مقترح
السياسة الوطنية للحوسبة السحابية لدولة ليبيا

2030-2026



ازدهارُ البلدان كرامةُ الإنسان

الأمم المتحدة
الاسكوا
ESCWA

دولة ليبيا
الهيئة العامة للمعلومات
GENERAL INFORMATION AUTHORITY

مقترح
السياسة الوطنية للحوسبة السحابية
لدولة ليبيا

2030-2026



مصادر الصور:

الغلاف: © Ar_TH/stock.adobe.com

صفحة 2: © blackboard/stock.adobe.com

صفحة 6: © Funtap/stock.adobe.com

صفحة 14: © Tierney/stock.adobe.com

صفحة 19: © thodonal/stock.adobe.com

المحتويات

1. المقدمة 5

2. الرؤية والأهداف 7

1.2. الرؤية 7

2.2. الأهداف الاستراتيجية 7

3.2. الغايات العددية 7

4.2. نطاق السياسة 7

5.2. النطاق الزمني 7

3. تحليل الواقع الراهن للحوسبة السحابية 8

1.3. مواطن القوة 8

2.3. مواطن الضعف 9

3.3. الفرص 9

4.3. التهديدات 9

4. البنية السحابية المقترحة 10

أ. طبقة البنية التحتية 10

ب. طبقة المنصّات والخدمات 10

ت. طبقة الأمن والخصوصية 10

ث. طبقة الحوكمة والإدارة 11

5. ركائز السياسة الوطنية المقترحة 12

1.5. الحوسبة السحابية أولاً 13

2.5. تصنيف البيانات 14

3.5. الأمن السيبراني والخصوصية 17

4.5. حوكمة السياسة 18

5.5. نموذج المسؤولية المشتركة 21

6.5. إرشادات التعامل مع مزوّدي الخدمات السحابية 23

6. الرصد والتقييم 24

7. الخطة الإعلامية 25

8. إدارة المخاطر 26

9. المراجع 27

الحواشي 27

قائمة الأشكال

الشكل 1: بنية السحابة المقترحة 11
الشكل 2: منهجية تصنيف البيانات..... 17
الشكل 3: هيكلية الحوكمة للسياسة الوطنية للحوسبة السحابية..... 19

قائمة الجداول

الجدول 1: الجدول الاستراتيجي لاعتماد الحوسبة السحابية في ليبيا 12
الجدول 2: التصنيفات الأكثر شيوعاً للبيانات والمعلومات..... 15
الجدول 3: موجز لأهم إجراءات الحماية 18
الجدول 4: المسؤوليات الأمنية حسب نماذج الخدمة المختلفة..... 22
الجدول 5: خطة إدارة المخاطر 26

1. المقدمة

تعتبر الحوسبة السحابية العنصر التمكيني الأبرز في التحوّل الرقمي الذي يمثل قوة دافعة رئيسية للنمو الاقتصادي والابتكار. فهي وفّرت المتطلبات التي تحتاجها المؤسسات لتطوير حلولها وخدماتها التقنية كالسرعة والمرونة وقابلية التوسع، بالإضافة إلى إمكانية الوصول إلى موارد الحوسبة مثل الخوادم، وقواعد البيانات، والبرامج عبر الإنترنت بدلاً من الاستثمار في بنية تحتية محلية باهظة التكلفة.

لقد شهدت الحوسبة السحابية تحوّلاً جذرياً في كيفية تقديم الخدمات الرقمية وتخزين البيانات وإدارتها، وهذا ما دفع الحكومات حول العالم إلى تطوير سياسات وطنية لتبني هذه التكنولوجيا والاستفادة من إمكاناتها الهائلة. فلم يعد تبني حلول السحابة مجرد خيار تقني، بل أصبح ضرورة استراتيجية لتحقيق الكفاءة التشغيلية، وتعزيز الابتكار، وضمان الأمن السيبراني في العصر الرقمي.

وشهدت تدفقات البيانات عبر الحدود الدولية ازدياداً بشكل غير مسبوق مع تزايد الاعتماد على السحابة في جمع البيانات ومعالجتها وتخزينها. ونتيجةً لذلك، ظهرت تحديات جوهرية تتعلق بكيفية التعامل مع هذه البيانات، وهذا ما استدعى وضع أطر تنظيمية وقانونية صارمة. فلم تعد قضايا مثل تصنيف البيانات والسيادة عليها مجرد ممارسات تقنية اختيارية، بل صارت متطلبات قانونية واستراتيجية تُفرض بموجب لوائح عالمية وإقليمية مثل اللائحة العامة لحماية البيانات[1] (GDPR-EU) في أوروبا، وقوانين حماية البيانات الشخصية في بلدان عربية مثل الإمارات العربية المتحدة والمملكة العربية السعودية.

وبدأ الاهتمام عالمياً بالحوسبة السحابية على المستوى الحكومي في العقد الأول من القرن الحادي والعشرين، مع تزايد الوعي بفوائدها المحتملة في خفض التكاليف، وزيادة المرونة، وتحسين كفاءة الخدمات الحكومية. ولكن سرعان ما برزت تحديات تتعلق بالأمن، والخصوصية، وسيادة البيانات، وهذا ما استدعى تطوير أطر تنظيمية أكثر شمولاً.

في المراحل المبكرة كانت الحكومات تركّز على الفوائد الاقتصادية والتشغيلية، ويمكن ملاحظة تطوّر السياسات لاحقاً من مجرد التركيز على التشجيع على تبني الحلول السحابية إلى وضع أطر حوكمة صارمة. وأدى هذا التطوّر إلى ظهور مفاهيم جديدة مثل "السحابة الحكومية" التي توفّر بيئات سحابية مخصّصة للجهات الحكومية مع مستويات عالية من الأمان والامتثال.

ومن أبرز التجارب الناجحة للسحب الحكومية المركزية الشاملة، التي توفر مئات الخدمات الحكومية للمستفيدين: "سحابة ديم" التي أطلقتها الهيئة السعودية للبيانات والذكاء الاصطناعي. نجحت هذه السحابة في استضافة أكثر من 200 جهة حكومية وتقديم أكثر من 500 خدمة عبر منصة موحدة. وتهدف "سحابة أبو ظبي الحكومية" إلى ربط جميع الدوائر الحكومية المحلية في منصة موحدة لتعزيز التحوّل الرقمي، وتوفر أكثر من 250 خدمة حكومية موحّدة، وتهدف إلى الوصول لنسبة 100% تبني للسحابة السيادية للعمليات الحكومية بحلول نهاية عام 2027. أما المملكة الأردنية الهاشمية فقد اعتمدت "السحابة الحكومية الخاصة – GPC" التي تربط الوزارات والمؤسسات الحكومية الرسمية. لقد تمّ عبر مراكز الخدمات الحكومية المرتبطة بالسحابة إنجاز أكثر من 2.9 مليون معاملة حتى الربع الأول من عام 2025، مع هدف استراتيجي للوصول إلى 100% للخدمات الحكومية بحلول نهاية عام 2026.

على المستوى المحلي، تُعدّ تجربة شركة المدار الجديد في ليبيا واحدة من أهم المحاولات المحلية للحاق بركب التحوّل الرقمي، خاصةً في ظل التحديات التي تواجه البنية التحتية. من حيث البنى التحتية تمتلك المدار أوسع شبكة تغطية 4G/5G وهذا ما يجعلها القناة الأسهل للوصول للمواطن في القرى والمدن

البعيدة بدون الحاجة لانتظار كابلات الألياف البصرية، وتتركز تجربة المدار في فئة "البنية التحتية كخدمة". وقد أدت المدار دور "الوسيط الرقمي"، فهي لم تصمّم الخدمات الحكومية، بل وفرت "الطريق" الذي تمر عبره هذه الخدمات ويعتبر مشروع "منظومة منحة الزوجة والأبناء" بالتعاون مع وزارة الشؤون الاجتماعية مثالاً ناجحاً على ذلك.

ولتقييم هذه التجربة، من الضروري النظر إليها من زاوية أنها "مُمكّن رقمي" وليس مجرد شركة اتصالات. وبناءً على المعطيات المتاحة: نجحت المدار في توفير مراكز بيانات داخل ليبيا، وهذا ما سمح للجهات الحكومية باستضافة بياناتها محلياً. وهذا يحلّ معضلة "قانونية" كانت تمنع الجهات الرسمية من تخزين بيانات المواطنين في الخارج. أما منصة "سداد" فهي تُعتبر أنجح نموذج قدمته الشركة لدعم الخدمات الحكومية. ومن خلال ربط الهوية الرقمية (رقم الهاتف) بالدفع الإلكتروني، مكّنت المدار الجهات الحكومية من جباية الرسوم (جوازات، مخالفات، فواتير كهرباء) بشكل سحابي وآمن.



2. الرؤية والأهداف

1.2. الرؤية

بيئة رقمية تعتمد على الحوسبة السحابية وتضمن خدمات عالية الجودة وموارد مستدامة وآمنة.

2.2. الأهداف الاستراتيجية

1. الاستفادة القصوى من مرونة السحابة وكفاءتها الاقتصادية وسرعة إطلاق الخدمات.
2. إنشاء وتطبيق إطار موحّد وفعّال لتصنيف البيانات الحكومية والسيادة عليها.
3. تعزيز أمن السحابة وحماية البيانات والخصوصية والخدمات الحكومية.
4. فرض الحوكمة الفعّالة لضمان تطبيق موحّد وفعّال للسياسة.
5. اعتماد نموذج واضح ومفصّل للمسؤولية المشتركة يغطي جميع أنواع الخدمات السحابية.
6. إنشاء إطار شامل لإدارة العلاقة مع المزوّدين، يغطي متطلبات العقود والامتثال والتدقيق والمخاطر.

3.2. الغايات العددية

تعرض هذه الفقرة الأهداف الكمّية الطموحة التي تسعى الدولة إلى إنجازها بنهاية مدة التنفيذ.

- نقل 60% من الخدمات الحكومية الرقمية إلى السحابة مرحلياً.
- تحقيق 100% من متطلبات الأمن السيبراني وفق المعايير المتعارف عليها وما تحدّده هيئة أمن وسلامة المعلومات.
- تدريب 100% من العاملين في مجال الحوسبة السحابية على التقنيات المتقدمة في هذا المجال.
- رفع قيمة الاستثمار في البنى التحتية للحوسبة السحابية إلى 25%.
- رفع نسبة رضا المستخدمين عن الخدمات الإلكترونية إلى 75%.

4.2. نطاق السياسة

تُطبّق هذه السياسة على كافة الجهات الحكومية المعنية وأصحاب المصلحة ومزوّدي الخدمات السحابية العاملين في ليبيا المحليين والدوليين.

5.2. النطاق الزمني

تسري أحكام هذه السياسة وتوجيهاتها التنفيذية لفترة تمتد لخمس سنوات، بدءاً من عام 2026 وحتى نهاية عام 2030.

3. تحليل الواقع الراهن للحوسبة السحابية

تمّ تحليل الواقع الراهن باستخدام التحليل الرباعي SWOT وبالاعتماد على البيانات التي تمّ جمعها من خلال الاستمارة التي أعدتها الاسكوا والهيئة العامة للمعلومات، وخلصت إلى النقاط التالية:

1.3. مواطن القوة

أ. الاستخدام الحالي للحوسبة السحابية

- بناء سحابة حكومية تتضمن مركز بيانات وطنياً لخدمة جميع القطاعات الحكومية.
- تستخدم الكثير من المؤسسات الحكومية خدمات حوسبة سحابية تجارية، مثل خدمات البريد الإلكتروني والتخزين السحابي واستضافة المواقع الإلكترونية.
- تعتمد بعض المؤسسات الحكومية على حلول استضافة تقليدية (سحابة خاصة) وأغلبها خدمات مؤجّرة من مزوّدي خدمة محليين وقلّة من مزوّدي خدمة دوليين.
- أكثر خدمات الحوسبة السحابية استخداماً هي من نوع "البرمجيات كخدمة" ثم "البنية التحتية كخدمة" ثمّ "المنصة كخدمة".
- تقدّم الكثير من المؤسسات الحكومية للمواطنين عدداً مهماً من الخدمات الرقمية وعدداً من التطبيقات القابلة للترحيل (التهجير) إلى السحابة الحكومية حال توفرها.

ب. السياسات والمعايير

- تأييد لتطوير سياسة وطنية للحوسبة السحابية وتوحيد معايير الحوسبة السحابية على المستوى الوطني.
- تأييد لدعم الشركات المحلية في مجال الحوسبة السحابية والاستثمار فيه.
- لدى معظم المؤسسات خطط مستقبلية لاستخدام الحوسبة السحابية.
- توفر سياسة وطنية لحوكمة البيانات الحكومية[2] ودليل إرشادي مرتبط بها.
- توفر سياسة لأمان الحوسبة السحابية[3].

ج. الأطر القانونية

- قانون مكافحة الجرائم الإلكترونية لعام 2022.
- قانون المعاملات الإلكترونية لعام 2022.
- القانون رقم 4 للنظام الوطني للمعلومات والتوثيق لعام 1990.
- السياسة الوطنية لحوكمة البيانات لعام 2022.

د. الوعي والمعرفة

- وعي المؤسسات بأهمية استخدام الحوسبة السحابية للمساهمة في تحقيق أهدافها، بما في ذلك الحد من التكاليف، وزيادة المرونة، وتحسين الأداء.
- توفر برامج تعليمية وتدريبية (وإن كانت غير كافية) لتأهيل الكوادر المحلية وتزويدها بمهارات الحوسبة السحابية اللازمة.

2.3. مواطن الضعف

أ. الاستخدام الحالي للحوسبة السحابية

- انخفاض جودة وسرعة الإنترنت في بعض المناطق، مما يؤثر سلباً على أداء الخدمات السحابية وقد يعوق انتشارها.
- قلة الكوادر المختصة التي تمتلك المهارات المناسبة ومحدودية البرامج التعليمية والتدريبية المختصة في مجال الحوسبة السحابية والتكنولوجيات الناشئة.
- الاعتماد على مزوّدي خدمات سحابية خارج البلاد، مما يزيد من خطر انتهاك الخصوصية وتعرض البيانات والمعلومات الوطنية للمخاطر ويعمق التبعية التقنية.

ب. الأطر القانونية

- عدم توفر تشريعات تنظّم استخدام وتصنيف البيانات والسيادة عليها.
- عدم توفر تشريعات تنظّم استخدام الحوسبة السحابية وعمل مزوّدي الخدمة المحليين والدوليين، مما يسبّب حالة من الغموض وعدم الوضوح للمستثمرين.
- لا يزال قانون حماية البيانات الشخصية في طور الإقرار.

ج. السياسات والمعايير

- عدم توفر سياسة وطنية للحوسبة السحابية تنظّم استخدام خدمات الحوسبة السحابية في المؤسسات الحكومية.
- الحلول المعتمدة للحوسبة السحابية متباينة من حيث الكلفة وجودة الخدمة وأمن البيانات ، وذلك بسبب محدودية الأدلة واللوائح المنظّمة.

3.3. الفرص

- توفير بيئة مناسبة لجذب المستثمرين المحليين والدوليين في مجالات الحوسبة السحابية.
- إمكانية شراء خدمات الحوسبة السحابية عالمياً.
- تعزيز الثقة في الخدمات السحابية، بالعمل على إعداد سياسة تدفع المؤسسات إلى استخدام الحوسبة السحابية، وتحمي الخصوصية والبيانات المخزّنة على السحابة.
- بناء شراكات بين المؤسسات الحكومية والشركات المحلية والدولية العاملة في المجال للاستفادة من تجاربها في تطوير الخبرات والكوادر.
- دعم وتشجيع المستثمرين المحليين في:
  - إنشاء مراكز بيانات محلية تضمن استضافة البيانات داخل حدود الدولة.
  - بناء التطبيقات التي تعمل عبر البيئة السحابية لتسهيل التحوّل الرقمي.
  - تدريب وتوظيف الكوادر الوطنية في مجالات متقدمة مثل هندسة السحابة والأمن السيبراني.

4.3. التهديدات

- ضعف الاستثمارات عموماً في تكنولوجيا المعلومات قد يقلّل من اعتماد الخدمات السحابية.
- مخاوف الخصوصية وحماية بيانات المستخدمين، خاصةً مع عدم توفّر ضمانات كافية لحماية البيانات.

4. البنية السحابية المقترحة

يهدف هذا المقترح إلى وضع تصور للبنية العامة السحابية في ليبيا لدعم عملية التحوّل الرقمي الوطني. ويرتكز النموذج المقترح على مبدأ الدمج بين السحابة الحكومية والسُحُب الخاصة المعتمدة (القطاعية)، بما يضمن تحقيق التوازن بين سيادة البيانات والمرونة التشغيلية والابتكار. وتتكوّن البنية المقترحة للسحابة الوطنية من نموذج متعدد الطبقات يجمع بين سحابة حكومية وأخرى خاصة، ومكوّنات الأمان، وخدمات البيانات. يعرض الشكل (1) هيكلية السحابة الحكومية المقترحة، تليه تفاصيل للمكوّنات الأساسية للنموذج المقترح.

أ. طبقة البنية التحتية

- المراكز الحكومية: مراكز بيانات محلية بمعايير Tier III+ أو أفضل، تضمن توفر، التبريد، والطاقة الاحتياطية، ونظام مكافحة الحرائق، والأمن المادي.
- شبكة وطنية آمنة (GovNet) تتميز باتصال عالي السرعة بين المؤسسات، وشبكات مخصّصة لربط المراكز.

ب. طبقة المنصّات والخدمات

يمكن أن تتضمن هذه الطبقة على سبيل المثال:

- منصة حاويات مُدارة (Kubernetes) لتشغيل مايكروسيرفيسز وتسهيل النشر.
- خدمات قواعد بيانات مُدارة (DBaaS) وأنظمة تخزين موزعة.
- منصة التكامل المستمر والتسليم المستمر (CI/CD) لنشر التطبيقات والتحديثات بسرعة، وضمان الجودة والأمان.
- بيئة توفر قدرات التحليلات الضخمة، والبيانات الكبيرة (Data Warehouse)، والذكاء الاصطناعي عند الحاجة.

ج. طبقة الأمن والخصوصية

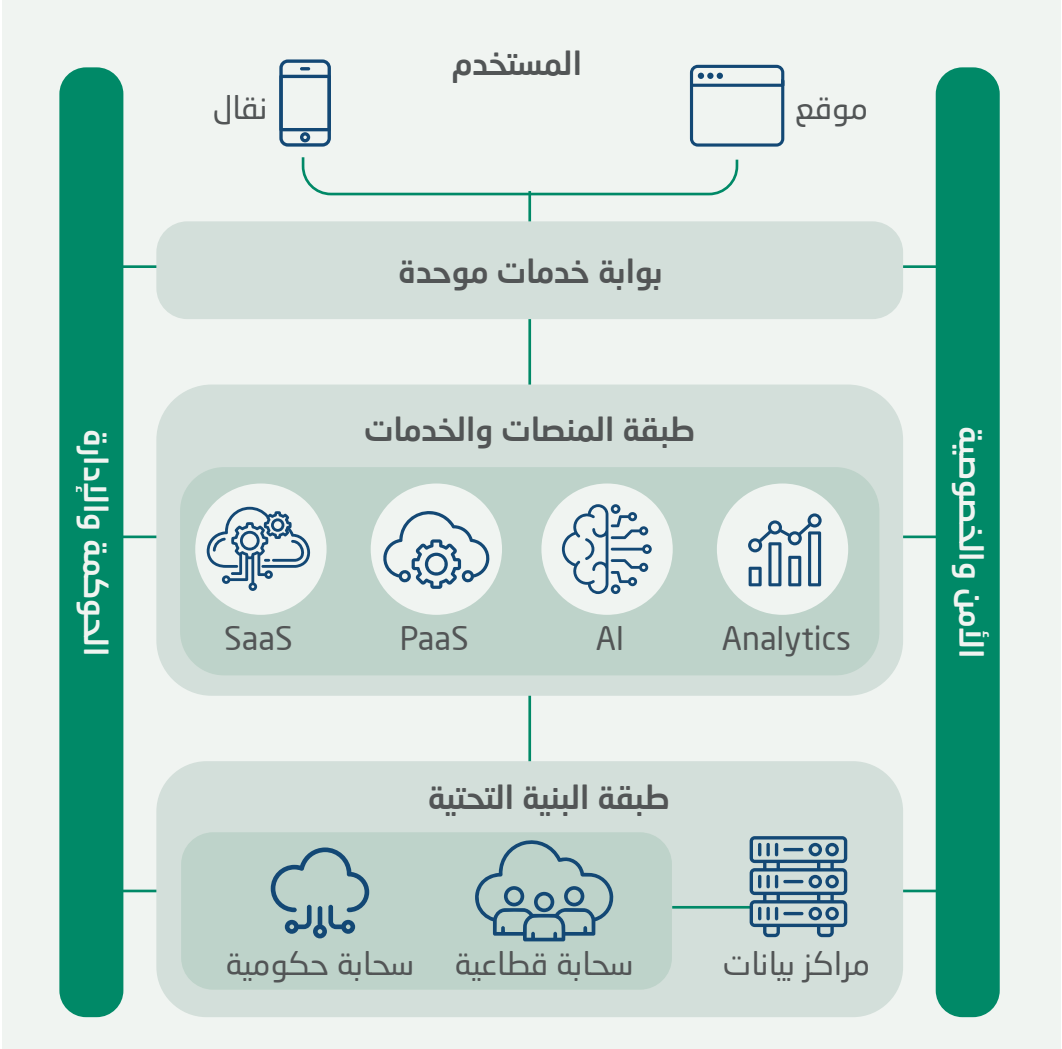
يمكن أن تتضمن هذه الطبقة على سبيل المثال:

- نموذجاً أمنياً متعدد الطبقات يتكوّن من جدار ناري، وأنظمة اكتشاف/منع التطفل (IDS/IPS)، ووسيط أمان الوصول السحابي.
- تشفيراً شامل للبيانات أثناء النقل أو الإرسال أو الحفظ بوسائط التخزين.
- مفاتيح مُدارة محلياً لضمان السيادة، ولحماية المفاتيح الرقمية وإدارة عمليات التشفير والتوقيعات الرقمية.
- نظاماً مركزياً لإدارة الهوية والوصول (Identity & Access Management) يُستخدم للتحقق من هوية المستخدمين وتحديد مستوى ونوع الوصول الذي مُنح لهم ومنع المتسللين والأشخاص غير

المصرّح لهم من الوصول، ويدعم تقنيات المصادقة مثل تسجيل الدخول الموحّد أو تسجيل الدخول مرة واحدة (SSO)، والمصادقة المتعددة العوامل (MFA)، ومبدأ الحدّ الأدنى من الامتيازات.

- مركز عمليات الأمن (SOC) وعمليات الرصد 7/24 والتخطيط لحوادث الأمن السيبراني، يختص بمراقبة الشبكات والأنظمة واكتشاف التهديدات السيبرانية والاستجابة لها.

الشكل 1: بنية السحابة المقترحة



ج. طبقة الحوكمة والإدارة

يمكن أن تتضمن هذه الطبقة على سبيل المثال:

- أنظمة التسجيل والمراقبة والتتبع (Logging, Monitoring, Tracing) لتوفير فهم معمّق لسلوك النظام من خلال تتبع مقاييس محدّدة للكشف عن أي خلل.
- أنظمة إدارة الامتثال والمخاطر والحوكمة (GRC) للمساعدة في المراقبة، وضمان الالتزام باللوائح، وتسهيل الامتثال.
- سياسات تصنيف البيانات ومنع فقدان البيانات (DLP)، وهي مجموعة من الأدوات والعمليات والتقنيات التي تهدف إلى حماية البيانات الحساسة من السرقة أو التسريب أو سوء الاستخدام.
- بوابة خدمات موحّدة لتقديم الخدمات للمواطن والموظف مع واجهات موثقة.
- النسخ الاحتياطي والاسترداد كخدمة (Backup & DRaaS) وخطط استمرارية الأعمال.

5. ركائز السياسة الوطنية المقترحة

تعتمد السياسات الوطنية الفعالة للحوسبة السحابية على مجموعة من الركائز الأساسية التي تضمن تبنياً آمناً وفعّالاً ومستداماً. هذه الركائز تتجاوز الجوانب التقنية لتشمل الأبعاد التنظيمية، والمالية، والبشرية. واستناداً إلى ما سبق، جرى اقتراح السياسة الوطنية للحوسبة السحابية التي توصي بتبني مفهوم "السحابة أولاً".

وترتكز هذه السياسة على ستة محاور استراتيجية رئيسية، تمثل الركائز الأساسية اللازمة لعملية التحوّل الآمن والممتثل نحو الحوسبة السحابية على المستوى الوطني. يتضمن هذا المستند تفصيلاً دقيقاً لكل ركيزة من هذه الركائز في الفقرات التالية.

1. الحوسبة السحابية أولاً
2. تصنيف البيانات
3. الأمن السيبراني والخصوصية
4. حوكمة السياسة
5. نموذج المسؤولية المشتركة
6. إرشادات التعامل مع مزوّدي الخدمات السحابية

يلخّص الجدول (1) العلاقة بين كل ركيزة من هذه الركائز والهدف الاستراتيجي المرتبط بها، الذي يوجه جميع الأنشطة والمهام التنفيذية ضمن السياسة:

الجدول 1: الجدول الاستراتيجي لاعتماد الحوسبة السحابية في ليبيا

ركائز السياسة	الهدف الاستراتيجي
الحوسبة السحابية أولاً	الاستفادة القصوى من مرونة السحابة وكفاءتها الاقتصادية وسرعة إطلاق الخدمات.
تصنيف البيانات	إنشاء وتطبيق إطار موحّد وفعّال لتصنيف البيانات الحكومية والسيادة عليها.
الأمن السيبراني والخصوصية	تعزيز أمن السحابة وحماية البيانات والخصوصية والخدمات الحكومية.
حوكمة السياسة	فرض الحوكمة الفعّالة لضمان تطبيق موحد وفعال للسياسة.
نموذج المسؤولية المشتركة	اعتماد نموذج واضح ومفصل للمسؤولية المشتركة يغطي جميع أنواع الخدمات السحابية.
إرشادات التعامل مع المزوّدين	إنشاء إطار شامل لإدارة العلاقة مع المزودين، يغطي متطلبات العقود والامتثال والتدقيق والمخاطر.

1.5. الحوسبة السحابية أولاً

يهدف مبدأ "السحابة أولاً" إلى تسريع وتيرة انتقال الجهات الحكومية من حلول تقنية المعلومات التقليدية إلى حلول الحوسبة السحابية. هذا المبدأ يجعل من خيار الحوسبة السحابية الخيار الأول للنظر فيه والمفضّل عند اتخاذ قرارات الاستثمار في تكنولوجيا المعلومات، وذلك قبل طرح أي مشروع يتضمن بناء أو شراء أو توسيع استضافة البيانات أو الخدمات الإلكترونية.

ويهدف تبني هذا المبدأ الاستراتيجي إلى الاستفادة القصوى من مرونة السحابة وكفاءتها الاقتصادية وسرعة إطلاق الخدمات حيث يوجّه الجهات الحكومية إلى اعتماد الحلول السحابية كخيار افتراضي وأساسي لجميع المشاريع والتطبيقات الجديدة أو عند تحديث الأنظمة القائمة. ولا يتم اللجوء إلى البنية التحتية المحلية إلا في حال وجود متطلبات أمنية أو تنظيمية أو فنية لا يمكن تلبيتها من خلال السحابة.

إن الهدف الرئيس من تطبيق مبدأ "السحابة أولاً" هو تحقيق فوائد استراتيجية للجهات الحكومية تتمثل في:

- خفض التكلفة الإجمالية عن طريق تحسين استخدام تكنولوجيا المعلومات، وتجنب الازدواجية في الإنفاق الحكومي على هذه التكنولوجيات.
- دعم الأمن السيبراني باستخدام منصّات معتمدة تتبنى أفضل معايير الأمن السيبراني، بالاعتماد على خبرات مزوّدي الخدمات السحابية في هذا المجال.
- تمكين قابلية التشغيل البيني مع الجهات الأخرى.
- زيادة جودة الخدمة بتبني حلول أكثر مرونة وابتكاراً في قطاع الخدمات الحكومية.

أ. متطلبات وإجراءات التطبيق

تفرض السياسة، على كافة الجهات الحكومية المستفيدة، عدة متطلبات وإجراءات:

- **تحديد مستوى السرية واختيار المزوّد:** يتعين على الجهة المستفيدة تحديد مستوى سرية بياناتها وفق التصنيف المذكور في هذه السياسة، واختيار مزوّد خدمة يمتلك ترخيصاً يناسب التصنيف.
- **خطة الانتقال (التهجير):** يتعين على الجهة المستفيدة وضع خطة لتنفيذ عملية الانتقال إلى الحوسبة السحابية بما يضمن عدم حصول أي ضرر في البيانات أو انقطاع في الخدمة لمدة لا تناسب طبيعة الخدمة.
- **التدريب المناسب:** يتعين على الجهات الحكومية توفير التدريب المناسب لكوادر تكنولوجيا المعلومات المعنيين بتشغيل وإدارة خدمات الحوسبة السحابية بالشكل الأمثل.
- **الحلّ التقليدي في الحالات الاستثنائية:** في حال تعذّر اعتماد حلول الحوسبة السحابية، يمكن اعتماد الحلول التقليدية بعد توضيح الأسباب التي تحول دون اعتماد الحوسبة السحابية، والحصول على موافقة اللجنة الوطنية للحوسبة السحابية.

ب. ترتيب أولويات النماذج والأنواع

تحدّد السياسة للجهات الحكومية أولويات واضحة لحلول ومنصّات الحوسبة السحابية، حسب نموذج الخدمة ونوع السحابة. ويجب على المؤسسات الحكومية المستفيدة عند اختيار أي من هذه الحلول مراعاة ترتيب الأولويات التالي:

1. حسب نوع السحابة تكون الأولوية للأنواع التالية: السحابة الحكومية، ثم السحابة الخاصة (أو القطاعية)، فالسحابة العامة، مع مراعاة محدّدات التراخيص ومستوى سرية البيانات.
2. حسب نموذج الخدمة تكون الأولوية للنماذج التالية: البرمجيات كخدمة، ثمّ المنصة كخدمة، فالبنية التحتية كخدمة.

ويُعدّ نموذج البرمجيات كخدمة الخيار المفضّل لأنه يحقق الاستفادة القصوى من حلول الحوسبة السحابية. وفي حال عدم إمكانية تطبيقه يجري اختيار نموذج المنصّة كخدمة. أما نموذج البنية التحتية كخدمة فيتم اختياره في حال تعذّر تطبيق النموذجين السابقين.

2.5. تصنيف البيانات

تصنيف البيانات هو حجر الأساس لأي استراتيجية فعّالة لحوكمة البيانات، فهو عملية منهجية لتنظيم أصول البيانات داخل المؤسسة بناءً على حساسيتها وأهميتها وقيمتها، وكذلك على مدى تأثير انكشافها أو فقدانها. إن عملية التصنيف ليست مجرد ممارسة تقنية، بل هي المرحلة الأساسية التي تُترجم الالتزامات القانونية إلى إجراءات قابلة للتطبيق. لذلك، فإن عدم تصنيف البيانات يمكن أن يؤدي إلى أحد مسارين محفوفين بالمخاطر: إما الإفراط في الحماية، وهذا ما يؤدي إلى إهدار الموارد على بيانات لا تتطلب ذلك، أو التقصير في الحماية، الذي يُعرّض المؤسسة إلى مخاطر قانونية وأمنية جسيمة.

وتفرض قوانين حماية البيانات الشخصية متطلبات محدّدة على البيانات الحساسة. ولكن بدون عملية تصنيف، لن تتمكن المؤسسة من تحديد البيانات التي تندرج تحت فئة "حساسة" أو "عامة" لتلبي هذه المتطلبات. فمن غير الممكن تحقيق الامتثال لهذه القوانين إلا إذا كان لدى المؤسسة فهم واضح لأنواع البيانات التي تعالجها. لذلك، يُعدّ تصنيف البيانات الجسر الرابط بين المتطلبات القانونية والإجراءات التقنية. فهو عملية منهجية لتحديد حساسية وقيمة البيانات الحكومية بناءً على تأثير الكشف عنها أو فقدانها.

ويهدف التصنيف إلى ربط كل فئة من البيانات بمستوى محدّد من إجراءات الحماية. فكلما زادت حساسية البيانات، وجب تطبيق ضوابط أمنية وتنظيمية أكثر صرامة عليها، خاصة فيما يتعلق بمكان تخزينها والسيادة عليها. في هذه العملية، يجري تقييم مستوى الضرر المحتمل الناتج عن الإفصاح غير المصرّح به أو الوصول غير القانوني للبيانات، وهذا ما يُتيح للمؤسسة تطبيق الضوابط الأمنية المناسبة لكل نوع من البيانات. ولا يقتصر الهدف على تحسين الأمان فحسب، بل يمتد ليشمل تعزيز حماية الخصوصية، وتسهيل الامتثال للوائح، وتحسين جودة البيانات، ودعم عملية اتخاذ القرارات الاستراتيجية.



أ. مستويات التصنيف والأطر الشائعة

تتضمن عملية تصنيف البيانات تقسيمها إلى فئات مثل عامة أو سرية. وتبدأ العملية بتحديد الأهداف مثل تحسين الأمان أوتحسين الإدارة، والمعايير مثل مستوى الحساسية أو الخصوصية أو الأهمية الاستراتيجية، ثمّ تقييم كل أصل بيانات وتعيين مستوى التصنيف المناسب له، ومن ثمّ تنفيذ الضوابط الأمنية اللازمة لكل مستوى، مع المراقبة والمراجعة الدورية. وبما أنه لا يوجد معيار عالمي موحّد للتصنيف، فكل مؤسسة تُحدّد مستوياتها بما يتوافق مع أهدافها ومتطلبات الامتثال الخاصة بها. ومع ذلك، فإن العديد من الأطر الوطنية والعالمية تُصنّف البيانات إلى أربعة مستويات رئيسية.

قد تختلف التسميات والترتيبات الدقيقة بين المؤسسات والبلدان، لكن هذا التسلسل يمثل ترتيب المصطلحات المستخدمة في تصنيفات البيانات والمعلومات بناءً على حساسيتها (من الأقل حساسية إلى الأكثر). ويمثل هذا الترتيب (الجدول 2) المبدأ العام لتصنيف البيانات وهو كما يلي: عام (Public)، غير مقيّد (Unrestricted)، داخلي (Internal)، حساس (Sensitive)، مقيّد (Restricted)، سري (Confidential)، سري للغاية (Secret).

الجدول 2: التصنيفات الأكثر شيوعاً للبيانات والمعلومات

الترتيب	المصطلح	الفئة العامة	الأثر المحتمل عند الإفصاح
1	عام	عامة/منخفضة	لا أثر أو أثر ضئيل جداً
2	غير مقيّد	عامة/منخفضة	لا أثر أو أثر ضئيل جداً
3	داخلي	متوسطة	بعض الإزعاج أو الإحراج للمؤسسة
4	حساس	متوسطة/عالية	ضرر مادي أو تشغيلي ملموس
5	مقيّد	عالية	ضرر كبير
6	سري	عالية جداً	ضرر خطير للمؤسسة
7	سري للغاية	قصوى	ضرر جسيم أو كارثي

والجدير بالذكر أن سياسة تصنيف المعلومات[4] الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات قد قسمت البيانات إلى الفئات الثلاث التالية: سرية (مقيدة) ، حسّاسة (داخلية)، عامة (غير مقيّدة). أما السياسة الوطنية لحوكمة البيانات الحكومية[5] فقد قسمتها إلى خمسة أقسام هي: سري للغاية، سري، مقيّد، متاحة لأصحاب المصلحة، متاحة للعامة.

تعتمد هذه الوثيقة تصنيفاً يتوافق مع الأطر الدولية ويتماشى مع التصنيفات الوطنية، ويتكون من الفئات الأربع التالية:

1. بيانات سرية (Secret)

- لها أعلى مستوى من الحساسية، وأعلى مستويات التصنيف للبيانات وقد يؤدي الكشف عنها إلى ضرر كارثي لا يمكن تداركه أو إصلاحه للمؤسسة أو الأفراد، وقد يترتب عليه مسؤوليات قانونية أو غرامات ضخمة.
- **مثال:** مفاتيح التشفير المستخدمة للبنى التحتية الوطنية، والأسرار التجارية، وبراءات الاختراع، والبيانات الشخصية الخاضعة لقوانين صارمة (مثل السجلات الطبية).
- **موقع التخزين:** في سحابة حكومية محلية مع مستويات أمان عالية، محمية ضد السرقة وفقدان الأجهزة.

- **إجراءات الحماية:**
  - تخزين البيانات بواسطة أنظمة مشفّرة بالكامل.
  - استخدام أنظمة إدارة مفاتيح التشفير، لضمان التحكم الصارم في المفاتيح.
  - تطبيق مبدأ أقلّ امتيازاً، بمنح المستخدمين والتطبيقات الحد الأدنى من الصلاحيات اللازمة لأداء المهام فقط.
  - إجراءات مصادقة متعددة.
  - عزل تام للشبكات، بفصل الأجزاء الحساسة من الشبكة، عن بقية الشبكة أو الإنترنت لزيادة الأمان.
  - سياسات حذف آمنة للبيانات المنتهية الصلاحية.

2. بيانات مقيّدة (Restricted)

- تتطلب حماية مشدّدة، ويؤدي الإفصاح عنها بشكل غير مصرّح به إلى ضرر جسيم للمؤسسة أو الأفراد. هذه البيانات مخصصة للاستخدام الداخلي ومقيّدة على مجموعة محدّدة من الموظفين.
- **مثال:** معلومات عن المنشآت الحيوية، البيانات المالية أو الملكية الفكرية، معلومات الموارد البشرية، بيانات العملاء غير العامة، التقارير المالية الداخلية، خطط التسويق المستقبلية.
- **موقع التخزين:** في أنظمة تخزين محلية (سحابة حكومية) أو سحابة خاصة مشفّرة، مع تطبيق قواعد صارمة للوصول، وخاصية النسخ الاحتياطي الدوري للبيانات.
- **إجراءات الحماية:**
  - تشفير للبيانات وفق المعايير الدولية أثناء النقل والتخزين.
  - تجزئة الوصول بحيث يكون الوصول فقط للموظفين المصرّح لهم.
  - أنظمة كشف التسلل للأنشطة المشبوهة.
  - استخدام اتصال آمن عند الوصول عن بُعد.
  - اختبارات اختراق دورية لتقييم مستوى الأمان.

3. بيانات حساسة (Sensitive)

- تتطلب عناية خاصة، ولا يجب نشرها خارج المؤسسة، ولكن الإفصاح عنها لا يُشكل تهديداً خطيراً، وقد يكون له تأثير سلبي أو ضرر متوسط على المؤسسة. هذه البيانات مخصّصة للاستخدام الداخلي العام ولا يُسمح بنشرها خارج المؤسسة.
- **مثال:** التقارير الداخلية للمشاريع، أو محاضر الاجتماعات، أو المراسلات الداخلية العامة، أو سياسات وإجراءات العمل، أو دليل الموظفين الداخلي.
- **موقع التخزين:** في أنظمة تخزين محلية داخل المؤسسة، أو في سحابة خاصة بشرط التخزين ضمن الحدود الجغرافية للدولة، مع تطبيق ضوابط وصول صارمة.
- **إجراءات الحماية:**
  - استخدام كلمات مرور متوافقة مع المعايير التنفيذية لحماية الملفات والحسابات.
  - تشفير أثناء النقل وعند التخزين.
  - تطبيق سياسة التحكم في الوصول بحيث لا يمكن لأي شخص الاطلاع على الموارد إلا بموافقة.

4. بيانات عامة (Public)

- متاحة للعامة ولا يترتب أي ضرر على الإفصاح عنها للمؤسسة أو الأفراد، أو البيانات التي يمكن مشاركتها علناً.

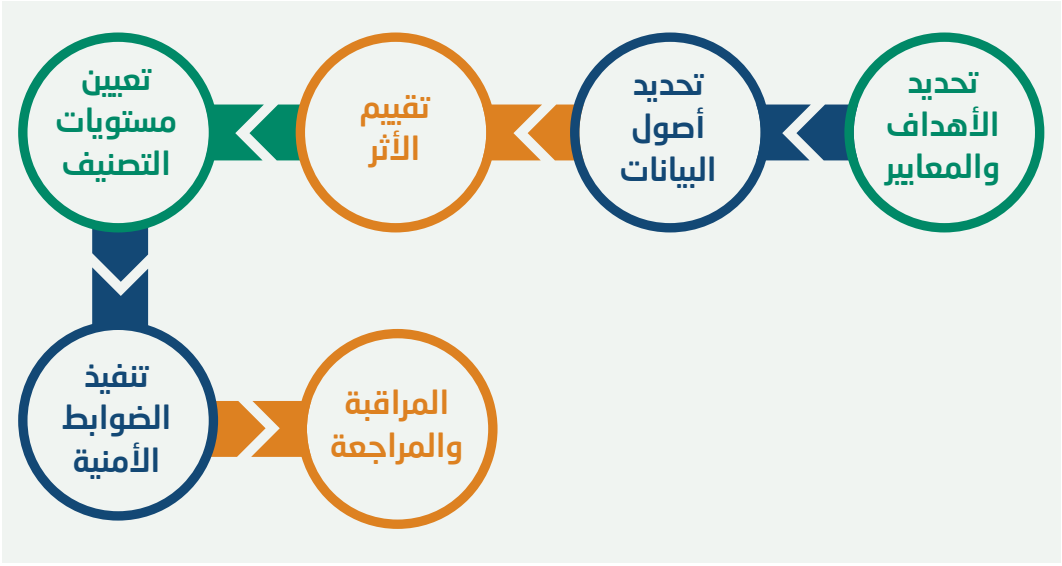
- **مثال:** الإحصاءات الوطنيّة حول عدد السكان والبيئة والأعمال، أو المواد التسويقية، أو الإعلانات، أو معلومات الاتصال العامة للمؤسسة، أو البيانات الصحفية، أو الكتيبات التسويقية، أو المعلومات المتاحة على الموقع الإلكتروني للمؤسسة.
- **موقع التخزين:** في أنظمة تخزين سحابية عامة أو أنظمة تخزين محلية يمكن الوصول إليها بسهولة من قبل عدد كبير من المستخدمين بدون قيود على الموقع الجغرافي.
- **إجراءات الحماية:**
  - تطبيق التحكم في التعديلات (عدم السماح لأي مستخدم بالتعديل العشوائي).
  - مراقبة الاستخدام العام لمنع التلاعب أو الإساءة.

ب. منهجية التصنيف

تتبع المؤسسات عادةً منهجية منظّمة لتنفيذ عملية التصنيف (الشكل 2)، تتضمن الخطوات التالية:

1. **حصر البيانات:** يجري في هذه المرحلة حصر جميع أصول البيانات والسجلات المملوكة للمؤسسة، بما في ذلك تلك المخزّنة في الأنظمة السحابية.
2. **تقييم الأثر:** تُجرى دراسة شاملة لتقييم الأثر المحتمل عند الإفصاح عن البيانات أو الوصول غير المصرّح به إليها. وبناءً على نتيجة التقييم (مرتفع، متوسط، منخفض، منعدم)، يجري تحديد مستوى التصنيف المناسب.
3. **تحديد التصنيف:** يجري تعيين مستوى التصنيف (سري، مقيّد، حساس، عام) لكل مجموعة من البيانات بناءً على نتيجة تقييم الأثر.
4. **تطبيق الضوابط:** تُنفّذ إجراءات الحماية المناسبة لكل مستوى تصنيف، مثل التشفير، والتحكم في الوصول، وتحديد سياسات الاحتفاظ بالبيانات.

الشكل 2: منهجية تصنيف البيانات



3.5. الأمن السيبراني والخصوصية

يركّز على مجموعة من المتطلبات والضوابط الواجب على الجهات الحكومية ومزوّدي الخدمات السحابية الالتزام بها لضمان حماية البيانات والخدمات الحكومية. وتشمل هذه الإجراءات تطبيق معايير الأمن السيبراني الصارمة، وآليات إدارة الهوية والوصول، وضمان المرونة للخدمات السحابية ضد الهجمات أو الانقطاعات، بالإضافة إلى إجراءات التشفير اللازمة للبيانات أثناء النقل والتخزين. ويضمن تطبيق نظام

فعّال لتصنيف البيانات توجيه الموارد الأمنية نحو الأصول الأكثر قيمة وحساسية. حيث تبدأ الحماية الفعّالة بتحديد ما يجب حمايته، ثمّ تطبيق الحماية المناسبة لكل مستوى من مستويات التصنيف.

الجدول 3: موجز لأهم إجراءات الحماية

التصنيف	تقييم الأثر	أهم إجراءات الحماية
بيانات سرية	مرتفع	عزل الشبكات، مصادقة متعددة العوامل، تشفير كامل، مراقبة دائمة
بيانات مقيّدة	متوسط	تشفير قوي، سجل دخول، مراقبة، شبكات خاصة
بيانات حساسة	منخفض	كلمات مرور قوية، تشفير أثناء النقل، تحكم بالوصول
بيانات عامة	منعدم	مراجعة قبل النشر، منع التعديل غير المصرح به

بالإضافة إلى إجراءات الحماية الخاصة بكل صنف من أصناف البيانات، سالفة الذكر، في ما يلي توضيح للإجراءات المتّبعة عادة لحماية البيانات في جميع مستويات التصنيف الأربعة:

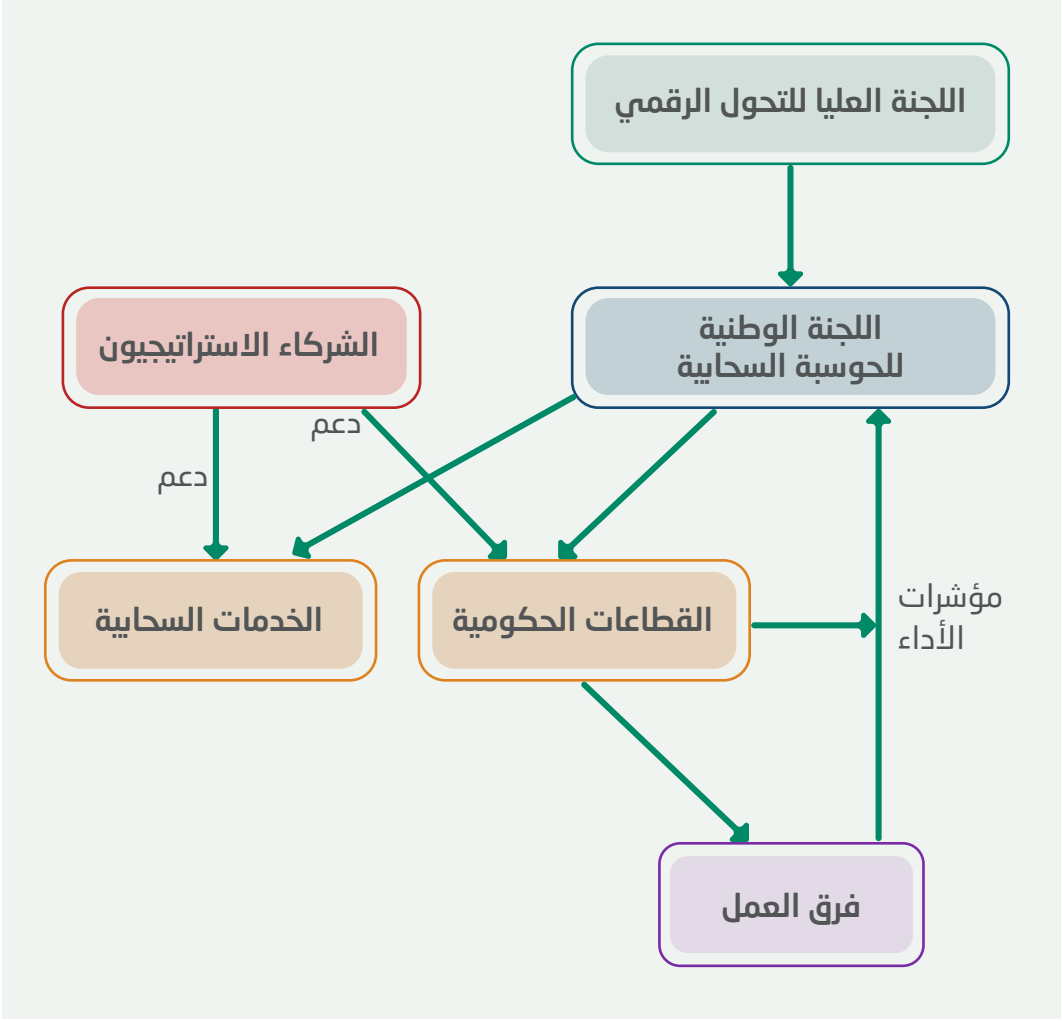
- مراجعة الأذونات بشكل دوري، تضمن منع تراكم الصلاحيات غير الضرورية وتقلّل مخاطر وصول غير المصرّح لهم.
- تعزيز الهوية بإجراءات مصادقة متعددة تُعتبَر طبقة دفاع إضافية ضد هجمات التصيّد وسرقة كلمات المرور، وتضمن أن يكون المستخدم هو فعلاً من يدّعي أنه هو.
- مراقبة أمنية على مدار الساعة 7/24، تتيح رصد الأنشطة المشبوهة والتهديدات الأمنية والاستجابة لها فور وقوعها بدون تأخير.
- تقييد الوصول المادي (غرف مؤمنة، بطاقات ذكية، بصمة) لضمان أن يقتصر الوصول إلى الأجهزة والخدمات الحساسة على الموظفين المخوّلين فقط.
- مراقبة الدخول والخروج لكل عملية وصول أو تعديل، مما يوفر سجلاً تفصيلياً لمن قام بالوصول إلى البيانات أو تعديلها ومتى، وهو أمر حيوي للمساءلة والتحقيق.
- حفظ النسخ الاحتياطية في مواقع مؤمنة خارجية يضمن استعادة البيانات بسرعة بعد أي حادث مثل الكوارث الطبيعية أو هجوم إلكتروني كبير.
- تدريب الموظفين على التعامل السليم مع هذه البيانات للتقليل من الأخطاء البشرية، التي تُعدّ أحد أهم أسباب التسريبات، ويرسّخ ثقافة الأمن.
- الاحتفاظ بنسخ احتياطية مشفّرة، يهدف إلى ضمان السرية وحماية البيانات الاحتياطية، حتى لو وقعت في الأيدي الخاطئة، وهذا ما يضمن سريتها التامة.
- التأكد من دقّة المعلومات قبل النشر، وهو إجراء يضمن تقديم معلومات صحيحة ومحدّثة للجمهور أو الأطراف المعنية، ويعزّز الثقة.
- المراجعة والموافقة قبل النشر لضمان عدم احتوائها على بيانات غير مصرّح بها، وهي آلية حاسمة تضمن عدم نشر أي بيانات سرية أو شخصية أو مصنّفة عن طريق الخطأ أو الإهمال.

4.5. حوكمة السياسة

1تُعنى بتحديد الإطار التنظيمي والتشريعي المسؤول عن إدارة وتنفيذ وتحديث السياسة الوطنية للحوسبة السحابية. وتشمل الحوكمة تحديد الأدوار والمسؤوليات بين الكيانات المعنية (كاللجنة العليا واللجنة الوطنية)، ووضع آليات للمراقبة وتقييم الأداء، وضمان التزام جميع الجهات الحكومية بالمعايير والأطر المعتمدة لضمان تطبيق موحّد وفعّال للسياسة.

وتؤدي حوكمة السياسة الوطنية للحوسبة السحابية دوراً محورياً في تنفيذها، وتُعدّ ركيزة أساسية لضمان تحقيق أهدافها، إذ تضمن تنفيذ السياسة على النحو المُخطّط له من خلال مجموعة من الممارسات المتسقة والآليات الفعّالة، في إطارٍ تنظيمي يُحدّد الأدوار والمسؤوليات وآليات اتخاذ القرارات المتعلقة بعملية التنفيذ. وتوفر هذه الهيكلية المتكاملة إطار عمل واضح للحوكمة والتنظيم والتنسيق بين جميع الأطراف المعنية. يعرض الشكل (3) النموذج المقترح لهذه الهيكلية.

الشكل 3: هيكلية الحوكمة للسياسة الوطنية للحوسبة السحابية





أ. اللجنة العليا للتحوّل الرقمي

الوظيفة: تتخذ القرارات الاستراتيجية العليا وتضمن التوافق الوطني.

المهام:

- ضمان التوافق مع الخطط الوطنية للتحوّل الرقمي.
- اعتماد الأطر التنظيمية والمعايير العامة.
- الإشراف على تطبيق آليات الحوكمة ومتابعة الأداء العام.

ب. اللجنة الوطنية للحوسبة السحابية

الوظيفة: الجهة المرجعية المعنية بإدارة السياسة الوطنية والإشراف على تطبيقها.

المهام:

- إعداد خطط العمل السنوية.
- إدارة برامج التحوّل السحابي الوطني.
- اعتماد الإرشادات التنفيذية والسياسات الفنية.
- التنسيق بين الجهات الحكومية والقطاع الخاص.
- متابعة التزام الجهات بالمعايير الوطنية للأمن والسيادة الرقمية.

ج. القطاعات الحكومية

الوظيفة: الجهة المعنية بإدارة السياسة داخل القطاع الحكومي والإشراف على تنفيذها.

المهام:

- تطوير خطة عمل خاصة بالقطاع الحكومي.
- تنفيذ المهام والمسؤوليات المكلّف بها وفق محاور العمل المحدّدة بالسياسة.
- إعداد تقارير دورية عن سير خطة عمل القطاع ومدى التقدّم في تنفيذ المهام المحدّدة فيها.

د. الخدمات السحابية

الوظيفة: الجهة التنفيذية والتنظيمية التي تدير ترحيل الخدمات على المستوى الوطني.

المهام:

- تحديد الأولويات والمشروعات المشتركة.
- تطوير منصات الخدمات السحابية المشتركة.
- تقديم الدعم الفني للجهات الحكومية في الانتقال إلى السحابة.
- ضمان تكامل البيانات والخدمات الرقمية عبر الأنظمة الحكومية.

هـ. فرق العمل

الوظيفة: الأذرع التنفيذية الميدانية لتنفيذ المشاريع المحددة.

المهام:

- تنفيذ المهام الفنية والتقنية ضمن المشاريع السحابية.
- إعداد الدراسات والتقارير الداعمة لصنع القرار.
- مراقبة الالتزام بالمعايير الأمنية والتقنية أثناء التنفيذ.
- رفع مؤشرات الأداء للجنة الحوسبة.

و. الشركاء الاستراتيجيون

الوظيفة: الجهات الداعمة من القطاعين العام والخاص.

المهام:

- تقديم خدمات واستشارات فنية وتقنية.
- المساهمة في مشاريع السحابة الوطنية.
- المشاركة في برامج التدريب والتطوير.
- دعم الابتكار في تقنيات الحوسبة السحابية.

ز. فض المنازعات

في إطار السياسة الوطنية للحوسبة السحابية، تعتمد آلية فض المنازعات التي قد تحدث بين أصحاب المصلحة (الجهات الحكومية، الشركات، مزودي الخدمة والمستخدمين) على مزيج من الإجراءات الإدارية والأطر القانونية والتعاقدية. هذه الآلية تعتمد منهجاً متدرجاً من ثلاث خطوات كالتالي:

1. التسوية الودية: هي الخطوة الأولى للتقاضي في معظم العقود السحابية، وفيها يتم تشكيل لجان فنية وإدارية من الطرفين لمحاولة حل النزاع سواء كان تقنياً أو مالياً، خلال فترة زمنية محددة (بين 30-60 يوماً).
2. اللجوء للجهات المنظمة: في حال فشل المفاوضات الودية، يتم اللجوء إلى "المنظّم" أو "الهيئة" المسؤولة عن القطاع مثل اللجنة الوطنية للحوسبة السحابية أو الهيئة العامة للاتصالات والتقنية.
3. القضاء الإداري أو التجاري: حسب نوع النزاع أو أطرافه، يتم اللجوء إما للقضاء الإداري (قضية تتعلق بعقود إدارية) أو التجاري (نزاع بين مزوّد الخدمة والمستفيد).

5.5. نموذج المسؤولية المشتركة

يُعدّ نموذج المسؤولية المشتركة مفهوماً محورياً وأساسياً في بيئات الحوسبة السحابية، إذ يهدف إلى توضيح وتوثيق تقسيم مسؤوليات الأمن بين طرفين رئيسيين: مزوّد الخدمة السحابية (المزوّد) وهو المسؤول عن أمن "السحابة" نفسها، والجهة الحكومية المستفيدة (العميل) وهي المسؤولة عن أمن "البيانات والخدمات في السحابة".

يضمن هذا النموذج عدم وجود فجوات أو ثغرات في الحماية ناتجة عن افتراضات خاطئة حول من يملك مسؤولية عنصر أمني معين. ويختلف تقسيم هذه المسؤوليات بوضوح بين الشركاء بناءً على نموذج الخدمة السحابية المعتمد، ووفقاً للتفصيل التالي:

أ. البنية التحتية كخدمة

- مسؤولية المؤسسة الحكومية (عالية): تشمل نظام التشغيل، والتطبيقات، والبيانات، وتكوين الشبكة (جدران الحماية الافتراضية)، وإدارة الهوية والوصول، والتشفير.
- مسؤولية مزوّد الخدمة السحابية (منخفضة): تشمل البنية التحتية المادية، والخوادم، والتخزين، والشبكة الأساسية.

ب. المنصّة كخدمة

- مسؤولية المؤسسة الحكومية (متوسطة): تشمل التطبيقات، والبيانات، وإدارة الهوية والوصول، وتشفير البيانات.
- مسؤولية مزوّد الخدمة السحابية (متوسطة): تشمل نظام التشغيل، والبرامج الوسيطة، والخوادم، والتخزين، والشبكة الأساسية.

ج. البرمجيات كخدمة

- مسؤولية المؤسسة الحكومية (منخفضة): تقتصر بشكل أساسي على البيانات، وإدارة الهوية والوصول، وتكوينات المستخدم (مثل سياسات مشاركة الملفات).
- مسؤولية مزوّد الخدمة السحابية (عالية): تشمل التطبيقات، ونظام التشغيل، والبنية التحتية، والتخزين.

ويوضح الجدول (4) توزيع المسؤوليات الأمنية حسب نماذج الخدمة المختلفة.

الجدول 4: المسؤوليات الأمنية حسب نماذج الخدمة المختلفة

المكوّن الأمني	البنية التحتية كخدمة	المنصة كخدمة	البرمجيات كخدمة
البيانات	المستفيد	المستفيد	المستفيد
التطبيقات	المستفيد	المستفيد	المزود
نظام التشغيل والبرامج الوسيطة	المستفيد	المزود	المزود
الشبكة	المستفيد	المزود	المزود
الخوادم والتخزين	المزود	المزود	المزود
البنية التحتية المادية	المزود	المزود	المزود

القاعدة الأساسية هنا، أن مزوّد الخدمة السحابية مسؤول عن أمن السحابة، أي البنية التحتية الأساسية التي تشغّل الخدمة. أما المؤسسة الحكومية فهي مسؤولة عن كل ما يتعلق بالبيانات والتكوينات الخاصة بالخدمة، أي أنها هي المسؤولة عن الأمن في السحابة. وفي كل الأحوال، على المؤسسة الحكومية مراعاة النقاط التالية:

- البيانات والهوية هي مسؤولية المؤسسة دائماً أياً كان نموذج الخدمة. وتظل المؤسسة الحكومية هي الجهة المسؤولة الوحيدة عن أمن بياناتها وإدارة هوياتها وأذونات الوصول.
- تتأكد المؤسسة من تطبيق التشفير القوي على البيانات المصنفة (سرية ومقيدة) سواء كانت في حالة التخزين أو أثناء النقل، حتى عند اعتماد نموذج المنصة كخدمة أو البرمجيات كخدمة، ولا تكتفي بأن يتولى المزود جزءاً من التشفير.
- الامتثال للوائح الوطنية المتعلقة بالبيانات هو مسؤولية المؤسسة الحكومية التي يجب عليها التأكد من أن المزود يمتثل لمتطلباتها الأمنية.

6.5. إرشادات التعامل مع مزوّدي الخدمات السحابية

تتضمن هذه الإرشادات مجموعة من التوجيهات والمتطلبات الإلزامية التي ينبغي على الجهات الحكومية اتباعها بعناية عند اختيار مزوّدي الخدمات السحابية، وتقييمهم، والتعاقد معهم. يهدف هذا الإطار إلى ضمان تحقيق أعلى مستويات الأمن والامتثال القانوني والمالي.

تشمل المتطلبات الأساسية التأكد من التزام المزوّدين بمعايير الأمن والامتثال الوطنية، ووضع شروط تعاقدية واضحة تغطي سيادة البيانات ومواقع التخزين، وتحديد آليات الخروج الآمن والمنظم من الخدمة.

ولضمان انتقال آمن وممتثل إلى بيئة الحوسبة السحابية والحفاظ على استمرارية الأعمال، يجب على المؤسسات الحكومية اتباع الإرشادات التالية التي تركّز على الجوانب الرئيسية:

أ. جانب الأمن والامتثال

- تصنيف البيانات وتوطينها: يجب تصنيف البيانات بدقة (سرية، مقيدة، حساسة، عامة) لتحديد متطلبات الحماية لكل فئة. ويجب الالتزام بتوطين البيانات الحكومية السرية والمقيّدة داخل الحدود الجغرافية للدولة، وفقاً للسياسات الوطنية (مثل "السحابة أولاً").
- فهم المسؤولية المشتركة: يجب تحديد حدود مسؤولية المؤسسة ومسؤولية المزوّد بوضوح بناءً على نموذج المسؤولية المشتركة.
- الضوابط الأمنية: يجب اختيار مزوّد معتمد يلتزم بالحد الأدنى من متطلبات الأمن السيبراني المحدّدة في ضوابط الأمن السيبراني للحوسبة السحابية[6]. ويجب تطبيق التشفير "القوي" على كافة البيانات المصنّفة "سرية" أو "مقيدة" في حالة التخزين وأثناء النقل.

ب. جانب الحوكمة والإدارة

- اختيار المزوّد: من الضروري الاعتماد فقط على مزوّدي الخدمات السحابية الذين حصلوا على التراخيص والاعتمادات اللازمة من اللجنة العليا للتحوّل الرقمي. وينبغي طلب تقارير تدقيق من طرف ثالث للتحقق من التزام المزوّد بالضوابط الأمنية.
- إدارة الهوية والوصول: من الضروري الاحتفاظ بالسيطرة الكاملة على إدارة هويات المستخدمين وأذونات الوصول. وينبغي جعل المصادقة المتعددة العوامل إلزامية لجميع المستخدمين الذين لديهم حق الوصول إلى البيانات الحساسة.
- التعافي من الكوارث واستمرارية الأعمال: ينبغي وضع خطة تعافي من الكوارث تتضمن سيناريوهات محدّدة للتعامل مع انقطاع الخدمة السحابية واستعادة البيانات الحيوية.

ج. الجوانب التعاقدية والقانونية

- حقوق الملكية والشفافية: ينبغي أن ينصّ العقد بوضوح على أن الجهة الحكومية هي المالك الوحيد للبيانات، وأن المزوّد يعمل كمعالج للبيانات فقط. ومن الضروري طلب الشفافية في تحديد مكان تخزين البيانات (التوطين الجغرافي) ومعرفة أي أطراف ثالثة قد تشارك في المعالجة.
- الاستجابة للحوادث: في العقد ينبغي تحديد مسؤوليات المزوّد في حالة وقوع حادث أمني، بما في ذلك الإجراءات الفورية والمدة الزمنية القصوى للإبلاغ عن الحادث للجهة الحكومية.
- استراتيجية الخروج: ينبغي وضع خطة خروج واضحة ومفصّلة ضمن العقد، تضمن القدرة على استرداد جميع البيانات بتنسيق قابل للاستخدام، وتدمير البيانات المتبقية لدى المزود بشكل آمن وموثق عند إنهاء الخدمة.

6. الرصد والتقييم

تتولى اللجنة الوطنية للحوسبة السحابية الإشراف بشكل عام على مدى التقدّم في تنفيذ السياسة في حين تقوم الإدارات المختصة بإعداد التقارير كل في ما يخصه لعرضها على اللجنة الوطنية. وتبدأ العملية من فرق العمل التي تجمع المؤشرات الفنية والتقنية بشكل مباشر من المشاريع الميدانية وتحيلها دورياً للقطاعات الحكومية المعنية، التي بدورها تقيّم مدى تقدم القطاع نحو تحقيق أهدافه القطاعية المحدّدة وتعدّ تقريراً شاملاً عن سير خطة عمل القطاع. كما ترصد وحدة الخدمات السحابية أداء المنصّات والخدمات السحابية المشتركة، وتقيّم مدى فعالية الدعم الفني المقدّم، وترفع تقارير حول حالة التكامل بين الأنظمة الحكومية.

وتتولى اللجنة الوطنية للحوسبة السحابية استقبال التقارير الموحّدة من القطاعات والإدارات، وتقوم بدمج وتحليل هذه البيانات لمعرفة الأداء الكلي مقابل الأهداف الاستراتيجية والغايات العددية، وتحدّد الانحرافات والمخاطر، وتقترح الإجراءات التصحيحية والتوصيات الاستراتيجية اللازمة. يجري اتخاذ الإجراءات التصحيحية على مستوى اللجنة الوطنية التي ترفع التوصيات الاستراتيجية إلى اللجنة العليا للتحوّل الرقمي لاتخاذ قرارات إشرافية عليا.

وفي ما يلي أهم المؤشرات الممكن استخدامها لتقييم وقياس الأداء موزّعة على محاور السياسة المختلفة، بالإضافة إلى تقييم مدى تحقيق الأهداف الكمية خلال مراحل التنفيذ المختلفة والمجالات ذات العلاقة:

- نسبة الخدمات الحكومية المنشورة على السحابة.
- معدل تهجير/نقل التطبيقات إلى السحابة.
- مدى توافر وسهولة الوصول إلى الخدمات والمعلومات الحكومية.
- نسبة البيانات المخزّنة محلياً.
- نسبة البيانات الآمنة والمشفّرة.
- مدى الالتزام بمعايير الأمان على السحابة.
- مستوى الالتزام بسيادة البيانات.
- مستوى الامتثال التنظيمي.
- عدد الكوادر المدربة/المُؤهلة سنوياً.
- عدد مراكز التدريب السحابي الوطنية.
- معدل التوظيف في المجالات السحابية.
- نسبة الخفض في كلفة استخدام تكنولوجيا المعلومات.

7. الخطة الإعلامية

تأتي هذه الخطة الإعلامية دعماً لتنفيذ السياسة الوطنية للحوسبة السحابية، الهادفة إلى رفع كفاءة الخدمات الحكومية، وضمان حماية البيانات الوطنية وسيادتها. وتهدف الخطة إلى توعية جميع المستهدفين بأهمية الحوسبة السحابية، ومنافعها الاقتصادية والتقنية، وإجراءات الأمن والحوكمة المصاحبة لها. وتحرص على إيصال الرسائل الإعلامية الأساسية التالية لأصحاب المصلحة:

- "الحوسبة السحابية ركيزة التحوّل الرقمي الوطني"
- "البيانات الوطنية مسؤولية مشتركة، وحمايتها تبدأ من الثقة بالسحابة الوطنية"
- "السحابة الوطنية تعني كفاءة أعلى، أماناً أقوى، وسيادة رقمية كاملة"

إن نجاح السياسة الوطنية للحوسبة السحابية لا يتحقق بالتشريعات والتنفيذ فقط، بل عبر تواصل فعّال وشامل يضمن الوعي والثقة والتفاعل من جميع الأطراف. والخطة الإعلامية المقترحة تمثل أداة استراتيجية لتحقيق هذا الهدف وتعزّز السيادة الرقمية والتحوّل الرقمي المستدام وذلك من خلال البنود التالية:

- الإعلان الرسمي عن السياسة الوطنية للحوسبة السحابية.
- نشر بيان صحفي وتقرير موجز يشرح أهداف السياسة وأثرها الوطني.
- تنظيم حملات إعلامية مكثفة على القنوات الرسمية ومواقع التواصل الاجتماعي.
- إنتاج محتوى مرئي توضيحي مثل فيديوهات قصيرة.
- إقامة ورش عمل توعوية ولاستقصاء رأي المستهدفين.
- عقد دورات تدريبية لموظفي الجهات الحكومية حول معايير الأمن السحابي والسيادة الرقمية.
- إطلاق منصة وطنية لتلقي الملاحظات والاستفسارات.
- إبراز قصص نجاح لمشروعات سحابية وطنية.
- نشر تقارير دورية عن التقدم في تطبيق السياسة الوطنية.

الجدول الزمني

يمكن تنفيذ الخطة الإعلامية خلال 12 شهراً على أن تقسم إلى ثلاث مراحل زمنية (3-6-3 أشهر)، على أن تغطي كل مرحلة زمنية ثلاثة عناصر على التوالي من الأنشطة السالفة الذكر.

8. إدارة المخاطر

قد يواجه أي مسعى لتحقيق تطلعات مستقبلية واعدة تحديات ومصاعب تهدّد مسيرة نجاحه وتعيق تقدمه نحو تحقيق الأهداف المرجوة. يأتي على رأسها، تحديات التكنولوجيا الرقمية، ونقص الموارد المالية والتمويل، وضعف البنية التحتية الرقمية، وقلة الكوادر البشرية المؤهلة. ولمعالجة هذه التحديات، ينبغي اعتماد خطة شاملة لإدارة المخاطر. وتتضمن هذه الخطة: تحديد المخاطر وبيان أثرها على تنفيذ السياسة ومستوى الخطر ثم الإجراءات المقترحة لمواجهته.

الجدول 5: خطة إدارة المخاطر

المخاطر	الأثر	مستوى الخطر	الإجراءات المقترحة
السيادة	فقدان أو تسرب البيانات الحساسة	مرتفع	• ضمان حفظ البيانات الحساسة محلياً • تطبيق ضوابط تصنيف البيانات • اتفاقيات صارمة مع المزودين
الأمان	• اختراق الشبكة • حجب الخدمة	مرتفع	• مراقبة مستمرة لرصد الحوادث • اختبارات اختراق دورية • سياسات تشفير قوية
الكفاءة/ التكلفة	• إعاقة تحقيق الأهداف • عرقلة التنفيذ وزيادة التكاليف • تفاوت الموارد المادية	متوسط	• تقييم مستمر للأداء والتكاليف • المراجعة الدورية لعقود المزودين
الاعتماد على مزوّد واحد	• احتمال توقف كافة الخدمات في حال تعرضه لأي مشكلة تقنية • الهيمنة على التعامل مع الجهات الحكومية	متوسط	• اعتماد استراتيجية للخروج • استخدام منصات مفتوحة المصدر • استخدام أدوات إدارة متعددة السُحُب (هجينة)
الامتثال والحوكمة	• فقدان ثقة الشركاء • تدني سمعة المؤسسة • دفع غرامات كبيرة	مرتفع	• الالتزام بإطار حوكمة البيانات • توثيق سياسات الخصوصية • توعية الموظفين بأنظمة وسياسات حماية البيانات
الموارد البشرية	• عزوف المهندسين الأكفاء عن العمل للمؤسسات الحكومية • ضعف الرواتب الحكومية	مرتفع	• اعتماد نموذج عمل منافس للقطاع الخاص

9. المراجع

Council Regulation (EU) 2016/679 of the European Parliament and of the Council11 .[2016] OJ L119/1

2. الهيئة العامة للمعلومات، السياسة الوطنية لحوكمة البيانات الحكومية، 2022 . https://www.gia.gov.ly/wp-content/uploads/2023/03/National-policy-for-government-data-governance-1.1-2022.pdf.

3. الهيئة الوطنية لأمن وسلامة المعلومات، سياسة حماية البيانات، 2020. https://nissa.gov.ly/main-services/data-protection-policy/#data-protection-police.

4. الهيئة الوطنية لأمن وسلامة المعلومات، سياسة كلمة السر أو المرور، 2020. https://nissa.gov.ly/main-services/policies/#password-police.

5. الهيئة الوطنية لأمن وسلامة المعلومات، سياسة تصنيف المعلومات، 2020. https://nissa.gov.ly/main-services/data-protection-policy/#information_classification_police.

الحواشي

1. Council Regulation (EU) 2016/679.
2. السياسة الوطنية لحوكمة البيانات الحكومية، الصادرة عن الهيئة العامة المعلومات.
3. سياسة حماية البيانات، الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات.
4. سياسة تصنيف المعلومات، الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات.
5. المرجع السابق.
6. سياسة حماية البيانات، الصادرة عن الهيئة الوطنية لأمن وسلامة المعلومات.



2600106A