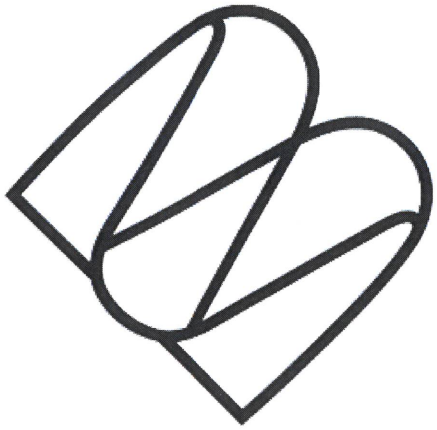
mercabarna

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ



mercabarna

Tipus de document		Política	
Versió	**Estat**	**Autor**	**Data**
V.2.2(rev.JUR)	Vigent	Tecnologies de la Informació	

ÚS INTERN

Índex de Contingut

1. OBJECTE I AMBIT D'APLICACIÓ

És objecte del present document establir les directrius que regeixen la forma en què Mercabarna gestiona i protegeix la informació que tracta i els serveis que presta a través dels seus Sistemes de la informació (definició de l'article 12.1 RD 311/2022 ENS). Així mateix, també és objecte d'aquest document la determinació del conjunt de mesures relacionades amb l'organització global de la seguretat de la informació per als sistemes d'informació de l'Àrea de Tecnologies de la Informació de Mercabarna.

2. DOCUMENTACIÓ

2.1. ESTÀNDARDS I REGULACIONS EXTERNES

- UNE-ISO/IEC 27001 de Seguretat de la Informació.

2.2. PRINCIPAL LEGISLACIÓ

- Normativa vigent en matèria de l'Esquema Nacional de Seguretat.
- Normativa nacional, comunitària i internacional vigent en matèria de seguretat de les xarxes i sistemes d'informació.

2.3. DOCUMENTACIÓ DE REFERÈNCIA

- Polítiques de seguretat
- Normes de seguretat
- Normativa de Seguretat
- Document LOPD dels treballadors

3. TERMES I DEFINICIONS

- N/A

4. DESCRIPCIÓ

4.1. OBJECTIUS DE L'ORGANITZACIÓ [ORG. 1.1]

La Direcció de Mercabarna, conscient de la criticitat del seu servei, la importància d'aquest per al ciutadà i el compromís que contreu amb la seguretat del mateix ha establert en la seva

organització una sèrie de polítiques i procediments operatius per a la Gestió de la Seguretat de la Informació sobre la base de les premisses establertes pel Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat (ENS), atenent els següents objectius:

- Assegurar que els serveis prestats i productes subministrats per l'Àrea de Tecnologies de la Informació són segurs, fiables, compleixen amb les normes i instruccions aplicables, s'adapten als requisits i expectatives dels seus clients i milloren contínuament.
- Mantenir al dia la legislació aplicable i complir tots els requisits legals i normatius establerts en matèria de seguretat de la informació.
- Aconseguir i mantenir el nivell de seguretat requerit per garantir de forma adequada la continuïtat del negoci, fins i tot en situacions adverses.
- Incrementar la integració i el suport mutu dels aspectes físics i lògics de la seguretat.
- Assegurar la disponibilitat, confidencialitat, integritat, traçabilitat i autenticitat de la informació.
- Establir l'estructura corporativa de seguretat definida pels òrgans de decisió de l'organització i crear els canals de comunicació adequats entre tots els implicats.
- Protegir les persones que treballen a Mercabarna, la confidencialitat i disponibilitat de les seves comunicacions i la integritat de la seva informació, d'acord amb la normativa de protecció de dades.
- Implicar, motivar i comprometre el personal propi i aquell que treballi en nom de Mercabarna, per tal de cercar la seva participació en la gestió, desenvolupament i aplicació de les polítiques de seguretat de la informació implantades.
- Establir i implantar plans de formació i divulgació en seguretat per a la millora contínua de la formació del personal.

4.2. MARC LEGAL I REGULATORI [ORG. 1.2]

Aquesta política de seguretat de la informació s'estableix i serà desenvolupada aplicant els següents requisits:

- Normativa de seguretat
- Document LOPD dels treballadors

Tot això, procurant donar resposta, entre d'altres, a les següents normes i regulació:

- UNE-ISO/IEC 27001 de la Seguretat de la Informació.
- Normativa estatal/nacional, comunitària i internacional vigent aplicable sobre la seguretat de les xarxes i sistemes d'informació.
- Normativa estatal/nacional, comunitària i internacional vigent aplicable sobre la identificació i les transaccions electròniques.

- Normativa estatal/nacional, comunitària i internacional vigent aplicable al tractament de dades personals i a la lliure circulació d'aquestes dades.
- Normativa estatal/nacional, comunitària i internacional vigent aplicable a la protecció de dades personals i garantia de drets digitals.
- Normativa estatal/nacional, comunitària i internacional vigent aplicable sobre els serveis de la societat de la informació i el comerç electrònic
- Normativa estatal/nacional, comunitària i internacional vigent aplicable sobre els contractes del sector públic
- Normativa relativa a l'Esquema Nacional de Seguretat en vigor.

4.3. ROLS I FUNCIONS DE SEGURETAT [1.3]

En matèria de seguretat de la informació es diferencien els rols i funcions següents:

- El **responsable de la informació,** a saber, la **Direcció General** de Mercabarna, serà el propietari d'aquesta i tindrà les següents funcions;
    - Classificar la informació conforme als criteris i categories establertes en l'ENS i en cadascuna de les dimensions de seguretat conegudes i aplicables (disponibilitat, autenticitat, traçabilitat, confidencialitat i integritat), dins del marc establert en l'ENS.
    - Donar suport a la realització dels anàlisis de riscos i valorar les diferents opcions de gestió del risc que cal implantar.
    - Valorar i decidir, juntament amb els responsables dels Serveis, els riscos residuals calculats en l'anàlisi de riscos, i de fer-ne el seguiment i control, sense perjudici de la possibilitat de delegar aquesta tasca.
    - Vetllar per la inclusió de clàusules sobre seguretat en els contractes amb terceres parts que puguin tenir accés a informació dels procediments administratius que gestiona i fer el seguiment del seu compliment.

- El **responsable del servei,** a saber, qui ostenti la **Direcció d'Àrea** en qüestió, serà qui determini els requisits dels serveis prestats, en consonància, tindrà les següents funcions:
    - Establir els requisits del servei en matèria de seguretat, o, en terminologia de l'ENS, la potestat de determinar els nivells de seguretat dels serveis.
    - Classificar els serveis conforme als criteris i categories establertes en l'ENS i en cadascuna de les dimensions de seguretat conegudes i aplicables (disponibilitat, autenticitat, traçabilitat, confidencialitat i integritat), dins del marc establert en l'ENS.

- Atendre els requisits de seguretat de la informació, com ara disponibilitat, accessibilitat, interoperabilitat, etc. que es demandin en la prestació dels serveis.
- Vetllar per la inclusió de clàusules sobre seguretat en els contractes amb terceres parts que puguin afectar els seus serveis i fer el seguiment del seu compliment.

- El **responsable de seguretat** serà qui prengui les decisions adequades per satisfer els requisits de seguretat de la informació i dels serveis. Disposarà de les funcions següents:
  - Supervisar el compliment de la present Política, de les seves normes i procediments derivats.
  - Coordinar la interacció amb altres organismes especialitzats.
  - Prendre coneixement i supervisar la investigació i monitoratge dels incidents de seguretat.
  - Establir les mesures de seguretat, adequades i eficaces per complir els requisits de seguretat establerts pels Responsables dels Serveis i de la Informació, seguint en tot moment l'exigit a l'ENS.
  - Assessorar, en col·laboració amb els Responsables dels Sistemes, els Responsables dels Serveis i de la Informació, en la realització de l'anàlisi i gestió de riscos
  - Monitoritzar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria implementats en el sistema.
  - Promoure les activitats de conscienciació i formació en matèria de seguretat en el seu àmbit de responsabilitat.
  - Realitzar o promoure les auditories periòdiques que permetin verificar el compliment de les obligacions en matèria de seguretat.
  - Elaboració i revisió de la normativa de seguretat.
  - Aprovació dels procediments de seguretat elaborats pel Responsable del Sistema.

Tot i que a l'Àrea de Tecnologies de la Informació de Mercabarna no hi ha un departament de seguretat com a tal, ni tampoc la figura diferenciada de Responsable de Seguretat, les seves funcions són assimilades pel **Cap del Departament d'Informàtica**.

- El **responsable dels sistemes d'informació**, a saber, el **Cap del Departament d'Informàtica**, dins de les seves àrees d'actuació, tindrà assignades les següents funcions:
    - Desenvolupament, operació i manteniment del sistema d'Informació durant tot el seu cicle de vida, de les seves especificacions, instal·lació i verificació del seu correcte funcionament.
    - Garantir que les mesures de seguretat s'integrin adequadament dins del marc general de la Seguretat de la Informació.
    - Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
    - Elaborar procediments tècnics de seguretat dels sistemes d'informació.
    - Elaborar plans de continuïtat dels sistemes d'informació.
    - Col·laborar per a la realització de l'anàlisi de riscos dels sistemes d'informació dels quals és responsable.
    - Implementar, gestionar i mantenir les mesures de seguretat aplicables al sistema d'informació.
    - Gestionar, configurar i actualitzar, si s'escau, el hardware y software en els quals es basen els mecanismes i serveis de seguretat del sistema d'informació.

La responsabilitat general de la seguretat de la informació recaurà sobre el responsable de Seguretat, essent la responsabilitat última de la Direcció com a màxima responsable de la seguretat de Mercabarna.

En cas de conflicte entre els diferents responsables, aquest serà resolt pel superior jeràrquic dels mateixos. En defecte de l'anterior, prevaldrà la decisió del Responsable de Seguretat.

La Direcció assumeix la responsabilitat final i última del compliment de la política. De la mateixa manera, la Direcció analitzarà els riscos i vulnerabilitats en matèria de seguretat que puguin afectar el bon funcionament del negoci i proposarà les normes, mitjans i mesures procedents per suprimir-los i en el seu defecte minimitzar-los.

La Direcció procedirà a la revisió periòdica de la present política i la seva modificació si fos necessari. És responsabilitat de tota l'organització de Mercabarna, l obligat compliment del que estableixen les polítiques de seguretat de la Informació, i fonamentalment de les persones encarregades de la realització de les activitats compreses dins dels sistemes esmentats, assumint les responsabilitats en matèria de seguretat i sobre els actius d'informació al seu càrrec.

4.4. ESTRUCTURA DEL COMITÈ PER A LA GESTIÓ I COORDINACIÓ DE LA SEGURETAT [1.4]

El detall de la composició del Comitè per a la gestió de la Seguretat integral de Mercabarna, així com les obligacions de cada rol en l'àmbit de la seguretat de la informació es determinen en les actes relatives al Comitè de Direcció, el qual assimila les funcions d'aquell.

4.5. DIRECTRIUS PER A L'ESTRUCTURACIÓ DE LA DOCUMENTACIÓ DE SEGURETAT, LA SEVA GESTIÓ I ACCÉS [1.5]

4.5.1. CATEGORITZACIÓ DE LA DOCUMENTACIÓ

A Mercabarna, els documents que descriuen els processos de treball i mètodes d'actuació de l'organització podrien ser classificats dins d'alguna de les categories que es descriuen a continuació:

Documents principals:

- **Polítiques (POL):** Són documents d'alt nivell que representen la filosofia global de l'organització, l'orientació estratègica de la Direcció i dels responsables de les diferents Àrees o Departaments.
- **Procediments (PR)/Fitxes de procés (FP):** Descriuen els processos que s'han de seguir per realitzar una activitat específica de gestió o implementar un control de seguretat.
- **Instruccions tècniques (IT):** Són procediments específics concrets que descriuen la forma correcta de realitzar o executar una tasca específica, o part d'una tasca que forma part d'un procés més gran. Generalment amplien la informació d'un procediment més genèric o expliquen de manera tècnica els passos per a l'execució d'una tasca en concret, servint de guia per a la mateixa, pertanyen a aquesta categoria, entre d'altres, les guies d'utilització de tecnologies i eines, i els manuals d'instal·lació.
- **Plantilles (PL):** Són els documents que s'ha identificat als procediments/fitxes de procés que s'han d'utilitzar per tal de poder executar els processos.

Documents complementaris:

- **Registres (REG), Documents auxiliars (D.A) i/o annexos (ANX):** Són tots aquells documents utilitzats per evidenciar el correcte funcionament de la seguretat i el compliment d'alguns dels mecanismes de seguiment de la seguretat o l'operativa diària implementats.

4.5.2. TRACTAMENT DE LA DOCUMENTACIÓ

4.5.2.1. Responsabilitat de la informació documentada

La responsabilitat de la informació recaurà sobre el responsable del departament al qual incumbeixi, a excepció d'aquella informació que sigui de caràcter personal, cas en el qual aquesta responsabilitat pertanyerà al Responsable del fitxer en qüestió.

Aquest responsable tindrà la competència exclusiva de determinar el nivell de seguretat de la informació, així com de modificar-lo.

4.5.2.2. Identificació de la documentació i control de versions

Les polítiques i procediments s'haurien de nomenar amb un identificador únic i inequívoc que permeti diferenciar el seu contingut mitjançant el mateix, utilitzant un nom que ofereixi una breu descripció del document i defineixi el seu contingut. A més, cada document s'hauria de versionar per evitar l'ús de documentació obsoleta en l'organització, formant part l'esmentat versionat de l'identificador amb el qual es nomeni l'arxiu, i no podent coexistir dos documents vigents amb el mateix nom i versió.

La versió s'hauria d'identificar mitjançant la lletra "V", seguida d'un punt i el número de versionat que es durà a terme mitjançant classificació numèrica correlativa de dos números enters separats per un punt, en el qual el primer (a l'esquerra del punt) equival a la versió del document i el segon (a la dreta del punt) equival a les modificacions menors o revisions que ha patit aquesta versió. Per exemple: Mitjançant la V.2.8 s'expressa que ens trobem davant la segona versió del document que ha estat modificada o revisada 8 vegades.

4.5.2.3. Arxiu de la documentació

L'emmagatzematge dels documents hauria de garantir l'accessibilitat en els punts d'ús i prevenir l'ús no intencionat de documents obsolets, aplicant-los la identificació adequada quan són mantinguts.

4.5.2.4. Reordenació de la documentació

Partint de la premissa que tota informació té una vida útil, es procedirà a l'eliminació d'aquella informació que hagi consumit la mateixa i es consideri innecessària, un cop passat el termini de conservació establert.

4.5.3. CLASSIFICACIÓ I ACCÉS A LA INFORMACIÓ

La informació es pot presentar de diverses maneres i en diferents suports. Qualsevol que sigui la forma de presentació de la informació requereix el mateix grau de protecció, tant si està en mitjans electrònics, com en suports de dades o paper. La classificació, tractament i etiquetatge de la informació s'hauria de realitzar de la manera següent:

Classificació i etiqueta	Obligatorietat de l'etiquetatge	Nivell de seguretat	Mesures de seguretat
ÚS PÚBLIC	Optatiu	Nivell 0	No requereix consideracions especials de seguretat.
ÚS INTERN	Optatiu	Nivell 1	El seu accés és únicament per al personal de l'organització i altres que hi tinguin relació. No ha de ser publicada, ni compartida amb personal sense relació amb l'organització.
DIFUSIÓ LIMITADA	Obligatori	Nivell 2	Accés restringit al personal de l'organització, personal col·laborador o clients sota la premissa de "necessitat de conèixer".

CONFIDENCIAL	Obligatori	Nivell 3	Accés limitat a un departament, Àrea o grup reduït de persones dins de l'organització.

Tota la informació que no estigui etiquetada s'entendrà que és d'ús intern, llevat que per la seva naturalesa es dedueixi que és de caràcter públic. Tot i que l'etiquetatge de documentació pública no és obligatori, resulta beneficiós per garantir-ne la màxima difusió.

4.6. RISCOS QUE ES DERIVEN DEL TRACTAMENT DE DADES PERSONALS *(ARTICLE 12.1.F RD 311/2022 ENS: CONTINGUT DE LA POLÍTICA DE SEGURETAT)*

- Analisis de Riesgos V1.2 – metodologia Margerit – que s'adjunta com annex num.1 al present document.

APROVAT I SIGNAT per:

mercabarna
MERCADOS DE ABASTECIMIENTOS DE BARCELONA, S.A.
N.I.F. A-08210403
Zona Franca, Sector C - 08040 BARCELONA

DIRECTOR GENERAL 01.06.23