compliment de la ISO/IEC 27002
Descripció i accions necessaris per a la seva posada en marxa	
En un Sistema de Gestió de la Seguretat de la Informació basat en la norma ISO/IEC 27001 es fa necessari dur a terme auditories internes cada cert temps per poder comprovar que l'estat del SGSI sigui el correcte. El principal objectiu de que es realitzin auditories internes de manera periòdica és poder determinar si els objectius, els controls, els processos i els procediments del SGSI es troben: • Conformes al requeriments que estableix l'estàndard internacional ISO/IEC 27001, a més de la legislació i els reglaments d'aplicació. • Concorde els requisits establerts en seguretat de la informació. • Eficaçment implementats. • Comportant-se de manera esperada. Per a més informació consultar l'apartat Annexe III – Procediment d'auditories internes.	
Departament/s implicat/s	Departament Compliance Àrea de seguretat corporativa
Planificació del projecte	Del 25/05/2020 al 16/07/2020
Recursos econòmic	18.755,00 €
Controls ISO afectats	18.2 Revisió de la seguretat de la informació
Resultats esperats	Compliment de les especificacions indicades en la Política de Seguretat
Riscos que mitiga	Evitar error o indefinicions en la implementació del SGSI. Garantir que s'implementa i opera la seguretat de la informació segons les polítiques i procediments definits.
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB) SGSI-2-1 Implementació d'un ATD (Advanced Threat Detection) SGSI-4-1 Programa de conscienciació sobre la seguretat SGSI-2-3 Pla de continuïtat de negoci
Factors crítics d'èxit	Aplicació del document «Procediment Auditories Internes» i definició del «Procediment d'auditories externes»

Projecte	**SGSI-7-1 Política de gestió de backups**
Responsables	Responsable de Seguretat
Objectiu	Disposar d'una política robusta de backups
Descripció i accions necessaris per a la seva posada en marxa	
Els sistemes de backup s'han convertit en un aspecte de suma importància per a l'organització. La pèrdua de dades pot causar importants danys econòmics i fins i tot derivar en aspectes legals. Per tal motiu l'organització establirà una política de backup tenint en compte els següents aspectes; • Definir el tipus de dades dels que es farà el backup. Establir el nivell d'importància de les dades. • Escollir en nivell o nivells de backup: ◦ Sistema backup complet ◦ Sistema backup incremental ◦ Sistema backup diferencial • Àmbit de restauració i disponibilitat. Es tracta d'establir el temps necessari per a restaurar un arxiu a una versió anterior. • Establir les tecnologies i plataformes que intervindran en el backup. És important també, conèixer els diferents recursos dels que es disposa. Per exemple, la velocitat de la xarxa, el hardware... • Entorns en els que es treballarà; pre-producció, desenvolupament, producció. • Temps de recuperació del backup. Com es pot veure, un dels aspectes importants a considerar és la periodicitat amb la que es farà el backup. El temps idoni és realitzar còpies de seguretat diàries de la informació que s'actualitza amb freqüència i que és d'alt valor per a l'organització. Per a dades amb informació menys sensible i que no s'actualitzi amb regularitat pot implementar-se un backup setmanal.	
Departament/s implicat/s	Departament IT
Planificació del projecte	Del 16/07/2020 al 30/09/2020
Recursos econòmic	15.730,00 €
Controls ISO afectats	12.3 Còpies de seguretat
Resultats esperats	Disposar d'un registre de backups que permeti la recuperació de la informació en cas de pèrdua d'aquesta
Riscos que mitiga	Danys o pèrdua de la informació / actius de la companyia.
Relació amb altres projectes	SGSI-4-1 Programa de conscienciació sobre la seguretat SGSI-5-1 Implementació d'auditories de compliment normatiu
Factors crítics d'èxit	Inventari de les dades corporatives implicades en el procés de backup i definició per cada una d'elles el nivell a aplicar

Annexe XIV – Projectes a mig termini

El següent quadre mostra la planificació dels projectes proposats.

	Nombre	Duracion	Inicio	Terminado	Predecesores
9	**Projectes mig termini**	**258 days**	**1/10/20 8:00**	**27/09/21 17:00**	**1**
10	SGSI-1-2 Actualització de software; SO i aplicacions corporatives	32,5 days	1/10/20 8:00	16/11/20 13:00	
11	SGSI-2-2 Actualització del sofware de backups	15 days	16/11/20 13:00	7/12/20 13:00	10
12	SGSI-3-2 Millora dels Centre de Processament de Dades	97,75 days	7/12/20 13:00	22/04/21 10:00	11
13	SGSI-4-2 Migració Windows 2003 a Windows server 2012	10 days	22/04/21 10:00	6/05/21 10:00	12
14	SGSI-5-2 Migració Oracle 10g a Oracle 12c	15 days	6/05/21 10:00	27/05/21 10:00	13
15	SGSI-6-2 Actualització patchs mòbils Apple	32,63 days	27/05/21 10:00	12/07/21 16:02	14
16	SGSI-7-2 Actualització patchs mòbils Android	55,12 days	12/07/21 16:02	27/09/21 17:00	15

A continuació es mostren les fitxes amb el detall de cada un dels projectes contemplats en aquest termini.

Projecte	**SGSI-1-2 Actualització de software; SO i aplicacions corporatives**
Responsables	Responsable IT
Objectiu	Disposar de de les últimes correccions en matèria de seguretat dels SO dels servidors corporatius així com de la resta d'aplicacions corporatives
Descripció i accions necessaris per a la seva posada en marxa	
S'actualitzaran tots els Sistemes Operatius amb les últimes revisions de seguretat dels servidors corporatius. Així mateix es procedirà a sol·licitar als proveïdors d'aplicacions corporatives tots els «fix» dels seus productes. Les actualitzacions es duran a terme fora de l'horari labora per a minimitzar l'impacte a l'usuari i generar la indisponibilitat dels serveis. Serà necessari disposar de les instruccions detallades per part dels proveïdors de software a fi de facilitar a l'equip d'IT la seva revisió (i en cas d'incongruències poder-les aclarir) així com el procediment d'actualització.	
Departament/s implicat/s	Departament IT Proveïdors del programari
Planificació del projecte	Del 01/10/2020 al 16/11/2020
Recursos econòmic	15.730,00 €
Controls ISO afectats	9.4 Control d'accés a sistemes i aplicacions 12.5 Control del software en explotació 14.1 Requisits de seguretat dels sistemes d'informació
Resultats esperats	Sistemes actualitzats amb els últims fix de seguretat dels diferents fabricants
Riscos que mitiga	«Bugs» de seguretat que posin en perill la informació sensible dels equips i aplicacions corporatives.
Relació amb altres projectes	Inventari d'actius Programa de conscienciació sobre la seguretat
Factors crítics d'èxit	Disposar del procediment validat entre el departament d'IT/Proveïdor

Projecte	**SGSI-2-2 Actualització del sofware de backups**
Responsables	Responsable IT
Objectiu	Disposar del programari actualitzat de backup que disminueixi el temps de còpia/restauració amb la possibilitat de tenir backups al núvol
Descripció i accions necessaris per a la seva posada en marxa	
La gestió de les còpies de seguretat i la seva restauració en un temps raonable és crític per a la companyia. A l'hora de seleccionar el programari per a la realització de còpies de seguretat caldrà tenir presents els següents requeriments; • Seguretat i fiabilitat; amb tots els arxius que s'emmagatzemin al núvol. • Automatització; el programari ha d'admetre diferents calendaris de procés. • Fàcil ús; el desitjable és que l'aplicació sigui el més intuïtiva possible, de manera que qualsevol persona autoritzada pugui recuperar informació de manera senzilla i en el menor temps possible.	
Departament/s implicat/s	Departament IT
Planificació del projecte	Del 16/11/2020 al 07/12/2020
Recursos econòmic	7.260,00 €
Controls ISO afectats	8.2 Classificació de la informació 8.3 Gestió de suports d'emmagatzematge 12.3 Còpies de Seguretat 13.2 Intercanvi de la informació amb terceres parts
Resultats esperats	Gestió eficients de les còpies/restauració de la informació en un temps raonable
Riscos que mitiga	Errors de programari / incompatibilitats amb el Sistema Operatiu que el soporta que provoquin un mal funcionament del programari de backup i com a resultat derivi en una còpia errònia.
Relació amb altres projectes	Inventari d'actius Política de gestió de backups
Factors crítics d'èxit	Selecció adequada del programa de backup / compatibilitat amb els dispositius de còpia de la companyia

Projecte	**SGSI-3-2 Millora dels Centre de Processament de Dades**
Responsables	Responsable de Seguretat Responsable IT
Objectiu	Condicionar el CPD amb les mesures de seguretat física segons la Política de Seguretat i en compliment del marc legal aplicable

Descripció i accions necessaris per a la seva posada en marxa

Els CPDs han crescut segons les necessitats de l'organització i es veu necessari revisar que disposen de les mesures de seguretat adequades segons els riscos;

- Talls elèctrics, pujades de tensió
- Foc
- Inundacions
- Temperatura inadequada per fallida de l'aire condicionat
- Humitat excessiva provocada per la condensació d'aigua
- Accessos no autoritzats, malintencionats, robatoris, actes vandàlics, etc.

Per a mitigar aquests riscos cal modernitzar el CPD, implantant mesures de seguretat i gestió mediambiental que permetin monitorar les incidències i actuar sobre aquestes.

Les mesures a implantar seran les descrites a continuació:

- **Mesures contra fallida del subministrament elèctric**; Instal·lar un sistema d'alimentació ininterrompuda (SAI) que permeti disposar de subministrament elèctric durant un temps i permetre la parada segura dels servidors.
- **Control d'accés** que permet un seguiment del personal que hi accedeix, amb obertura segura, sensors en les portes i dispositius d'autorització i gravació d'imatges en el seu interior.
- **Mesures de detecció contra incendis**; Sistema de detecció de foc i extinció.
- **Mesures de control ambiental**; Sistema que permeti monitorar i generar alertes si el CPD supera els rangs establerts d'humitat, temperatura, partícules en l'aire.
- **Sistema de climatització**; Tot això controlat des de una consola i monitoritzat en temps real per a poder actuar en cas d'incident.

Departament/s implicat/s	Departament IT
Planificació del projecte	Del 07/12/2020 al 22/04/2021
Recursos econòmic	47.311,00 €
Controls ISO afectats	17.1 Continuïtat de la seguretat de la informació 17.2 Redundàncies 18.1 Compliment dels requisits legals i contractuals
Resultats esperats	Increment de la seguretat física del CPD
Riscos que mitiga	- Evitar fallides del subministrament electric. - Evitar l'accés a personal no autoritzat. - Evitar incendis o incidents medioambientals - Evitar l'augment de temperatura que provoqui un malfuncionament al CPD.
Relació amb altres projectes	Implementació d'auditories de compliment normatiu
Factors crítics d'èxit	N/A

Projecte	**SGSI-4-2 Migració Windows 2003 a Windows server 2012**
Responsables	Responsable IT
Objectiu	Migració del Sistema Operatiu de Windows Server 2003 Server a Windows Server 2012
Descripció i accions necessaris per a la seva posada en marxa	
Microsoft ha deixat de donar suport a Windows Server 2003. Qualsevol manteniment d'aquesta versió haurà de contractar-se a banda suportant l'elevat cost imposat per Microsoft. La migració caldrà fer-se de manera escalonada (no big-bang), és a dir, establir en el pla de migració sobre quins servidors es farà la migració i quines seran les proves per a donar per bo el procés. El procés de migració es durà a terme seguint les instruccions del fabricant del Software. Addicionalment i per minimitzar qualsevol risc caldrà disposar de suport per part de Microsoft.	
Departament/s implicat/s	Departament IT
Planificació del projecte	Del 22/04/2021 al 06/05/2021
Recursos econòmic	4.840,00 €
Controls ISO afectats	12.5 Control del software en explotació
Resultats esperats	Upgrade del sistema operatiu dels servidors de la companyia
Riscos que mitiga	Evitar que el software quedi fora de manteniment per part del proveïdor així com la absencia de les últimes modificacions (fix) a nivell de seguretat.
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB)
Factors crítics d'èxit	Planificació del procés de migració de manera escalonada (no big-bang)

Projecte	**SGSI-5-2 Migració Oracle 10g a Oracle 12c**
Responsables	Responsable IT
Objectiu	

Descripció i accions necessaris per a la seva posada en marxa

A fi de disposar de l'última tecnologia a nivell de Base de Dades d'Oracle incloent les millores proporcionades per la nova versió així com aspectes clau de seguretat, es procedirà a la migració de la versió 10g a la versió 12c.
Aquesta migració (upgrade de versió) es durà a terme mitjançant l'eina «Database Upgrade Assistant (DBUA)».
El DBUA és un «Graphical User Intergace (GUI)» que guiarà al «DBA» a través del procés de upgrade de base de dades presentant una sèrie de pantalles que permetran l'especificació de les opcions dessitjades.
Durant el procés, el «DBUA» invocarà els mateixos scripts utilitzats pel «Command-line Upgrade». Addicionalment el «DBUA» durà a terme la validació «pre-upgrade» i «post-upgrade».
Mitjançant aquesta eina es reduirà significativament la quantitat de temps per a la realització de la migració.

Les fases per a la migració des de el «Command-line upgrade» són les següents:
Fase "Pre-upgrade"
- Executar el nou «Pre-Upgrade Information Tool» (preupgrd.sql) qui realitzarà les validacions
- Executar l'script «preupgrade_fixups.sql» per a resoldre totes les incongruències senyalades pel procés anterior
- Dur a terme el «Manual Fixups» senyalats pel «Pre-Upgrade Information Tool»

Fase de "Upgrade"
- Execució del «Parallel Upgrade Utility» (catcrl.pl)

Fase de "Post-Upgrade"
- Execució de l'script «postupgrade_fixups.sql» per a resoldre automàticament qualsevol incongruència identificada pel procés «Pre-Upgrade Information Tool»
- Execució del procés «Post-Upgrade Status Tool» (utlu121s.sql) per a visualitzar un resum dels resultats de l'upgrade
- Validar els arxius «logs» generats pel procés «Parallel Upgrade Utility»
- Re-compilar objectes no vàlids executant el procés utlrp.sql
- Verificar l'status dels objectes pre-compilats (utluiobj.sql)

L'upgrade de les BDD objecte del projecte es realitzarà en servidors virtuals dedicats a fi de no generar indisponibilitat als sistemes productius. Un cop validat el procés, el traslladarà a producció fora de l'horari laboral.

Departament/s implicat/s	Departament IT (Administradors BDD)
Planificació del projecte	Del 06/05/2021 al 27/05/2021
Recursos econòmic	7.260,00 €
Controls ISO afectats	12.5 Control del software en explotació
Resultats esperats	Bases de dades Oracle dels entorns productius migrades a la versió 12c.
Riscos que mitiga	Evitar que el software quedi fora de manteniment per part del proveïdor així com la absencia de les últimes modificacions (fix) a nivell de seguretat.
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB)
Factors crítics d'èxit	Migració segons les especificacions del fabricant (https://www.oracle.com/technetwork/es/articles/database-performance/upgrade-database-12c-parte-)

Projecte	**SGSI-6-2 Actualització patchs mòbils Apple**
Responsables	Responsable IT
Objectiu	Elaborar un procediment amb les instruccions necessàries per a que els usuaris de dispositius mòbils Apple puguin realitzar les actualitzacions de seguretat.

Descripció i accions necessaris per a la seva posada en marxa

Amb l'objectiu de mantenir el nivell de seguretat desitjat, s'elaborarà un procediment amb les instruccions necessàries per a l'actualització dels dispositius mòbils Appel. Aquest procediment es distribuirà entre tots aquells empleats de la companyia que siguin els responsables d'un dispositiu mòbil Appel.
El procediment haurà de ser d'obligat compliment.

Departament/s implicat/s	Departament IT
Planificació del projecte	Del 27/05/2021 al 12/07/2021
Recursos econòmic	15.790,50 €
Controls ISO afectats	6.2 Dispositius per a la mobilitat i el tele-treball 18.2 Revisions de la seguretat de la informació
Resultats esperats	Actualització de tots els dispositius mòbils Apple
Riscos que mitiga	«Bugs» de seguretat que posin en perill la informació sensible dels dispositius mòbils.
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB) SGSI-4-1 Programa de conscienciació sobre la seguretat
Factors crítics d'èxit	Aplicació del procediment per part dels usuaris

Projecte	**SGSI-7-2 Actualització patchs mòbils Android**
Responsables	Responsable IT
Objectiu	Elaborar un procediment amb les instruccions necessàries per a que els usuaris de dispositius mòbils Android puguin realitzar les actualitzacions de seguretat.
Descripció i accions necessaris per a la seva posada en marxa	
Amb l'objectiu de mantenir el nivell de seguretat desitjat, s'elaborarà un procediment amb les instruccions necessàries per a l'actualització dels dispositius mòbils Android. Aquest procediment es distribuirà entre tots aquells empleats de la companyia que siguin els responsables d'un dispositiu mòbil Android. El procediment haurà de ser d'obligat compliment.	
Departament/s implicat/s	Departament IT
Planificació del projecte	Del 12/07/2021 al 27/09/2021
Recursos econòmic	15.790,50 €
Controls ISO afectats	6.2 Dispositius per a la mobilitat i el tele-treball 18.2 Revisions de la seguretat de la informació
Resultats esperats	Actualització de tots els dispositius mòbils Android
Riscos que mitiga	«Bugs» de seguretat que posin en perill la informació sensible dels dispositius mòbils.
Relació amb altres projectes	SGSI-1-1 Inventari d'actius (CMDB) SGSI-4-1 Programa de conscienciació sobre la seguretat
Factors crítics d'èxit	Aplicació del procediment per part dels usuaris

Annexe XV – Projectes a llarg termini
El següent quadre mostra la planificació dels projectes proposats.

	Nombre	Duracion	Inicio	Terminado	Predecesores
17	**Projectes llarg termini**	**296 days**	**28/09/21 8:00**	**15/11/22 17:00**	**9**
18	SGSI-1-3 Reestructuració del departament TIC	122,5 days	28/09/21 8:00	17/03/22 13:00	
19	SGSI-2-3 Pla de continuïtat de negoci	86,75 days	17/03/22 13:00	18/07/22 10:00	18
20	SGSI-3-3 Externalització de serveis	86,75 days	18/07/22 10:00	15/11/22 17:00	19

A continuació es mostren les fitxes amb el detall de cada un dels projectes contemplats en aquest termini.

Projecte	**SGSI-1-3 Reestructuració del departament TIC**
Responsables	Direcció de Sistemes (CIO)
Objectiu	Reorganitzar el departament d'IT dotant-lo d'una estructura organitzativa més òptima
Descripció i accions necessaris per a la seva posada en marxa	
Atès les necessitats de l'organització és necessari reorganitzar el departament d'IT amb l'objectiu d'aportar valor a les diferents àrees de negoci. El departament d'IT disposarà de les següents àrees operatives: **Àrea de Comunicacions**; Encarregada de gestionar les xarxes internes, externes, les comunicacions tan de línia fixa, com línies mòbils, instal·lacions i contractes amb els proveïdors de comunicacions. **Àrea de gestió, planificació i estratègia de serveis**; depenent de la direcció de sistemes de la informació. **Àrea de control de riscos** que gestionarà els diferents riscos del departament, dictaminarà els nivells de seguretat del departament, controlarà els plans de contingència, back-up, recuperació i sortida dels proveïdors. Addicionalment s'encarregarà de realitzar les auditories internes. **Àrea de negoci i aplicacions corporatives**, qui farà de pont entre el personal tècnic i el personal de negoci. Conceptualitzarà els processos de negoci en les eines empresarials; ERP, BI, CRM, BPM, HCM i nòmina. **Àrea de Centre d'atenció a l'usuari o CAU**, qui recollirà les peticions e incidències dels usuaris i de la seva resolució si la incidència és de primer nivell. Serà la primera línia de suport del deparament de sistemes de informació. **Àrea de sistemes e infraestructures** que mantindrà els sistemes i infraestructures que donen servei als sistemes d'informació. **Àrea de desenvolupament i noves tecnologies** que desenvoluparà les noves aplicacions a mida per l'organització i anàlisi de les noves tecnologies que puguin aplicar-se a la companyia.	
Departament/s implicat/s	Departament IT
Planificació del projecte	Del 28/09/2021 al 17/03/2022
Recursos econòmic	59.290,00 €
Controls ISO afectats	N/A
Resultats esperats	Estructura òptima del departament d'IT
Riscos que mitiga	N/A
Relació amb altres projectes	SGSI-3-3 Externalització de serveis
Factors crítics d'èxit	Grau de satisfacció per part dels departaments interns

Projecte	**SGSI-2-3 Pla de continuïtat de negoci**
Responsables	Direcció de Sistemes (CIO) Seguretat Corporativa Responsable IT
Objectiu	Elaborar un document «viu» que permeti a l'organització recuperar-se davant esdeveniments que puguin detenir o reduir dramàticament els processos crítics de negoci
Descripció i accions necessaris per a la seva posada en marxa	
L'organització hauria de tenir un PCN (Pla de Continuïtat del Negoci) on es detalli l'estratègia a seguir per a mitigar i minimitzar l'impacte que tindria en el negoci un accident o desastre i continuar amb l'activitat normal davant aquest imprevist. A l'hora de dissenyar l'estratègia del PCN caldrà tenir en compte els següents aspectes: • Contactes clau i membres de l'equip • Serveis que poden veure's afectats pel desastres • Anàlisi de l'impacte sobre l'activitat normal de l'organització en cas de produir-se una crisi • Pla de Contingència i Recuperació de Desastres per a serveis específics del negoci • Utilitzar mètriques RTO i RPO • Garantir que les dades més importants estan protegides • Designar una ubicació per a les rasques de Failover i Recuperació de Desastres • Fer simulacres, comprovar que el back-up i les rèpliques funcionen.	
Departament/s implicat/s	N/A
Planificació del projecte	Del 17/03/2022 al 18/07/2022
Recursos econòmic	41.987,00 €
Controls ISO afectats	17.1 Continuïtat de la seguretat de la Informació 17.2 Redundàncies
Resultats esperats	Document amb les mesures que permetin mitigar i minimitzar l'impacte que tindria en el negoci un accident o desastre.
Riscos que mitiga	Deixar de donar servei com a resultat de qualsevol incident.
Relació amb altres projectes	N/A
Factors crítics d'èxit	Compliment segons l'estàndard ISO-22301

Projecte	**SGSI-3-3 Externalització de serveis**
Responsables	Direcció de Sistemes (CIO)
Objectiu	Externalitzar aquells serveis que no siguin propis de l'activitat de la companyia
Descripció i accions necessaris per a la seva posada en marxa	
Dintre del Pla Director de Seguretat es contempla l'externalització d'aquells servis que no siguin propis de l'activitat normal de la companyia. Per a dur a terme la tasca caldrà inventariar aquells serveis amb alt grau d'externalització i el proveïdor que donarà servei a l'organització; Possibles serveis a externalitzar serien: • Correu corporatiu • Emmagatzematge al nuvol • Manteniment equips incendi • Proveïdor d'equips portàtils • Proveïdor/s de dispositius mòbils • Web corporativa • Lloguer dels edificis/seus corporatives • Desenvolupament d'aplicacions internes • etc.	
Departament/s implicat/s	N/A
Planificació del projecte	Del 18/07/2022 al 15/11/2022
Recursos econòmic	31.520,50 €
Controls ISO afectats	15.1 Seguretat de la informació en les relacions amb subministradors 15.2 Gestió de les prestacions del servei per subministradors
Resultats esperats	Minimització dels costos d'estructura i infraestructura Optimització dels serveis
Riscos que mitiga	Reducció dels actius gestionats per la pròpia companyia. Reducció dels controls de seguretat atès que seràn els proveïdors qui s'encarregaran d'aquesta tasca.
Relació amb altres projectes	N/A
Factors crítics d'èxit	Definir i establir els KPIs (Key Perfomance Indicators) per a mesurar l'eficiència del servei Delimitar de forma clara i explícita els límits de cada procés

Annexe XVI – Informe d'auditoria

Informe d'auditoria

SCRIPTIX

Índex

Informe executiu

El servei d'auditoria de seguretat versus el referencial ISO/IEC 27002:2013 analitza la seguretat de la informació d'una organització, sigui del tipus que sigui, i sigui de la mida que sigui. L'anàlisi es realitza respecte als 14 dominis, 35 objectius de control i 114 controls.

El resultat de l'auditoria estableix, en tots els àmbits de protecció: físic, lògic, organitzatiu i legal, l'estat de seguretat d'una organització en un moment determinat del temps.

Aquest nivell de seguretat quantitatiu en base a una avaluació objectiva de l'estat de la seguretat permet a l'organització establir el full de ruta per assolir l'objectiu de seguretat alineat amb el seu enfocament estratègic, li permet comparar-se amb altres organitzacions del mateix sector o regió geogràfica o simplement establir el grau de millora contínua en la base de la implantació de salvaguardes o controls que es defineixen de forma gradual.

Identificació del beneficiari

A continuació es presenten les dades identificatives de l'organització.

NOM DE L'ORGANITZACIÓ	SCRIPTIX S.A.U.
DATA	Maig-2019
NÚMERO CONTRACTE	2019-0004-CAT-SGSI-01
UBICACIÓ DE L'AUDITORIA	Avda. Diagonal 561
	08029, Barcelona
PERSONES ENTREVISTADES	19

Abast

L'abast serà tots els controls aplicables en el document *Declaració d'Aplicabilitat del SGSI*.

Equip Auditor

La selecció de l'equip auditor s'ha seguit mitjançant la premissa de *màxima imparcialitat o objectivitat*.

Auditor: Juanjo Carrasco Puy

Dates d'execució de l'auditoria

Aquesta auditoria s'ha realitzat entre el 01 de desembre del 2022 i el 06 març 2023. Els diferents períodes i tasques realitzats són:

Inici	Durada (d)	Final	Tasques
01/12/2022	15	22/12/2022	Recull d'informació, així com l'estudi de la mateixa.
23/12/2022	20	20/01/2023	Realització d'entrevistes, visites i proves tècniques.
23/01/2023	30	06/03/2023	Anàlisi de la Informació i Elaboració d'Informes.

Normativa emprada

Aquesta Auditoria es realitza respecte als 14 dominis, 35 objectius de control i 114 controls de la ISO/IEC 27002:2013, i que ens permetrà conèixer de manera global l'estat actual de la Organització en relació a la Seguretat de la Informació.

Aquesta valoració la realitzarem segons la següent taula, basada en el Model de Maduresa de la Capacitat (CMM - *Capability Maturity Model*):

CMM	Efectivitat	Significat	Descripció
L0	0%	Inexistent	Manca completa de qualsevol procés recognoscible. No s'ha reconegut que existeix un problema a resoldre
L1	10%	Inicial / Ad hoc	Estat inicial on l'èxit de les activitats del procés es basa, la majoria de vegades, en l'esforç personal. Els processos són inexistents o localitzats en àrees concretes. No existeixen plantilles definides a nivell corporatiu
L2	50%	Reproduïble, però intuïtiu	Els processos similars es duen a terme de manera similar per persones amb la mateixa tasca. Es normalitzen les tasques en base a l'experiència al mètode. No hi ha comunicació o entrenament formal, les responsabilitats queden a càrrec de cada individu. Es depèn del grau de coneixement de cada persona
L3	90%	Procés definit	L'organització sencera participa en el procés Els processos estan implantats, documentats i comunicats mitjançant entrenament
L4	95%	Gestionat i mesurable	Poden seguir-se amb indicadors numèrics i estadístics l'evolució del procés. Es disposa de tecnologia per automatitzar el fluix de treball. Es disposa d'eines per a millorar la qualitat i la eficiència
L5	100%	Optimitzat	Els processos es troben sota millora constant. En base a criteris quantitatius es determinen les desviacions i s'optimitzen els processos

Informe detallat

A continuació s'analitza cada control, la feina realitzada, les observacions i les conclusions.

Àrea	5. Polítiques de la Seguretat de la Informació			Conclusió	Conforme
Control ISO/IEC 27002:2013: 5.1 Direcció de gestió de seguretat de la informació					
Dirigir i donar suport a la gestió de la seguretat de la informació d'acord amb els requeriments del negoci, les lleis i les regulacions.					
Treball realitzat					
Es revisa l'existència del document «Política de Seguretat»					
Observacions					
Es verifica l'existència d'una Política de Seguretat aprovada per la direcció. El document es troba publicat i comunicat a tots els empleats i col·laboradors externs de la companyia.					
Evidències					
Es detallen les evidències recollides: ***EV_001***: Document Política de Seguretat publicat el 16/03/2019					
Recomanacions					
N/A					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	8. Gestió d'actius			Conclusió	Conforme
Control ISO/IEC 27002:2013: 8.1 Responsabilitat sobre els actius					
L'objectiu és identificat els actius en l'organització i definir les responsabilitats per a una protecció adequada.					
Treball realitzat					
Es revisa que hi hagi un inventari dels actius que tracten o emmagatzemen informació corporativa.					
Observacions					
És revisa alguns actius al atzar de l'organització, es revisa que tingui definit un propietari.					
Evidències					
És detallen les evidencies recollides: ***EV_002***: Extracció d'actius a l'atzar de la CMDB					
Recomanacions					
N/A					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	8. Gestió d'actius			Conclusió	Conforme
Control ISO/IEC 27002:2013: 8.2 Classificació de la Informació					
L'objectiu és assegurar que s'aplica un nivell de protecció adequat a la informació.					
Treball realitzat					
Es revisa la classificació de la informació i s'estableixin mesures de seguretat per a la gestió de suports					
Observacions					
Es revisen els actius identificats amb dades confidencials, perfectament indicats a la CMDB. Es revisen els últims informes de compliment normatiu d'aquest actius i el seu nivell de protecció.					
Evidències					
És detallen les evidencies recollides: ***EV_002***: Extracció d'actius a l'atzar de la CMDB.					
Recomanacions					
N/A					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	8. Gestió d'actius			Conclusió	No Conforme
Control ISO/IEC 27002:2013: 8.3 Mitjans de manipulació					
L'objectiu és evitar la divulgació, modificació, retirada o destrucció dels actius no autoritzats emmagatzemats en suports D'emmagatzematge.					
Treball realitzat					
Es revisen els procediments operatius per a la protecció dels documents, mitjans informàtics (discos, cintes, etc.), dades d'entrada o sortida i documentació del sistema contra la divulgació, modificació, retirada o destrucció dels actius no autoritzats.					
Observacions					
Els procediments estan incomplets i no contempla la totalitat dels actius recollits en la CMDB.					
Evidències					
És detallen les evidencies recollides: ***EV_002***: Extracció d'actius a l'atzar de la CMDB. ***EV_003***: Gestió d'altes i baixes a la CMDB.					
Recomanacions					
Es recomana ampliar els actius recollits en els procediments operatius segons l'inventari dels actius recollits en la CMDB.					
Estat	Pendent	**Responsable**	Roberto Ramos	**Termini**	3 mesos

Àrea	9. Control d'accés			Conclusió	No Conforme
Control ISO/IEC 27002:2013: 9.1 Els requisits de negoci de control d'accés					
L'objectiu és controlar l'accés a la informació i les instal·lacions utilitzades per al seu processament.					
Treball realitzat					
És revisa el procediment d'accessos de visites i d'externs, el registre d'entrada i sortida i el mètode per accedir.					
Observacions					
En els diferents edificis es detecta que pot accedir-se per diferents zones sense identificació. Per accedir als edificis on es troba el CPD si que es obligatori accedir per un torn. Addicionalment es pot passar la mateixa targeta identificadora múltiples vegades.					
Evidències					
És detallen les evidencies recollides: ***EV_004***: Procediment d'accés de visites/personal extern ***EV_005***: Registre d'entrada i sortida.					
Recomanacions					
Definir un accés on sigui obligatori la presentació de la targeta identificadora.					
Estat	Pendent	**Responsable**	Sergio Corbacho	**Termini**	3 mesos

Àrea	9. Control d'accés			Conclusió	Conforme
Control ISO/IEC 27002:2013: 9.2 Gestió d'accés dels usuaris					
L'objectiu és garantitzar l'accés als usuaris autoritzats i impedir l'accés als no autoritzats als sistemes de informació i serveis.					
Treball realitzat					
S'observa la gestió d'altes i baixes dels usuaris dels sistemes a traves dels aplicatius IDM i AD.					
Observacions					
És verifica els control d'accessos als sistemes, i els controls de verificació realitzats a través del SIEM.					
Evidències					
Es detallen les evidencies recollides: ***EV_006***: Procediment d'accés lògic ***EV_007***: Gestió d'altes i baixes					
Recomanacions					
N/A					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	9. Control d'accés			Conclusió	Conforme
Control ISO/IEC 27002:2013: 9.3 Responsabilitat dels usuaris					
L'objectiu és fer que els usuaris siguin responsables de la protecció de la informació per a la seva identificació.					
Treball realitzat					
Es revisa la política de llocs de treball. Així mateix s'examinen els llocs de treball a l'atzar per a validar si es compleix amb l'establert a la política de llocs de treball.					
Observacions					
S'observa la gestió d'usuaris privilegiats i altres de servei. Existeix una política aprovada i distribuïda a tots els empleats de la companyia on s'indica la necessitat imperativa de mantenir els llocs de treball i monitors lliures de qualsevol informació amb l'objectiu de reduir qualsevol accés no autoritzat.					
Evidències					
Es detallen les evidencies recollides: ***EV_006***: Procediment d'accés lògic ***EV_007***: Política de llocs de treball					
Recomanacions					
N/A					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	9. Control d'accés	Conclusió	Conforme
Control ISO/IEC 27002:2013: 9.4 Control d'accés a sistemes i aplicacions			
L'objectiu és impedir l'accés no autoritzat a la informació mantinguda pels sistemes i aplicacions.			
Treball realitzat			
Es revisen els diferents events generats al SIEM per aquest tipus de control. Es revisa el registre de consultes realitzada a diferents usuaris amb privilegis en el PMP.			
Observacions			
Es verifica els control d'accessos als sistemes, i els controls de verificació realitzats a través del SIEM. També es verifica que l'ús d'usuaris privilegiats queda registrat qui consulta aquesta informació en el PMP.			
Evidències			
Es detallen les evidencies recollides: ***EV_008***: Gestió d'alertes SIEM ***EV_009***: Gestió d'usuaris PMP			
Recomanacions			
N/A			
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	11. La seguretat física i ambiental	Conclusió	Conforme
Control ISO/IEC 27002:2013: 11.1 Les àrees segures			
L'objectiu és evitar l'accés físic no autoritzat, els danys i interferències a la informació de l'organització i les instal·lacions de processament d'informació.			
Treball realitzat			
Es revisen les mesures de seguretat existents en l'accés físic a les instal·lacions i en especial a les zones més crítiques com el Centre de Procés de Dades (CPD) i l'arxiu.			
Observacions			
Es verificar que el CPD disposa de mesures que garanteixin la integritat física dels sistemes d'informació (climatització, detecció i extinció d'incendis, subministrament elèctric de suport, etc).			
Evidències			
Es detallen les evidencies recollides: ***EV_010:*** Projecte SGSI-3-2 Millora dels Centre de Processament de Dades			
Recomanacions			
N/A			
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	11. La seguretat física i ambiental			Conclusió	No Conforme
Control ISO/IEC 27002:2013: 11.2 Seguretat dels equips					
L'objectiu és evitar la pèrdua, danys, robatori o el compromís d'actius i la interrupció a les operacions de la organització.					
Treball realitzat					
Revisió de la seguretat física dels llocs de treball i les mesures de seguretat física dels equips					
Observacions					
No es disposa de cadenat per assegurar l'equip i evitar el robatori.					
Evidències					
Es detallen les evidencies recollides: ***EV_011***: Anàlisi de riscos					
Recomanacions					
Tots els equips portàtils haurien de disposar de cadenat per a poder assegurar l'equip tant dintre de la companyia com fora d'ella i evitar així el robatori de l'equip.					
Estat	Pendent	**Responsable**	Ana Claramunt	**Termini**	2 mesos

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.1 Procediments i responsabilitats operacionals					
L'objectiu és assegurar la operació correcta i segura dels mitjans de processament de la informació mitjançant el desenvolupament dels procediments d'operació apropiats.					
Treball realitzat					
Es realitza l'entrevista amb el responsable de Seguretat IT. S'identifiquen els responsables de cada servei.					
Observacions					
S'observa a la política els rols de cadascú definits i les seves responsabilitats.					
Evidències					
Es detallen les evidencies recollides: ***EV_012***: Política de seguretat, rols i responsabilitats					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.2 Protecció contra el malware					
L'objectiu és garantir que la informació i les instal·lacions de processament de informació estiguin protegides contra malware.					
Treball realitzat					
Entrevista amb els administradors i responsable del ATD en seguretat. Es revisen els procediments i una activitat pràctica del funcionament del ATD.					
Observacions					
S'observa que tot el phising es filtrat per l'antivirus, a més a més el ATD compta amb una amplia BBDD de coneixement pels casos que l'antivirus no actiu.					
Evidències					
Es detallen les evidencies recollides: ***EV_013***: Gestió del antivirus i les regles en SCRIPTIX ***EV_014***: Procediment del ATD.					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.3 Còpia de seguretat					
L'objectiu és assolir un grau de protecció desitjat contra la pèrdua de dades.					
Treball realitzat					
Es realitza entrevista amb el responsable de IT on es detalla cada acció del procediment de còpia de seguretat. Es tria varies mostres a examinar l'estat de l'últim backup realitzat.					
Observacions					
Es verifica que coincideix amb els backups que s'han de realitzar.					
Evidències					
Es detallen les evidencies recollides: ***EV_015***: Procediment de gestió de backups					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.4 Registre i supervisió					
L'objectiu és enregistrar els events relacions amb la seguretat de la informació i generar les evidències.					
Treball realitzat					
Es revisen els procediments a seguir en quant a la detecció d'alertes, es revisen els KPI (Key Perfomance Indicator) reportats mensualment d'aquestes alertes i s'extrau un excel amb les alertes registrades en l'eina de monitorització.					
Observacions					
S'observa que cada alerta generada està automatitzada amb l'eina de monitoring, d'aquesta manera es registra tots els esdeveniments.					
Evidències					
Es detallen les evidencies recollides: ***EV_016***: Gestió d'alertes IPS ***EV_017***: Gestió d'alertes de monitorització ***EV_018***: KPI de seguretat					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.5 Control de programari operacional					
L'objectiu és garantir la integritat dels sistemes operacions per a l'organització.					
Treball realitzat					
S'entrevista els desenvolupadors i als administradors. Es disposa de programari per al controls de versió del software així com programari per a la implantació de software en entorns productius.					
Observacions					
Un cop es desplega el nou software s'ha de validar per l'equip de seguretat, aquests realitzen un control de la versió de software i de programari maliciós.					
Evidències					
Es detallen les evidencies recollides: ***EV_019***: Procediment de gestió de vulnerabilitats. ***EV_020***: Sol·licitud d'instal·lació de software.					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.6 Gestió tècnica de la vulnerabilitat					
L'objectiu és evitar la explotació de vulnerabilitats tècniques.					
Treball realitzat					
S'entrevista la persona responsable del procés i el responsable de riscos. Es revisa el fluxe del procediment i la generació de scans de vulnerabilitats					
Observacions					
S'observa que per cada scan de vulnerabilitats es genera un change en l'eina de ticketing, per a la correcció de vulnerabilitats es generen change i es reporten a l'eina de gestió de scans i vulnerabilitats Qualys, es realitza un extracte de les remediacions.					
Evidències					
Es detallen les evidencies recollides: ***EV_019***: Procediment de gestió de vulnerabilitats. ***EV_021***: Procés de remediació de vulnerabilitats.					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	12. Seguretat en la Operativa			Conclusió	Conforme
Control ISO/IEC 27002:2013: 12.7 Sistemes d'informació consideracions d'auditoria					
L'objectiu és minimitzar l'impacte de les activitats d'auditoria en els sistemes operacionals.					
Treball realitzat					
S'entrevista el responsable del procés i els controls a revisar els KPI mensuals i l'extracció d'auditories de SANS					
Observacions					
Tot es gestiona a través del Qualys, on es pot analitzar totes les auditories realitzades y els seus resultats.					
Evidències					
Es detallen les evidencies recollides: ***EV_022:*** Procediment de Policy Compliance. ***EV_023***: Diferents guies de hardening.					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	13. Seguretat en les comunicacions			Conclusió	Conforme
Control ISO/IEC 27002:2013: 13.1 de gestió de seguretat de xarxa					
L'objectiu és evitar l'accés físic no autoritzat, els danys i interferències a la informació de l'organització o les instal·lacions de processament d'informació.					
Treball realitzat					
S'entrevista el responsable de l'àrea, és revisen els procediments i els contractes externs.					
Observacions					
Es verifica tant l'existència de mecanismes per garantir la seva seguretat (sistemes tallafocs, sistemes IPS), com la seva correcta implantació i configuració.					
Evidències					
Es detallen les evidencies recollides: ***EV_024:*** Contractes de diferents proveïdors de serveis en xarxa. ***EV_025***: Procediment de gestió de xarxes.					
Recomanacions					
Estat	N/A	**Responsable**	N/A	**Termini**	N/A

Àrea	13. Seguretat en les comunicacions			Conclusió	No Conforme
Control ISO/IEC 27002:2013: 13.2 Intercanvi d'informació amb parts externes					
L'objectiu és mantenir la seguretat de la informació que es transfereix una organització internament o amb entitats externes.					
Treball realitzat					
Es detalla la feina realitzada en aquesta àrea concreta.					
Observacions					
No es realitza una revisió adequada dels logs, i tampoc estan configurats tots els equips de xarxa per reportar esdeveniments que permetin detectar accions que puguin afectar la seguretat de la informació. Els contractes amb els proveïdors de serveis en xarxa enuncien les mesures de seguretat aplicables però no es concreten aquestes mesures i tampoc hi ha clàusules específiques sobre els mecanismes de supervisió i auditoria d'aquestes mesures.					
Evidències					
Es detallen les evidencies recollides: ***EV_024:*** Contractes de diferents proveïdors de serveis en xarxa.					
Recomanacions					
Establir procediments de generació i revisió de logs per a tots els equips de xarxa, de manera que permetin detectar errors o activitats maliciosa					
Estat	Pendent	**Responsable**	Xavier Valls	**Termini**	3 mesos

Àrea	14. Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 14.1 Requeriments de seguretat dels sistemes d'informació

L'objectiu és garantir que la seguretat de la informació sigui una part integral dels sistemes d'informació en tot el cicle de vida, incloent els requeriments per aquells que proporcionen serveis en xarxes públiques.

Treball realitzat

S'entrevista als responsables del WAF, els procediments i les remediacions que duen a terme.

Observacions

Tots els sistemes i les URL publiques es troben darrera del WAF (web application firewall), tota la seguretat es gestiona a través de ells.

Evidències

Es detallen les evidencies recollides:
EV_024: Contractes de diferents proveïdors de serveis en xarxa.
EV_022: Procediment de Policy Compliance.
EV_023: Diferents guies de hardening.
EV_026: Procediment de gestió del WAF

Recomanacions

Estat		Responsable	N/A	Termini	N/A

Àrea	14. Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 14.2 Seguretat en els processos de desenvolupament i suport

L'objectiu és garantir que la seguretat de la informació es dissenyi i implementi dintre del cicle de vida de desenvolupament dels sistemes d'informació.

Treball realitzat

S'entrevista l'analista en seguretat qui representa totes les reunions de nous desenvolupaments, on s'han de verificar amb les eines de seguretat.

Observacions

S'observa els fluxe de nous projectes la implicació i la verificació per part de seguretat, a cada tasca realitzada hi ha adjunt els informes d'aprovació des de Seguretat.

Evidències

Es detallen les evidencies recollides:
EV_024: Contractes de diferents proveïdors de serveis en xarxa.
EV_022: Procediment de Policy Compliance.
EV_023: Diferents guies de hardening.
EV_026: Procediment de gestió del WAF

Recomanacions

Estat		Responsable	N/A	Termini	N/A

Àrea	14. Sistema d'adquisició, desenvolupament i manteniment	Conclusió	Conforme

Control ISO/IEC 27002:2013: 14.3 Dades de prova

L'objectiu és garantir la protecció de les dades que s'utilitzen per a processos de proves.

Treball realitzat

S'entrevista l'analista de riscos, tots aquells entorns no productius s'emmascaren les dades, SCRIPTIX disposa de l'eina adequada i desplegada als altres departaments.

Observacions

S'analitzen alguns entorns de pre-producció i desenvolupament on s'emmascaren les dades.

Evidències

Es detallen les evidencies recollides:
EV_024: Contractes de diferents proveïdors de serveis en xarxa.
EV_022: Procediment de Policy Compliance.
EV_023: Diferents guies de hardening.
EV_026: Procediment de gestió del WAF

Recomanacions

Estat		Responsable	N/A	Termini	N/A

Resultats de l'auditoria

En l'auditoria s'ha realitzat una sèrie d'entrevistes, visites i proves per avaluar el grau de maduresa de les mesures de seguretat implantades pel que fa als diferents dominis i objectius de control de la Norma ISO/IEC 27002: 2013.

El grau de maduresa en què es troben els diferents dominis ha passat d'una mitjana de «L2 i L3» a una mitjana actual de «L4 i L5» segons els nivells de maduresa utilitzats.

L'evolució d'aquesta maduresa podem veure reflectida en la següent taula:

Norma	Dominis	CMM 2019	Efectivitat	CMM 2022	Efectivitat
5	Polítiques de Seguretat	L3	90%	L5	100%
8	Gestió d'actius	L2	50%	L3	90%
9	Control d'accés	L2	50%	L4	95%
11	Seguretat física i ambiental	L2	50%	L2	50%
12	Seguretat en la operativa	L3	90%	L5	100%
13	Seguretat en les telecomunicacions	L2	50%	L2	50%
14	Adquisició, desenvolupament o manteniment dels sistemes d'informació	L2	50%	L5	100%
	Compliment General		61%		84%

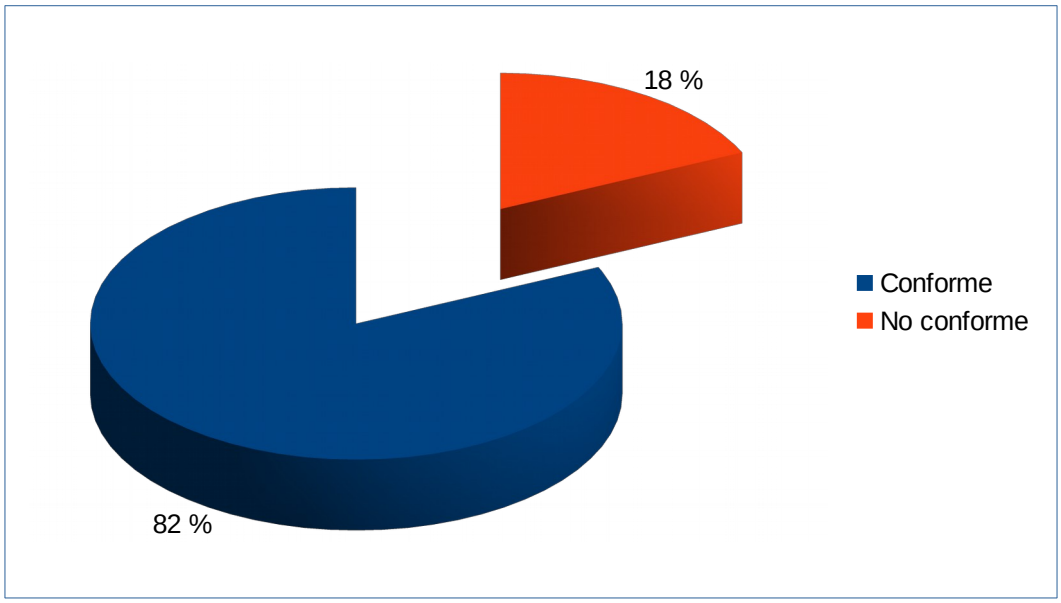
Com a resultat de l'anàlisi de cada un dels controls de la ISO/IEC 27002:2013 de referència s'han trobat un total de 4 «No Conformitats» que hauran de ser corregides.

Aquestes «No Conformitats» es troben en els següents controls de la norma:

- 8.3 Mitjans de manipulació
- 9.1 Els requisits de negoci de control d'accés
- 11.2 Seguretat dels equips
- 13.2 Intercanvi d'informació amb parts externes

A continuació es mostra el detall de les conformitats/no conformitats dels controls així com la gràfica representativa que mostra la distribució en % de la conformitat i no conformitat.

Norma	Dominis		Conforme	No conforme
5	Polítiques de la Seguretat de la Informació	5. Polítiques de la Seguretat de la Informació	1	0
8	Gestió d'actius	8. Gestió d'actius	2	1
9	Control d'accés	9. Control d'accés	3	1
11	La seguretat física i ambiental	11. La seguretat física i ambiental	1	1
12	Seguretat en la Operativa	12. Seguretat en la Operativa	7	0
13	Seguretat en les comunicacions	13. Seguretat en les comunicacions	1	1
14	Sistema d'adquisició, desenvolupament i manteniment	14. Sistema d'adquisició, desenvolupament i manteniment	3	0
TOTAL			18	4
			81,82 %	18,18 %



Bibliografia

Material MISTIC (Màster Interuniversitari en Seguretat de les Tecnologies de la Informació i les Comunicacions)
Les referències bibliogràfiques utilitzades en la memòria són referents als mòduls estudiats durant l'assignatura Sistemes de Gestió de la Seguretat:

- Mòdul 1 - Introducció a la seguretat de la informació
- Mòdul 2 - Anàlisi de riscos
- Mòdul 3 - Implantació d'un sistema de gestió de la seguretat de la informació (SGSI)
- Mòdul 4 - Desenvolupament d'alguns objectius de control de l'SGSI
- Mòdul 5 - Plans de continuïtat de negoci

Addicionalment s'ha consultat els següents mòduls de l'assignatura Auditoria Tècnica:

- Mòdul 2 - Auditoria de certificació ISO 27001
- Mòdul 3 - Auditoria tècnica de seguretat de sistemes d'informació i comunicacions

ISO/IEC 27000

- Wikipedia: https://es.wikipedia.org/wiki/ISO/IEC_27001
- El portal de ISO 27002 en Español: http://www.iso27000.es/iso27002.html

Basilea III

http://www.caixabankresearch.com/documents/10180/51459/de24_esp.pdf

PCI-DSS:

https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

https://es.wikipedia.org/wiki/PCI_DSS

GDPR

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

PSD2

https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_es

MAGERIT

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Sistema de traces

https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf

Programa de concienciació sobre la seguretat

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

NVD (NATIONAL VULNERABILITY DATABASE)

https://nvd.nist.gov/vuln/search?form_type=Basic&results_type=overview&query=iphone+os&search_type=all

Glossari de Termes

Terme	Definició
SGSI	Sistemes de Gestió de la Seguretat de la Informació
PDCA	(Del l'anglès Plan-Do-Check-Act, això és, planificar-fer-verificar-actuar) o espiral de millora continua, és una estratègia de millora continua de la qualitat en quatre fases, basat en el concepte idea per Walter A. Shewhart.
PCI-DSS	És l'estàndard de seguretat de dades per a l'industria de targetes de pagament (en anglès Payment Card Industry Data Security Standard).
GDPR	Reglament General de Protecció de Dades, és el reglament europeu relatiu a la protecció de persones físiques en el que respecta al tractament de les seves dades personals i a la lliure circulació d'aquestes dardes.
Actiu	Component o funcionalitat d'un sistema d'informació susceptible de ser atacat deliberada o accidentalment amb conseqüències per a l'organització. Inclou: informació, dades, serveis, aplicacions (software), equips (hardware), comunicacions, recursos administratius, recursos físics i recursos humans.
PSD2	De l'anglès Payment Services Directive, és la continuació de la primera directiva europea en mitjans de pagament (PSD, per les seves sigles en anglès), vident des del 2007, i que va entrar en vigor en Espanya en 2009.
CHD	*Relatiu a PCI-DSS* Cardholder data; les dades del titular de targetes i que inclouen el PAN (Primary Account Number o número principal de compte), el nom del titular, data d'expiració i codi de servei.
ATD	Advanced Threat Detection (Detecció avançada d'amenaces) és un tipus de seguretat que va més enllà de l'anàlisi de seguretat bàsica. Està integrat en «dispositius» i altres solucions que funcionen en un nivell més profund per a corregir les vulnerabilitats de seguretat i prevenir les amenaces informàtiques.
SAD	*Relatiu a PCI-DSS* Sensitive Account Data; les dades d'autenticació sensibles que inclouen el registre total de dades (banda magnètica, o recentment, en xip), el codi de seguretat de la targeta (CAV2/CVC2/CVV2/CID) i els números d'identificació personal (PIN) utilitzats per a completar la transacció.
CISO	Director de la Seguretat de la Informació (en anglès Chief Information Security Officer)
Anàlisis de Riscos	També conegut com PHA (en anglès Process Hazards Analysis) és l'estudi de les causes de les possibles amenaces i probables esdeveniments no desitjats i els danys i conseqüències que aquestes puguin produir.

Incident de Seguretat	Es defineix com un accés, intent d'accés, ús, divulgació, modificació o destrucció no autoritzada d'informació, un impediment en l'operació normal de les xarxes, sistemes o recursos informàtics, o una violació de la política de seguretat.
Tolerància al risc	El nivell de risc que una entitat està disposat a assumir per tal d'aconseguir un resultat potencial desitjat
Amenaça	És tota acció que aprofita una vulnerabilitat per atemptar contra la seguretat d'un sistema de informació.
CSI	Comitè de Seguretat de la Informació
RSI	Responsable de seguretat de la informació
CPD	Centres de processament de dades
VPN	Xarxa Privada Virtual (en anglès Virtual Private Network), és una tecnologia de xarxa de computadores que permet l'extensió d'una xarxa d'àrea local (LAN; Local Area Network).
FTP	El protocol de transferència d'arxius (en anglès File Transfer Protocol o FTP) és un protocol de xarxa per a la transferència d'arxius entre sistemes connectats a una xarxa TCO (Transmission Control Protocol), basat en arquitectura client-servidor.
IDS	Un sistema de detecció d'intrusions (o IDS de les seves sigles en anglès Intrusion Detection System), és un programa de detecció d'accessos no autoritzats a un computador o a una xarxa.
P2P	Peer-to-Peer és una xarxa d'ordinadors interconnectats com a nodes que es comporten com a iguals entre sí; és a dir, actuen simultàniament com a client i servidor respecte la resta de nodes i permet l'intercanvi directe d'informació (p.e eMule),
NVD	El NVD és el repositori del govern dels Estats Units de dades de gestió de vulnerabilitats basades en estàndards representades mitjançant el protocol de seguretat d'automatització de contingut (SCAP)
TIC	Tecnologia de la Informació i les Comunicacions
ISO	International Organization for Standardization
IEC	La Comisión Electrotécnica Internacional (CEI), més coneguda per les seves sigles en anglès: IEC (International Electrotechnical Commission), és una organització de normalització en els camps elèctric, electrònic i tecnologies relacionades.
CMDB	Base de Dades de la Gestió de Configuració.
CMM	Model de Maduresa de la Capacitat.