شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

مدل مرجع امنیت

نسخه ۱,۰ – مرداد ماه ۱۳۹۶

پیشگفتار

این سند در راستای ارائه مدل مرجع امنیت، به عنوان یکی از شش مدل مرجع چارچوب معماری سازمانی ایران، تهیه و منتشر می‌شود. این مدل دربردارنده طبقه‌بندی جامعی از حوزه‌های امنیت، اصول امنیتی پایه، مکانیزم‌ها، استانداردها و سیاست‌های امنیتی در جهت فراهم کردن امنیت برای تمامی ذی‌نفعان می‌باشد.

استفاده از مدل مرجع امنیت در سطح ملی (دولت و کلیه دستگاه‌های اجرایی) باعث ایجاد یک چارچوب و ساختار مشترک برای امنیت می‌شود و نیز دایره‌المعارفی مشترک از سرویس‌ها و استانداردهای امنیتی فراهم می‌کند که همکاری و تعامل‌پذیری بین دستگاه‌های مختلف را تسهیل می‌نماید. با استفاده از مدل مرجع امنیت، کلیه دستگاه‌های اجرایی و دولتی نیازی به بررسی مکرر استانداردها جهت انتخاب نداشته و در وقت و هزینه تحلیل‌ها صرفه‌جویی قابل توجهی خواهد شد.

این سند، تنها به تشریح یکی از شش مدل مرجع چارچوب معماری سازمانی ایران می‌پردازد و مخاطبان باید سایر اسناد مربوط به چارچوب را نیز مطالعه کرده و در کنار این سند مورد استفاده قرار دهند.

از آنجا که محتوای این سند حاصل اولین تجربه تدوین مدل مرجع امنیت در دولت جمهوری اسلامی ایران است، احتمال می‌رود اشکالات و نواقصی در این سند دیده شود که امید است با همکاری و مشارکت صاحب‌نظران امر، تکمیل شود، لذا از مخاطبان درخواست می‌شود نظرات و پیشنهادات اصلاحی خود را از طریق پست الکترونیکی info@ieaf.ir به اطلاع متولیان طرح برسانند.

توجه به این نکته ضروری است که امروزه زیرساخت فناوری اطلاعات سازمان‌ها در محیطی قرار گرفته که به‌طور فزاینده بر تعداد دشمنان و مهاجمانی که علاقه‌مند به حضور مستمر، مطمئن و سودمند سیستم‌های کامپیوتری نمی‌باشند، افزوده می‌گردد. حملات، سیری کاملا صعودی داشته و می‌بایست نگاه پویا و زنده به مقوله امنیت داشت و از نگاه مقطعی و روزمره پرهیز نماییم.

از این رو این سند در طی زمان پشتیبانی و به‌روزرسانی خواهد شد و ایستا بودن آن برای رفع مشکلات و تهدیدات کارایی نخواهد داشت.

جهت اطلاع و دریافت اسناد فنی، رهنمون‌ها و مثال‌ها، ضوابط قانونی، مدل‌های مرجع و اطلاع از آخرین تغییرات مربوط به چارچوب معماری سازمانی ایران، به پورتال www.IEAF.ir مراجعه شود.

ارکان اجرای طرح تدوین چارچوب معماری مرجع امنیت	
کارفرمای طرح	شورای اجرایی(عالی) فناوری اطلاعات کشور –کمیسیون توسعه دولت الکترونیکی
مدیریت طرح	معاونت دولت الکترونیکی سازمان فناوری اطلاعات ایران
ناظر طرح	مدیریت امور اصلاح ساختار و توسعه دولت الکترونیک سازمان امور اداری و استخدامی کشور
مشاور(مجری)	آزمایشگاه مرجع معماری سازمانی سرویس گرا دانشگاه شهید بهشتی آزمایشگاه امنیت پیشرفته فناوری اطلاعات و ارتباطات دانشگاه بین‌المللی امام رضا (علیه‌السلام)

اعضای تیم مدیریت و نظارت طرح	
مدیر ارشد طرح	جناب آقای نصرالله جهانگرد جناب آقای رضا باقری اصل جناب آقای سید هادی سجادی
مدیریت فنی و اجرایی	جناب آقای مازیار مباشری جناب آقای تسلیمی سرکار خانم ساناز غفارزادگان سرکار خانم فائزه حسینی سرکار خانم پریسا صیادی
نظارت بر طرح	جناب آقای علی رضا شاه پری جناب آقای محمدرضا زینالدینی

اعضای تیم تدوین مدل مرجع امنیت (مجری)	
راهبر و مدیر ارشد پروژه	جناب آقای فریدون شمس علیئی جناب آقای حمیدرضا محروقی
مدیر فنی و اجرایی پروژه	جناب آقای سبحان علی‌آبادی
تیم فنی و کارشناسی	سرکار خانم محیا خیرخواه سرکار خانم مهناز زارع جناب آقای احسان میر سرکار خانم راضیه قوامی سرکار خانم فرشته کهندل سرکار خانم زهره نیکزاد سرکار خانم ندا خسروی سرکار خانم فائزه خورسند سرکار خانم فهیمه شریعتی سرکار خانم آسیه سلیمانی سرکار خانم نازنین میریونسی جناب آقای مرتضی ارجمند سرکار خانم افسانه چهکندی سرکار خانم مریم ترابی

فهرست

۱- معرفی مدل مرجع امنیت ۲

۱-۱- مقدمه ۲

۱-۲- تعریف مدل مرجع امنیت ۲

۱-۳- امنیت در معماری سازمانی ۳

۱-۴- ضرورت تدوین مدل مرجع امنیت ۵

۱-۵- جایگاه مدل در چارچوب معماری سازمانی ایران ۶

۲- تشریح چارچوب معماری مرجع امنیت ۹

۲-۱- جمع‌آوری الزامات و نیازمندی‌ها ۱۰

۲-۲- تدوین اصول، استراتژی و سیاست ۱۲

۲-۳- تجزیه و تحلیل (درک) امنیتی ۱۳

۲-۴- تحلیل و ارزیابی ریسک ۱۴

۲-۴-۱- مدیریت ریسک ۱۶

۲-۵- حوزه‌های اصلی امنیت در مدل مرجع ۲۸

۲-۵-۱- افراد ۲۸

۲-۵-۲- داده ۳۰

۲-۵-۳- نرم‌افزار ۳۲

۲-۵-۴- زیرساخت ۳۳

۲-۶-کنترل‌های امنیتی ۳۵

۲-۶-۱- اصول پایه امنیت ۳۶

۲-۶-۲- زیرساخت و سرویس‌های امنیتی ۳۷

۲-۶-۳- مؤلفه‌های اصول پایه امنیت ۳۹

۲-۷- ارتباط مدل مرجع امنیت با سایرمدل‌های مرجع ۷۴

۲-۸- مدل بلوغ امنیت ۷۹

۳- اصول طراحی معماری امنیتی ۸۲

۴- انواع چارچوب‌های معماری امنیتی ۸۵

۴-۱- مدل امنیتی SABSA ۸۶

۴-۲- معماری امنیتی باز (OSA) ۸۶
۴-۳- معماری امنیت فراسازمانی باز (O-ESA) ۸۷
۴-۴- معماری امنیت اطلاعات فراسازمانی گارتنر ۸۷
۴-۵- معماری فراسازمانی فدرال ۸۸
۴-۶- مدل TOGAF 9.1 ..... ۸۸
۴-۷- مدل معماری فراسازمانی NIST ۸۹
۴-۸- چارچوب معماری فراسازمانی خزانه‌داری ۹۰
پیوست شماره ۱: سازمان‌های امنیت فضای تبادل اطلاعات و استانداردهای امنیتی ملی ۹۱
پیوست شماره ۲: سازمان‌ها و استانداردهای امنیتی بین‌المللی ۱۰۷
پیوست شماره ۳: لغت‌نامه ۱۴۵

فهرست اشکال

شکل (۱-۱): جایگاه مدل مرجع امنیت در چارچوب معماری سازمانی ایران ۷
شکل (۲-۱): چارچوب مدل مرجع امنیت ۱۰
شکل (۲- ۲): چرخه مدیریت ریسک..... ۱۶
شکل (۲- ۳): زیرمؤلفه‌های مدیریت کنترل و فرمان..... ۱۸
شکل (۲- ۴): زیرمؤلفه‌های مدیریت سیاست‌های امنیتی ۲۰
شکل (۲- ۵): زیرمؤلفه‌های ارزیابی ریسک و تطابق‌پذیری ۲۴
شکل (۲- ۶): زیرساخت و سرویس‌های امنیتی..... ۳۷
شکل (۲- ۷): نمای کلی مؤلفه و زیرمؤلفه‌های اصول پایه امنیت ۴۰
شکل (۲- ۸): زیرمؤلفه‌های مدیریت هویت، دسترسی و مجوز به همراه زیرساخت و سرویس‌های امنیتی مربوطه..... ۴۱
شکل (۲- ۹): زیرمؤلفه‌های مدیریت حافظت از داده و اطلاعات به همراه زیرساخت و سرویس‌های امنیتی مربوطه ۴۷
شکل (۲- ۱۰): زیرمؤلفه‌های تضمین نرم‌افزار، سیستم و سرویس به همراه زیرساخت و سرویس‌های امنیتی مربوطه ۵۶
شکل (۲- ۱۱): زیرمؤلفه‌های مدیریت آسیب پذیری و تهدید به همراه مؤلفه‌های زیرساخت و سرویس‌های امنیتی مربوطه ۶۱
شکل (۲- ۱۲): زیرمؤلفه‌های مدیریت سرویس فناوری اطلاعات به همراه مؤلفه‌های زیرساخت و سرویس‌های امنیتی مربوطه ۶۷
شکل (۲- ۱۳): زیرمؤلفه‌های مدیریت دارایی فیزیکی به همراه مؤلفه‌های زیرساخت و سرویس‌های امنیتی مربوطه..... ۷۰
شکل (۲- ۱۴): ارتباط سایر مدل‌های مرجع با مدل مرجع امنیت ۷۳
شکل (۲- ۱۵): ارتباط سایر مدل‌های مرجع با مدل مرجع امنیت ۷۷
شکل (۲- ۱۶): ارتباط مدل مرجع امنیت با سایر مدل‌های مرجع ۷۸
شکل (۲- ۱۷): مدل بلوغ امنیت..... ۸۰

فهرست جداول

جدول (۲- ۱): لایه تجزیه و تحلیل (درک) امنیتی ۱۴
جدول (۲- ۲): حوزه افراد..... ۳۱
جدول (۲- ۳): حوزه داده ۳۳
جدول (۲- ۴): حوزه نرم‌افزار ۳۴
جدول (۲- ۵): حوزه زیرساخت ۳۶

فصل اول

معرفی مدل مرجع امنیت

۱- معرفی مدل مرجع امنیت

محتوای این فصل به معرفی تعاریف، مفاهیم، محدوده و کاربردهای مدل مرجع امنیت اختصاص دارد.

۱-۱- مقدمه

روش‌های توسعه معماری، ابزاری در دستان مسئولین امنیت هستند تا در جهت ایجاد بهترین روش و قابلیت‌های امنیتی خاص سازمان مورد استفاده قرار گیرند. این راهنما برای کمک به طراحان فراسازمانی و مسئولین امنیت به منظور اجتناب از نادیده گرفته شدن ملاحظات امنیتی حیاتی در نظر گرفته شده است. اغلب، معماری امنیت به عنوان یک حوزه معماری جداگانه در داخل معماری فراسازمانی تلقی و بحث می‌شود در حالی که نیازمند این است که به طور کامل در آن یکپارچه شود. تمرکز طراح امنیت بر اعمال سیاست‌های امنیتی سازمان بدون حذف یا کاستن از ارزش آن‌ها می‌باشد.

۱-۲- تعریف مدل مرجع امنیت

"مدل مرجع امنیت"[1] به‌عنوان یکی از شش مدل مرجع "چارچوب معماری سازمانی ایران"[2] یک راهنمای کلان ملی را در اختیار کلیه دستگاه‌های دولتی و بخش‌های دولت الکترونیک قرار می‌دهد. مدل مرجع امنیت تنها مدلی است که با همه مدل‌های دیگر ارتباط دارد، اگرچه از نظر فنی، بیشترین وابستگی را با مدل مرجع فناوری دارد. در گذشته موضوع امنیت بیشتر در لایه فناوری مورد بحث قرار می‌گرفت تا اینکه به تدریج با توجه به اهمیت موضوع امنیت در قالب یک لایه جداگانه مورد پذیرش قرار گرفت.

یک معماری امنیتی دارای ساختاری از مؤلفه‌های سازمانی، مفهومی، منطقی و فیزیکی می‌باشد که به روشی منسجم به منظور دستیابی و حفظ وضعیت ریسک، تعامل دارند. در واقع معماری امنیتی محرک و فراهم‌کننده رفتار امن، ایمن و قابل اعتماد می‌باشد و به تمامی ریسک‌های سازمان رسیدگی می‌نماید.

[1] Security Reference Model
[2] Iran Enterprise Architecture Framework (IEAF)

هدف معماری امنیتی فراسازمانی ارائه یک رویکرد جامع برای امنیت در سطح فراسازمانی و ارائه راهنمایی‌های مؤثر و کارامد برای تمامی اهداف امنیتی در داخل سازمان می‌باشد.

به طور کلی معماری امنیت دارای مشخصات زیر می‌باشد:

- متدولوژی امنیتی مجزای خود را دارد.
- دیدها و نقطه نظرات مجزا و گسسته خود را ایجاد می‌کند.
- یک روش واحد برای معماری و مدیریت الزامات در سراسر سازمان را ارائه می‌نماید.
- ساختار، انسجام و ارتباط را حفظ می‌نماید.
- یک زبان مشترک برای امنیت اطلاعات را در داخل سازمان ارائه می‌کند.
- در تمامی سطوح سازمان از کسب و کار تا تکنولوژی عمل می‌نماید.

۳-۱- امنیت در معماری سازمانی

نگرانی‌های امنیتی در سراسر حوزه‌های معماری و در تمام مراحل توسعه آن‌ها گسترده شده است. از آنجایی که امنیت زیرساختی است که به ندرت در عملیات کسب‌وکار مشاهده می‌شود، به صورت لایه‌ای جداگانه نامگذاری می‌شود. هدف اصلی آن محافظت از سیستم‌ها و دارایی‌های اطلاعاتی سازمان می‌باشد. اغلب ماهیت امنیت در فراسازمان این گونه است که اگر هیچ اتفاقی نیفتد که برای کاربر یا دیگر ناظران قابل مشاهده باشد و یا هیچ خسارت یا آسیبی برای سازمان به وجود نیاید، امنیت موفق تلقی می‌شود. به عنوان مثال، داده‌های درون یک پایگاه داده سوابق مشتری فاش نشده یا آسیب نبینند.

دیدگاه معماری امنیت فراسازمانی بخش‌های سازنده[1] منحصربه‌فرد و رابط‌های خودش را دارد. این عناصر منحصربه‌فرد امنیتی باید با سیستم‌های کسب‌وکار به شیوه‌ای متعادل و مقرون به صرفه تعامل داشته باشند تا سیاست‌های امنیتی فراسازمان را حفظ کرده و در عین حال در عملیات و عملکرد سیستم اختلال ایجاد نکنند. این کار برای برنامه‌ریزی جهت اجرا و پیاده‌سازی عملیات امنیتی خاص در معماری هدف و در چرخه

[1] Building Block

توسعه به منظور جلوگیری از عملیات پرهزینه و دوباره‌کاری، مقرون به صرفه‌تر و مؤثرتر می‌باشد؛ زیرا بخش‌های سازنده مورد نیاز برای امنیت در طول استقرار و توسعه سیستم‌ها، اضافه یا استفاده نشده‌اند. رویکرد طراح امنیت نه تنها جریان هنجار (طبیعی) برنامه‌کاربردی را بلکه جریان‌های غیرنرمال، حالات شکست و راه‌هایی که سیستم‌ها و برنامه‌ها می‌توانند دچار وقفه و یا شکست (خرابی) شوند را نیز درنظر می‌گیرد. تمام گروه‌های ذی‌نفع در فراسازمان نگرانی‌های امنیتی خواهند داشت و مطلوب آن است که در اسرع وقت یک طراح امنیت به سازمان‌ها اضافه شود.

به‌طور کلی زمینه‌های نگرانی‌های امنیتی عبارت است از:

- **احرازهویت:** اثبات هویت یک شخص یا موجودیت مرتبط با سازمان یا سیستم به روش‌های مختلف.
- **مجوزدهی**: تعریف و اجرای قابلیت‌های اجازه داده شده به یک شخص یا موجودیت دارای هویت.
- **ممیزی:** توانایی ارائه داده‌های قانونی که استفاده از سیستم‌ها را مطابق با سیاست‌های امنیتی وضع شده تصدیق می‌کند.
- **اطمینان:** توانایی آزمایش و اثبات این که معماری فراسازمانی، ویژگی‌های امنیتی موردنیاز برای حمایت از سیاست‌های امنیتی وضع شده را دارند.
- **دسترس‌پذیری:** توانایی سازمان برای ارائه بدون وقفه سرویس و خدمات با وجود حوادث غیرطبیعی و یا رویدادهای مخرب.
- **حافظت از دارایی‌ها:** حفاظت از اطلاعات در برابر گم شدن (از دست دادن) یا افشای غیرعمد و حفاظت از منابع در برابر استفاده غیرمجاز و ناخواسته.
- **مدیریت:** توانایی تدوین و تغییر سیاست‌های امنیتی و نحوه پیاده‌سازی آن‌ها در سازمان و تغییر اشخاص یا موجودیت‌های مرتبط با سامانه‌ها.
- **مدیریت ریسک:** نگرش و تحمل سازمان در برابر خطر و ریسک. (این مفهوم مدیریت ریسک با مفهومی که در بازارهای مالی و غیره وجود دارد، متفاوت است).

۴-۱- ضرورت تدوین مدل مرجع امنیت

بر اساس بررسی‌های انجام شده در اکثر سازمان‌های موجود، امنیت معمولاً براساس یک سری اقدامات واکنشی طراحی، جمع‌آوری و پیاده‌سازی می‌شود؛ به این صورت که یک نیازمندی شناخته شده و جزئیات آن توسعه داده شده و راه‌حلی برای مقابله با یک وضعیت خاص ارائه می‌شود. در این فرایند هیچ فرصتی برای در نظر گرفتن ابعاد استراتژیک موضوع داده نمی‌شود و نتیجه این نوع رفتار، این خواهد بود که سازمان براساس یک سری راه‌حل‌های فنی پیچیده که برمبنای تجربیات فردی ارائه شده، ساخته می‌شود. همچنین هریک از این راه‌حل‌ها به طور مستقل طراحی و توسعه داده شده‌اند و هیچ تضمینی برای اینکه مجموعه این راه‌حل‌ها با هم سازگاری و همکاری متقابل داشته باشند، وجود ندارد. معمولاً تحلیلی بر هزینه‌های بلندمدت، به ویژه هزینه‌های عملیاتی که سهم زیادی از هزینه‌های کل سازمان را در بر می‌گیرد، انجام نمی‌شود و همچنین استراتژی که بتواند از اهداف کلی سازمان حمایت کند وجود ندارد.

یک روش برای پرهیز از مشکلات بوجود آمده از تکه‌تکه شدن بخش‌های مختلف سازمان، توسعه یک معماری امنیتی است که براساس فعالیت سازمان طراحی شده باشد؛ همچنین معماری که توصیفی از روابط بین روال‌های فنی و راه‌حل‌های ارائه شده برای پشتیبانی از نیازهای بلندمدت سازمان را به صورت قابل فهم و شفاف ارائه کند. اگر معماری انتخاب شده موفق باشد، یک چارچوب منطقی برای تصمیم‌گیری براساس مجموعه‌ای از راه‌حل‌های امنیتی ارائه شده مهیا خواهد شد.

ضوابط تصمیم‌گیری باید از یک درک کامل برآمده از نیازهای سازمان مشتق شده باشد که این ضوابط شامل موارد ذیل می‌باشد:

- نیاز به کاهش هزینه
- پیمانه‌ای بودن[1]
- مقیاس‌پذیری

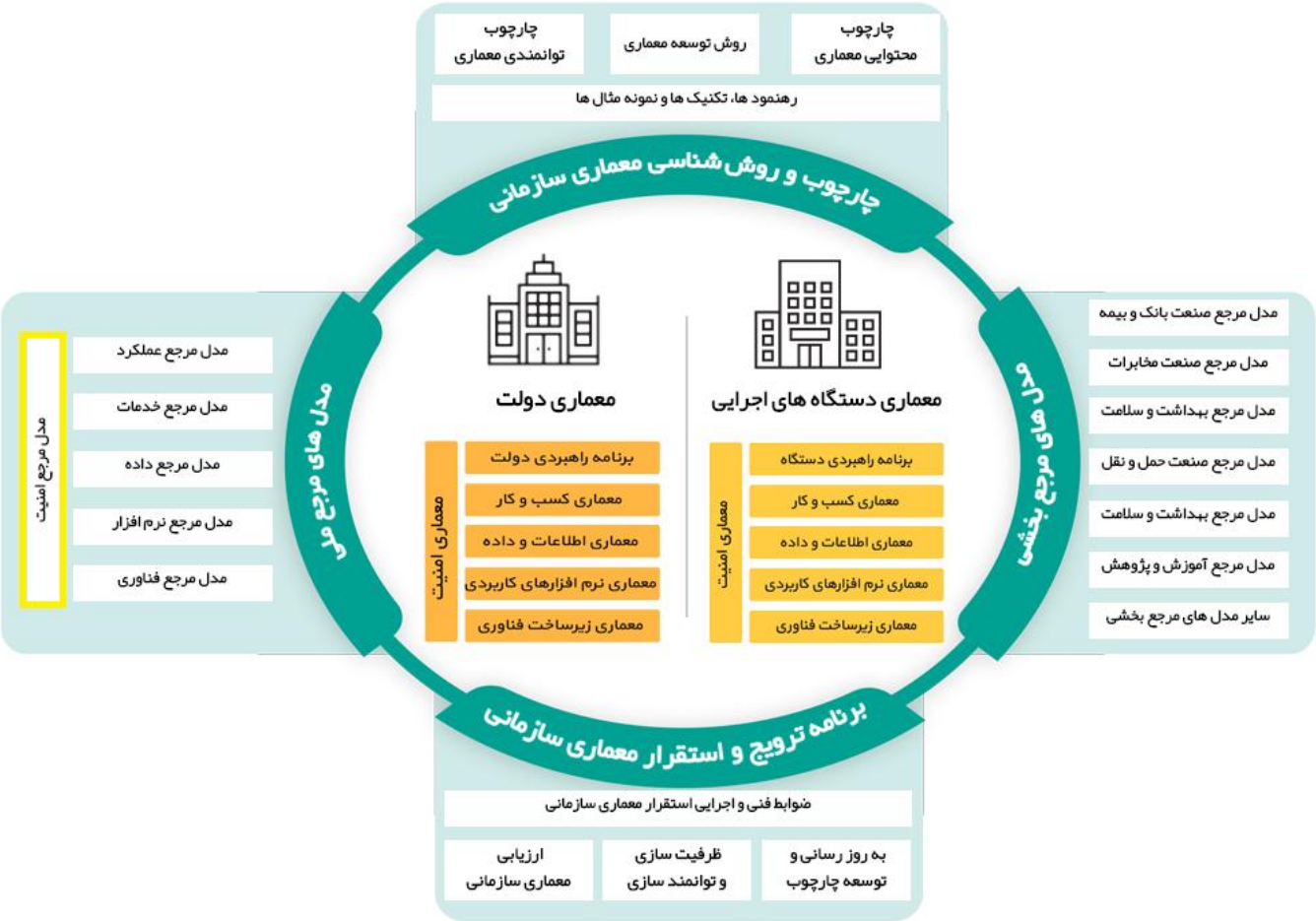
[1] Madularity

- سهولت در استفاده مجدد مؤلفه‌ها
- قابلیت عملکرد
- قابلیت پیاده‌سازی و استفاده در سازمان
- قابلیت عملکرد هم به‌صورت داخلی و هم به‌صورت خارجی
- قابلیت یکپارچگی با معماری فناوری اطلاعات سازمان و سیستم‌های قبلی

امنیت سازمان در برگیرنده امنیت اطلاعات، تداوم فعالیت سازمان، امنیت فیزیکی و محیطی سازمان می‌باشد.

۱-۵- جایگاه مدل در چارچوب معماری سازمانی ایران

چارچوب معماری سازمانی ایران شامل چهار مؤلفه (جزء) اصلی "چارچوب و متدولوژی"، "مدل‌های مرجع ملی"، "مدل‌های مرجع بخشی" و "برنامه ترویج و استقرار" می‌شود که در شکل (۱-۱) نشان داده شده است. همان‌طور که در شکل مشخص است، مدل مرجع امنیت که در این گزارش به صورت تفصیلی تشریح می‌شود، یکی از شش مدل مرجع از چارچوب معماری سازمانی ایران است که در طول سایر مدل‌های مرجع قرار گرفته و ورودی خود را از آن‌ها می‌گیرد و اگرچه تنها مدلی است که با همه مدل‌های دیگر ارتباط دارد، اما بیشترین وابستگی را با مدل مرجع فناوری دارد.



شکل (۱-۱): جایگاه مدل مرجع امنیت در چارچوب معماری سازمانی ایران

فصل دوم

تشریح مدل مرجع امنیت

۲- تشریح چارچوب معماری مرجع امنیت

این مدل براساس چندین سال بررسی و تحلیل نمونه مدل‌های مرجع امنیت و مدل‌های مرجع معماری در دیگر کشورها و انطباق آن با نیازهای کشور طراحی و سفارشی‌سازی شده است و تضمین می‌کند تمام جنبه‌های ضروری امنیت فناوری اطلاعات هنگام استفاده از یک رویکرد جامع برای امنیت مبتنی بر کسب‌وکار به طور مناسب پوشش داده می‌شود. این مدل وابسته به فروشنده، محصول و راه‌حل خاصی نبوده و با استفاده از تعاریف صنعتی پذیرفته شده و متداول تدوین شده است.

مدل مرجع امنیت شامل چهار حوزه امنیتی اصلی و چهار لایه پشتیبان مطابق با شکل (۱-۲) می‌باشد. مدل پیشنهادی پس از بررسی مدل‌های مرجع امنیتی مختلف به‌گونه‌ای ارائه شده است که تمامی زمینه‌های امنیت را در یک سازمان پوشش می‌دهد.

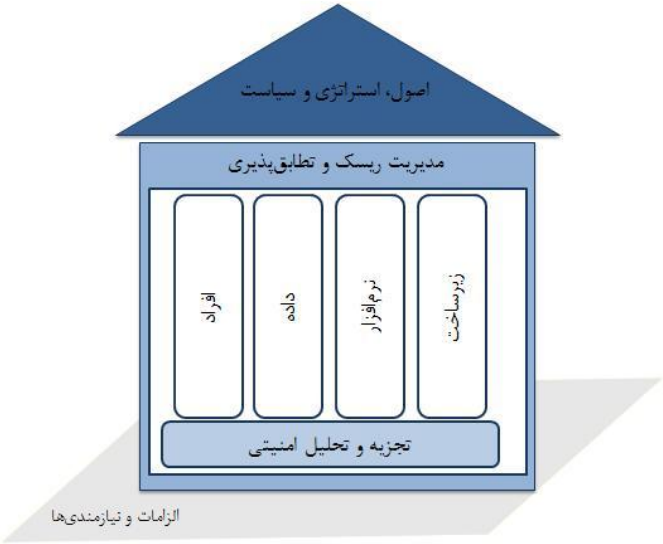
حوزه‌های اصلی امنیت در مدل مرجع امنیت عبارتند از:

- افراد
- داده
- نرم‌افزار
- زیرساخت

و چهار لایه پشتیبان عبارتند از:

- الزامات و نیازمندی‌ها
- اصول، استراتژی و سیاست
- تجزیه و تحلیل (درک) امنیتی
- مدیریت ریسک

در ادامه قسمت‌های مختلف مدل شرح داده شده است.



شکل (۲-۱): چارچوب مدل مرجع امنیت

۱-۲- جمع‌آوری الزامات و نیازمندی‌ها

این مرحله برای اطمینان از این که الزامات امنیتی در مراحل معماری فراسازمانی پوشش داده می‌شوند، مناسب است. هدف این مرحله، جمع‌آوری، ارزیابی و تحلیل الزامات کسب‌وکار (تحلیل ریسک‌های کسب‌وکار شامل تحلیل تهدیدات بر روی دارایی‌های کسب‌وکار و غیره)، ساختار سازمانی پرسنل، شرکا، بودجه، محدودیت‌های فنی، وابستگی به زمان و سایر موارد مربوطه می‌باشد. در ادامه مواردی که باید در جمع‌آوری و بررسی نیازمندی‌ها مورد توجه قرار گیرد، بیان می‌شود.

تعیین محدوده سازمان‌های فراسازمانی تحت تأثیر معماری امنیت از جمله مواردی است که باید به آن توجه شود:

- شناسایی سازمان یا واحدهای اصلی[1]- آن دسته از سازمان‌ها یا واحدهایی که بیشتر تحت تأثیر قرار می‌گیرند و بیشترین بهره را از کار امنیت به دست می‌آورند.

[1] Core Enterprise

- شناسایی سازمان یا واحدهای نرم[1]- سازمان یا واحدهایی که به واسطه کار با واحدهای اصلی با تغییراتی در قابلیت‌های خود مواجه می‌شوند و به صورت مستقیم تحت تأثیر قرار نمی‌گیرند.
- شناسایی سازمان یا واحدهای گسترده[2]- آن دسته از واحدهای خارج از سازمان مورد نظر که نیاز به بهبود معماری امنیت خود جهت ایجاد قابلیت همکاری خواهند داشت.
- شناسایی جوامع درگیر (سازمان‌ها)[3]- آن دسته از ذی‌نفعان که تحت تأثیر قابلیت‌های امنیتی قرار خواهند گرفت.

تعیین و مستند کردن موارد حیاتی و بحرانی سیستم، بحرانی از لحاظ ایمنی/ بحرانی از لحاظ مأموریت/ غیربحرانی[4]، مورد دیگری است که در زمان شناسایی نیازمندی‌ها باید به آن توجه کرد. سیستم‌های حیاتی از لحاظ ایمنی در صورت شکست یا نقصی به صورت مستقیم در معرض خطر قرار دارند. در سیستم‌های حیاتی از لحاظ مأموریت، در صورت شکست، سرمایه، سهم بازار یا حقوق صاحبان سهام در معرض خطر قرار می‌گیرد. سیستم‌های غیربحرانی در صورت شکست اثرات ناچیزی دارند.

شناسایی و ثبت محیط‌های فیزیکی/ کسب وکار/ نظارتی پیش‌بینی شده در هر سیستمی که مستقر خواهد شد، تعیین و مستند کردن الزامات/ طرح‌های مناسب و قابل اجرا جهت تداوم کسب وکار یا بازیابی فاجعه[5]، وضعیت محیط نظارتی، تعیین بازیگران[6] قانونی که با فرایند، سرویس و یا محصول تعامل خواهند داشت، تعیین این که چه کسی و به چه اندازه‌ای در استفاده از معیارها و اقدامات امنیتی دچار مشکل شود قابل قبول است، شناسایی و مستندسازی سیستم‌های متصل خارج از کنترل پروژه، تعیین دارایی‌های در معرض خطر در صورت وقوع حادثه، تعیین هزینه (کمی و کیفی) از دست دادن دارایی یا تأثیرات موارد شکست، شناسایی و مستند کردن صاحبان دارایی‌ها، تعیین و مستند کردن فرایندهای جرم‌یابی (قانونی) امنیتی مناسب و ارزیابی

[1] Soft Enterprise
[2] Extended Enterprise
[3] Communities Involved
[4] Safety-critical/mission-critical/non-critical
[5] Disaster Recovery
[6] Actors

هماهنگی یا تضاد سیاست‌های امنیتی شناسایی شده با اهداف کسب و کار از دیگر موارد مهمی است که باید مورد توجه قرار گیرد.

۲-۲- تدوین اصول، استراتژی و سیاست

در این قسمت با در نظر گرفتن نیازمندی‌ها بایستی استراتژی، اصول، قوانین، سیاست‌ها و استانداردهای امنیتی تعریف و مستند گردد.

به‌طورکلی تدوین استراتژی، اصول، قوانین، سیاست‌ها و استانداردهای امنیتی در یک معماری امنیتی فراسازمانی مشخص نمودن چگونگی پیاده‌سازی امنیت به منظور کاهش ریسک‌های شناسایی شده در یک سطح قابل قبول می‌باشد. در واقع سیاست و استانداردهای امنیتی بخشی از فرایند مدیریت نیازمندی‌های فراسازمانی نیز به حساب می‌آیند، به طوری که تمام نیازهای توسعه معماری فراسازمانی بایستی از استراتژی، اصول، قوانین، سیاست امنیتی، محدودیت‌ها، کنترل‌ها و مصنوعات[1] آگاه بوده و بهره ببرند. این موارد در ذیل شرح داده شده است:

استراتژی: استراتژی امنیتی کاملاً در راستای تمام استراتژی‌های کسب و کار قراردارد. استراتژی امنیتی جهت کلی امنیت و نیز سطح اهداف امنیتی و محافظتی که باید به آن دست یافت را تعیین می‌کند و همچنین مرزهای کلی برای کنترل‌های قابل اجرا جهت دستیابی به اهداف را تنظیم می‌کند.

اصول: شامل مفروضات پایه‌ای است که رهنمودهای امنیتی را ارائه می‌دهند.

سیاست‌ها: به معنای قوانین امنیتی هستند که در حوزه‌های کنترلی مختلف اعمال می‌گردند و برای هر سازمانی بایستی تعریف گردد. همچنین به دلیل وجود تغییرات محیطی، سیاست‌ها بایستی به‌روز و به‌صورت دوره‌ای مورد تجدید نظر قرار گیرند.

ا ستانداردها: شامل اجرای سیا ست‌ها از طریق الزامات فنی، روش‌ها و د ستورالعمل‌های تو صیه شده می‌باشد.

[1] Artifact

تمام این موارد بایستی با توجه به استراتژی، اصول، قوانین، سیاست و استانداردهای کلی کشور باشد. دولت مسیری را برای مدیریت سازمان جهت تحقق بخشیدن به برنامه‌های امنیتی موردنیاز در سطح فراسازمان فراهم می‌کند. لیست اسناد بالادستی مرتبط با حوزه امنیت در پیوست شماره ۲ مشخص شده است.

۳-۲- تجزیه و تحلیل (درک) امنیتی

تحلیل و درک امنیتی مرکز کنترلی است که لایه‌ای از کشف و گزارش‌دهی را برای ثبت وقایع[1]، مشاهده، تجزیه و تحلیل، هشدار دادن و گزارش‌دهی در مورد رویدادها، بر روی تمامی حوزه‌های امنیتی ارائه می‌کند؛ این لایه، یک معماری یکپارچه از جمع‌آوری، تجمیع و تجزیه و تحلیل وقایع برنامه‌های کاربردی، رویدادهای امنیتی، داده‌های آسیب‌پذیر، مدیریت هویت و دسترسی به داده، جریان شبکه و پیکربندی فایل‌های برنامه‌های کاربردی و دستگاه‌های امنیتی در سراسر دامنه‌های امنیتی را فراهم می‌کند.

علاوه بر این، لایه تحلیل و درک امنیتی بستر مشترکی برای تمام تحقیقات، گزارش‌دهی و همچنین یک رابط کاربری برای مدیریت ثبت وقایع، مدل‌سازی ریسک، اولویت‌بندی آسیب‌پذیری، تشخیص حادثه و تجزیه و تحلیل تأثیر وظایف فراهم می‌کند. جدول (۲- ۱) لایه تجزیه و تحلیل (درک) امنیتی از مدل مرجع امنیت را نشان می‌دهد.

[1] Logging

جدول (۲- ۱): لایه تجزیه و تحلیل (درک) امنیتی

تجزیه و تحلیل (درک) امنیتی	
هدف	کمک به بهبود امنیت از طریق تجزیه و تحلیل رویدادها و وقایع
مشکلات	• تشخیص تقلب و تهدیدات مبتنی‌بر اینترنت دشوار است. • بیلیون‌ها رویداد امنیتی منجر به تکرار مثبت کاذب[1] می‌شوند. • داده‌های امنیتی به پیدا کردن الگوهای حملات و آسیب‌پذیری‌های جدیدی که برای تجزیه و تحلیل در دسترس نیستند، نیاز دارند. • ضعف در سیستم‌های کنترل و گزارش‌دهی متمرکز
مزایا	• یکپارچه کردن جمع‌آوری، تجمیع و تجزیه و تحلیل وقایع، رویدادهای امنیتی، داده‌های آسیب‌پذیر، فایل‌های پیکربندی و جریان‌های شبکه • فراهم کردن یک بستر مشترک برای تحقیقات، فیلتر کردن، قوانین نوشتاری و گزارش‌دهی • کاهش هزینه و پیچیدگی مدیریت وقایع، تشخیص حادثه و تحلیل تأثیر وظایف

۴-۲- تحلیل و ارزیابی ریسک

با توجه به استاندارد NIST SP 800-30، ریسک معیاری است از این که یک موجودیت تا چه حد توسط شرایط یا رویداد بالقوه‌ای در معرض تهدید قرار می‌گیرد و معمولاً تابعی از اثرات نامطلوب ناشی از وقوع شرایط یا رویداد و احتمال وقوع ریسک می‌باشد.

ریسک در مواردی مانند عملیات سازمانی (شامل مأموریت، توابع، شهرت)، دارایی‌های سازمانی، افراد، سازمان‌های دیگر به علت پتانسیل دسترسی، استفاده، انتشار، اختلال، اصلاح یا تخریب غیرمجاز اطلاعات و یا سیستم‌های اطلاعاتی وجود دارد.

مدیریت ریسک متشکل از مراحل شناسایی ریسک‌های امنیتی، ارزیابی ریسک‌های شناسایی شده، دسته‌بندی ریسک‌های ارزیابی‌شده، کاهش و یا حذف ریسک‌های امنیتی موجود است. در واقع مدیریت

[1] False Positive

ریسک‌های امنیتی، اجرای منظمی از سیاست‌های امنیتی، فرآیندها و روش‌هایی است، که به مدیر سازمان در شناسایی ریسک‌های امنیتی، تحلیل، ارزیابی و طبقه‌بندی آن‌ها کمک می‌کند.

فرآیند مدیریت ریسک‌های امنیتی عبارت است از:

✓ **شناسایی ریسک‌های امنیتی**

شناسایی ریسک اشاره به قابلیت کشف، تشخیص و بررسی وجود ریسک‌های خاص اشاره دارد و شامل موارد زیر است:

- شناسایی دارایی‌های سازمان و منابع اطلاعاتی مرتبط با آن‌ها
- شناسایی تهدیدات مرتبط با دارایی‌های سازمان
- شناسایی آسیب‌پذیری‌هایی که امکان سوءاستفاده از آن‌ها توسط تهدیدات شناسایی شده وجود دارد.
- شناسایی تاثیرات ناشی از عدم حفظ محرمانگی، صحت و دسترس‌پذیری اطلاعات بر روی دارایی‌های امنیتی سازمان

✓ **تحلیل و ارزیابی ریسک‌های امنیتی**

- ارزیابی تأثیرات تجاری بر روی سازمان، که ممکن است حاصل شکست‌های امنیتی ناشی از توالی‌های گوناگونی از عدم وجود محرمانگی، صحت و دسترس‌پذیری اطلاعات مرتبط با دارایی‌های امنیتی باشد.
- ارزیابی احتمال وقوع شکست‌های امنیتی بر اساس تهدیدات و آسیب‌پذیری‌های مرتبط با دارایی‌ها و کنترل‌های امنیتی که در حال اجرا هستند.
- تخمین سطح هر یک از ریسک‌های امنیتی
- تعیین ریسک‌های قابل قبول

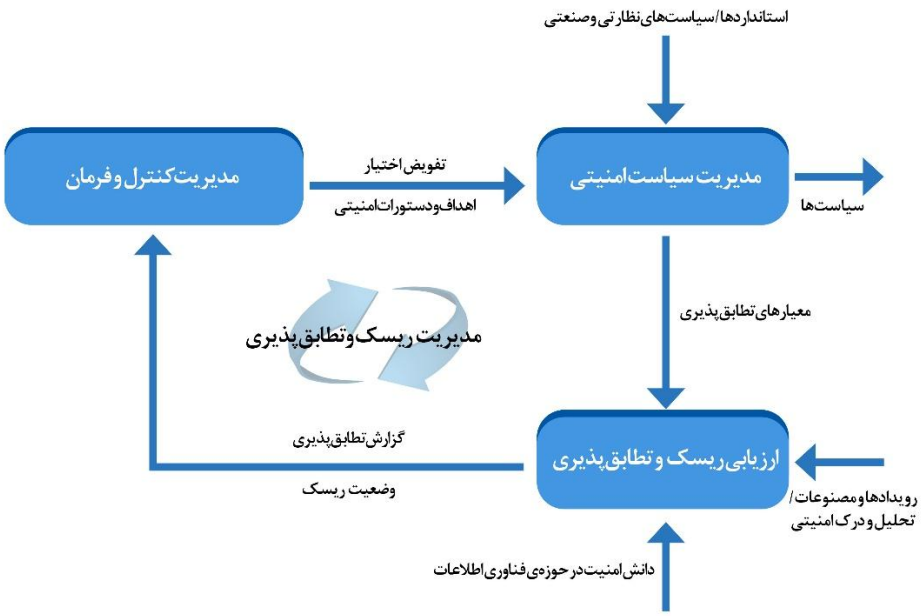
✓ **شناسایی و ارزیابی گزینه‌های مرتبط با کاهش ریسک**

- به‌کارگیری کنترل‌های امنیتی مناسب

- پذیرفتن ریسک‌های امنیتی شناسایی شده
- اجتناب از ریسک‌های امنیتی شناسایی شده

۲-۴-۱- مدیریت ریسک

ریسک بایستی در تمامی سطوح چرخه حیات توسعه سیستم، ارزیابی، کاهش و مدیریت شود. شکل (۲- ۲) چرخه (حلقه بسته) مدیریت ریسک را نشان می‌دهد که برای تحقق مدیریت امنیت جامع ضروری می‌باشد. چرخه مدیریت ریسکی که در ادامه بیان می‌شود بر پایه فرایندی است که در بخش ۲-۴ شرح داده شد.



شکل (۲- ۲): چرخه مدیریت ریسک

مدیریت کنترل و فرمان، اهداف و د ستورات امنیتی را تعیین می‌کند که به و سیله مدیریت سیا ست‌های امنیتی در ترکیب با استانداردهای نظارتی و صنعتی جهت تولید و تنظیم اصول پایه امنیتی استفاده می‌شود، این دستورات بایستی در دیگر زمینه‌های کاربردی امنیت رعایت شوند. همچنین، مدیریت سیاست‌های امنیتی معیارهای انطباق‌پذیری را به‌عنوان ورودی به مؤلفه ارزیابی ریسک و تطابق‌پذیری[1] ارائه می‌دهد؛ به‌طوری که این مؤلفه، رویدادها و مصنوعات امنیتی که بیشتر توسط مؤلفه‌های امنیتی مبتنی‌بر فناوری

[1] Compliance

اطلاعات تولید می شوند را نیز دریافت می‌کند. سپس مؤلفه ارزیابی ریسک و تطابق‌پذیری، به منظور تولید گزارش‌های تطابق‌پذیری و نیز برای استخراج وضعیت ریسک، رویدادها و مصنوعات را ترکیب کرده و با معیارهای تطابق‌پذیری تطبیق می‌دهد، به گونه‌ای که هر دو می‌توانند به عنوان ورودی برای مدیریت کنترل و فرمان به کار روند.

با توجه به شکل فوق، مؤلفه‌های مدیریت کنترل و فرمان، مدیریت سیاست‌های امنیتی و مدیریت ریسک و تطابق‌پذیری با یکدیگر بازتاب‌کننده دامنه مدیریت ریسک و تطابق‌پذیری در چارچوب امنیتی هستند.

در ادامه مؤلفه‌ها و زیرمؤلفه‌های چرخه مدیریت ریسک شرح داده می‌شوند.

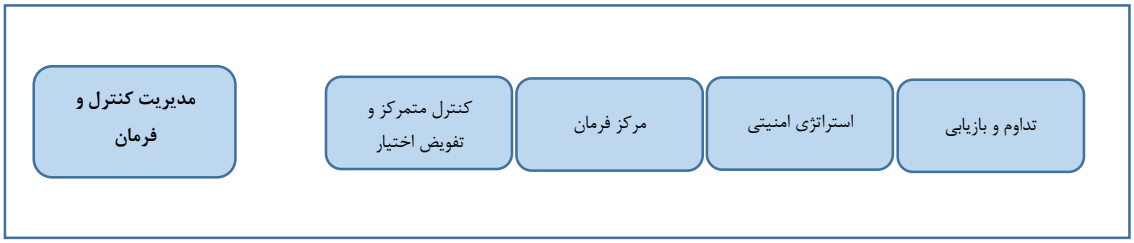
۲-۴-۱-۱- مدیریت کنترل و فرمان

مؤلفه مدیریت کنترل و فرمان، یک مرکز فرمان را برای مدیریت امنیت و قابلیت‌های امنیتی برای دارایی‌های غیر فناوری اطلاعات و نیز سرویس‌هایی را برای اطمینان از محافظت، پاسخ‌گویی، تداوم و بازیابی فراهم می‌کند. این مؤلفه موضوعات مختلفی را پوشش می‌دهد:

- تصویب مجوزهایی برای تأمین امنیت
- تضمین این که امنیت فیزیکی و عملیاتی برای مکان‌ها، دارایی‌ها، افراد، محیط‌ها و تجهیزات برقرار می‌شود.
- فراهم کردن مراقبت و نظارت بر مکان‌ها، محیط پیرامون و نواحی.
- اعمال کنترل‌های ورود.
- قابلیت موقعیت‌یابی، ردیابی و شناسایی افراد و دارایی‌ها.
- ارائه یک نقطه کانونی برای عملیات تداوم و بازیابی.

مدیریت کنترل و فرمان شامل آگاهی از موقعیت و واکنش به مسائل امنیتی فوری و همچنین دارای قابلیت مشاهده و واکنش به روندهای طولانی مدت نیز می‌باشد. در هر دو مورد، مدیریت کنترل و فرمان دارای قابلیت فعال‌سازی[1] و انجام تغییرات واکنشی و فعال در زمینه امنیت فناوری اطلاعات می‌باشد.

مدیریت کنترل و فرمان ممکن است از مؤلفه‌های اصول پایه امنیت، که در بخش ۲-۶-۳- توضیح داده شده‌اند، نیز استفاده کند و می‌تواند به عنوان نقطه کنترلی برای آن‌ها به کار رود. شکل (۲- ۳) یک دیدکلی از مؤلفه‌های مدیریت کنترل و فرمان را نشان می‌دهد.



شکل (۲- ۳): زیرمؤلفه‌های مدیریت کنترل و فرمان

مدیریت کنترل و فرمان شامل زیرمؤلفه‌های زیر می‌باشد:

- **کنترل متمرکز و تفویض اختیار:** مشابه مفهوم سیستم‌های اسکادا (SCADA[2]) در مکان‌های فیزیکی و مراکز صنعتی، این مؤلفه نشان‌دهنده نقش‌های نظارتی در مدیریت امنیت اطلاعات می‌باشد. این مؤلفه شامل مفاهیم تفویض اختیار برای امنیت فناوری اطلاعات به افراد و نقش‌های مناسب در سازمان و مدیریت زیرساخت امنیت فناوری اطلاعات از راه دور می‌باشد. به‌عنوان بخشی از وظایف نظارتی، این مؤلفه دارای قابلیت برقراری امنیت به‌عنوان یک کل و نیز تضمین انطباق سیاست‌ها، استانداردها و رویه‌ها با عناصر مربوط به حقوق کیفری، مدنی، اداری، نظارتی به منظور به حداقل رساندن عواقب عدم پیروی از قانون می‌باشند.
- **مرکز فرمان:** مرکز فرمان نماینده یک واحد سازمانی است که برای پاسخ به تهدیدات آنی فیزیکی یا امنیت فناوری اطلاعات، از طریق پاسخ‌های خودکار یا سناریوهای مستند شده، مورد نیاز می‌باشد.

[1] Trigger
[2] Supervisory Control and Data Acquisition

همچنین دربرگیرنده توسعه و به کارگیری روش‌های مدیریت بحران نیز می‌باشد. بعد فناوری مرکز فرمان می‌تواند یک داشبورد فراسازمانی باشد که یک نقطه متمرکز برای امنیت در سراسر سازمان را فراهم می‌کند. مرکز فرمان، نقطه کانونی برای مدیریت ارتباطات با سازمان‌های خارجی مانند خدمات اورژانس، آتش‌نشانی، پلیس و دیگر سازمان‌های اجرایی قانونی نیز می‌باشد.

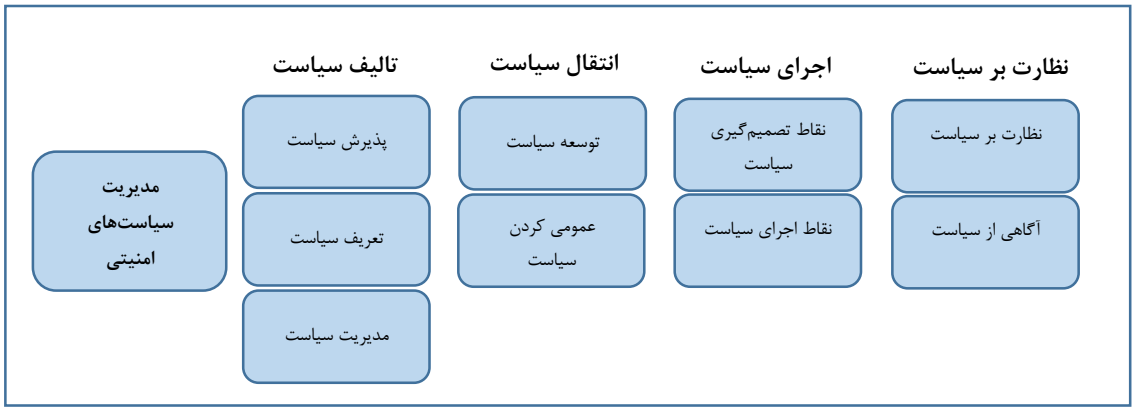
- **استراتژی امنیتی:** یک استراتژی امنیتی کاملاً در راستای تمام استراتژی‌های کسب و کار قراردارد. استراتژی امنیتی جهت کلی امنیت و نیز سطح اهداف امنیتی و محافظتی که باید به آن دست یافت را تعیین می‌کند و همچنین مرزهای کلی برای کنترل‌های قابل اجرا جهت دستیابی به اهداف را تنظیم می‌کند.

- **تداوم و بازیابی:** تداوم و بازیابی بیانگر سرویسی است که یک مجموعه تخصصی شامل قابلیت‌ها، رویه‌ها و فناوری‌هایی را جهت بازیابی و بهبود یک حادثه یا اختلال غیرمنتظره بزرگ به‌کار می‌برد. این سرویس‌ها شامل برنامه‌ریزی اضطراری مانند آموزش کارمندان، رویه‌ها و دستورالعمل‌هایی برای انواع فوریت‌های مهم و طبقه‌بندی خطرات بالقوه می‌باشند. این سرویس‌ها با تداوم کسب وکار (تداوم کسب و کار در طول یک فاجعه و پس از آن) و همچنین با بازیابی فاجعه (ساخت مجدد منابع کلیدی در یک سطح عملیاتی نرمال) متناسب و هماهنگ هستند.

۲-۴-۱-۲- مدیریت سیاست‌های امنیتی

مدیریت سیاست‌های امنیتی کنترل‌هایی برای تألیف، کشف، تجزیه و تحلیل، تبدیل، توزیع و ارزیابی سیاست‌های امنیتی فناوری اطلاعات ارائه می‌کند. این مؤلفه نشان‌دهنده یک نقطه کانونی برای تبدیل نیازمندی‌های امنیتی به سیاست‌هایی است که برای کاهش ریسک‌های کسب‌وکار از دیدگاه فناوری اطلاعات مورد نیاز می‌باشد. یک سیاست امنیتی با استفاده از کسب‌وکار تعریف می‌شود و سپس به وسیله زیرساخت فناوری اطلاعات، کارکنان و مشتریان سازمان اجرا می‌شود.

شکل (۲- ۴) دیدکلی از زیرمؤلفه‌های مدیریت سیاست‌های امنیتی را نشان می‌دهند.



شکل (۲- ۴): زیرمؤلفه‌های مدیریت سیاست‌های امنیتی

مدیریت سیاست‌های امنیتی شامل گروه‌های زیرمؤلفه زیر می‌باشد:

- **تألیف سیاست:** تألیف سیاست فعالیت‌هایی را پوشش می‌دهد که برای درک الزامات کنترل‌های امنیتی و تعریف و مدیریت سیاست‌ها مورد نیاز هستند. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:
  - *پذیرش سیاست:* قابلیت سازمان در درک و قبول الزامات سیاست‌های خارجی را بیان می‌کند. این قابلیت به دلیل این‌که تضمین می‌کند سیاست‌های سازمانی و نظارتی از نظر تناسب و قابلیت اجرا برای کسب و کار، ارزیابی می‌شوند، مؤلفه بسیار مهمی است.

    با توجه به رشد سیاست‌های نظارتی، مهم است که سازمان‌ها به طور مداوم تغییرات سیاست خارجی و الزامات پذیرش و اعمال آن را ارزیابی و بررسی نمایند. این زیرمؤلفه شکاف‌های درون سیاست‌های سازمان را به وسیله نگاشت سیاست‌های خارجی به سیاست‌های ارائه شده از سوی مدیریت کنترل و فرمان مشخص می‌کند.

    این مساله مهم است که توجه داشته باشید که تطبیق ساده و ظاهری با مقررات لزوماً به این معنی نیست که ریسک‌های امنیتی به اندازه مورد نیاز کاهش می‌یابند یا کنترل امنیتی در سازمان به اندازه کافی بالغ (کامل) است.
  - *تعریف سیاست:* این زیرمؤلفه مسئول ثبت مفاد و پیش‌زمینه مربوط به سیاست امنیت فناوری اطلاعات با پیگیری اسناد سیاسی بالادستی (داخلی و خارجی) که آن را تحت تأثیر قرار

می‌دهند یا آن را استدلال و توجیه می‌کنند، می‌باشد. این زیرمؤلفه سیاست را در دو بعد فنی و غیرفنی پوشش می‌دهد که به زیرساخت فناوری اطلاعات سازمان مربوط می‌شود.

- *اداره سیاست:* اداره سیاست، فرایندهای کاری انسان را که شامل ایجاد، اصلاح و نگه‌داری وظایف مربوط به سیاست‌ها در طول زمان می‌باشد را پوشش می‌دهد. همچنین، مدیریت نسخه‌های متعدد از یک سیاست و الزامات انتقال از یکی به دیگری را نیز پوشش می‌دهد. در حوزه اداره سیاست، سیاست‌ها تأیید، اعلام و منتشر می‌شوند. همچنین آموزش و اطلاع‌رسانی در زمینه امنیت از جمله فعالیت‌های دیگر این زیرمؤلفه می‌باشد.

- *انتقال سیاست:* انتقال سیاست، پیگیر حصول سیاست‌های نوشته شده و توزیع شده در درون زیرساخت سازمان، از جمله سیستم‌های فناوری اطلاعات و نیروهای انسانی می‌باشد.

- *توسعه سیاست:* سیاست‌های کسب‌وکار برای سیاست‌های خاص خدمت، مانند امنیت، شاخص‌ها و معیارهای عملکرد و سیاست‌های اعتماد مجدداً پایش می‌شوند. سیاست‌های امنیتی حاصل شده باید به منظور تصمیم‌گیری درباره نکات فنی و اجرایی تفسیر و توزیع شوند.

- *عمومی کردن سیاست*[1]*:* تمام سیاست‌های امنیتی به سیاست‌های اجرایی تبدیل نمی‌شوند. از این رو مهم است که رفتار انسان و سیاست‌های امنیت فرهنگی[2] که سازمان برای کاهش ریسک نیاز دارد، شناسایی شود. در یک محیط که سیاست‌ها و مقررات اغلب تغییر می‌کنند، مهم است که از هماهنگی و هم‌راستایی فرهنگ، باورها، ارزش‌ها و رفتارهای امنیتی درخور کسب‌وکار با این تغییرات مطمئن بود؛ در غیر این صورت، دستورالعمل‌های امنیتی سازمانی می‌تواند خارج از هنجارهای سیاست امنیتی تعریف شوند. در نتیجه عمومی کردن سیاست، یک فرهنگ شناخت امنیتی را بر اساس سیاست‌های سازمانی ایجاد می‌کند.

---

[1] Policy Socialization
[2] Cultural Security Policies

- **اجرای سیاست:** پس از این که سیاست‌ها در سازمان به درستی تألیف و منتقل شدند، سیاست‌ها توسط سیستم‌های فناوری اطلاعات جهت تصمیم‌گیری و اجرای مناسب استفاده می‌شوند. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:
  - *نقاط تصمیم‌گیری سیاست:* نقاط تصمیم‌گیری سیاست بیانگر قابلیتی برای ارزیابی یک درخواست و تصمیم‌گیری در خصوص تطابق درخواست با سیاست، می‌باشند. در موارد خاص، تمام اطلاعاتی که برای تصمیم‌گیری مورد نیاز است در خود درخواست گنجانده می‌شود. در موارد دیگر، اطلاعات زمینه‌ای خارجی مورد نیاز می‌باشد.

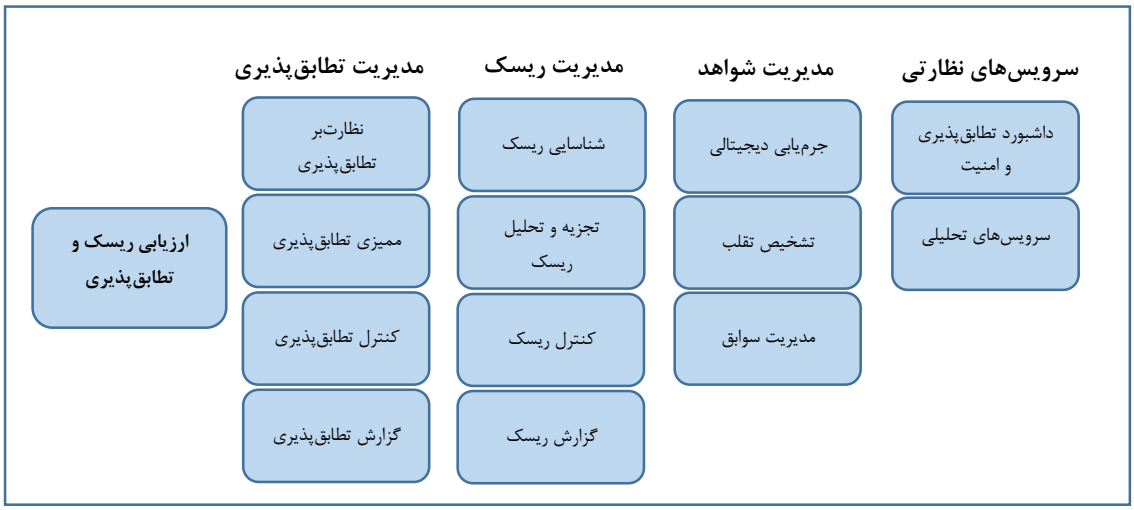
    مسائل مهمی وجود دارد که بر روی محل نقاط تصمیم‌گیری سیاست در یک محیط فناوری اطلاعات تأثیر می‌گذارد. متمرکز ساختن نقاط تصمیم‌گیری می‌تواند سربار اداری و خطاهای احتمالی را در طول توسعه و استقرار کاهش دهد. همچنین متمرکز ساختن نقاط تصمیم‌گیری می‌تواند یک نقطه تصمیم‌گیری سیاست را برای خدمت به نقاط اجرایی متعدد فراهم کند.
  - *نقاط اجرای سیاست:* نقاط اجرای سیاست بر مبنای تطابق درخواست با سیاست عمل می‌کنند. این عمل ممکن است یک اقدام اجرایی باشد که منجر به پذیرش یا رد درخواست شود. همچنین نقطه اجرای سیاست ممکن است اعمالی همچون نظارت، ثبت وقایع و اعلام هشدار را بدون نیاز به درخواست نیز انجام دهد.
- **نظارت بر سیاست:** در نهایت، نظارت بر سیاست، رویدادها و تصمیمات را ثبت و ضبط می‌کند. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:
  - *نظارت بر سیاست:* تأثیرات سیاست می‌تواند از سوی منابع داخلی و یا خارجی باشد. این فعالیت‌ها و اهداف باید به طور مداوم تحت نظارت باشند. همچنین، نظارت بر سیاست، حلقه بازخورد داخلی را فراهم می‌کند که منجر به بازبینی و اعتبارسنجی مجدد یک سیاست بر

اساس تأثیر آن بر روی اجرا و موفقیت یا عدم موفقیت آن سیاست در پایبندی به شاخص‌های کلیدی عملکرد می‌شود. تبعیت از سیاست باید قابل اندازه‌گیری باشد و معیارهای آن می‌توانند برای ارزیابی ریسک و تطابق‌پذیری به منظور ارزیابی مستمر ارائه شوند.

- *درک سیاست*[1]: آگاهی از سیاست می‌تواند یک معیار مؤثر برای موفقیت فعالیت‌های انتقال و عمومی کردن سیاست فراهم نماید. آگاهی از سیاست یک مرحله حیاتی در ایجاد هنجارهای رفتاری و اجتماعی مناسب در یک سازمان است. از طریق نظارت بر سیاست‌های امنیتی سازمان، سازمان‌ها قادرند تضمین کنند که منابع سیاست امنیتی معتبری ایجاد می‌شود و تغییر سیاست‌ها به طور مؤثر ابلاغ می‌گردد. آگاهی‌های تصدیق شده و ارزیابی مجدد آگاهی می‌تواند به محافظت از سازمان در برابر نقض سیاست‌ها کمک کند.

۲-۴-۱-۳- ارزیابی ریسک و تطابق‌پذیری

ارزیابی ریسک و تطابق‌پذیری، به یک سازمان فناوری اطلاعات در جمع‌آوری، تجزیه و تحلیل، گزارش اطلاعات و رویدادهای امنیتی به منظور شناسایی، اندازه‌گیری، ارزیابی و گزارش‌دهی درباره ریسک‌های مربوط به فناوری اطلاعات کمک می‌کند. این مؤلفه مدیریت تطابق‌پذیری، مدیریت ریسک، مدیریت شواهد و سرویس‌های نظارتی را پوشش می‌دهد.شکل (۵-۲) دید کلی از زیرمؤلفه‌های ارزیابی ریسک و تطابق‌پذیری را نشان می‌دهد.



[1] Policy Awareness

شکل (۲- ۵): زیرمؤلفه‌های ارزیابی ریسک و تطابق‌پذیری

ارزیابی ریسک و تطابق‌پذیری شامل گروه‌های زیرمؤلفه زیر می‌باشد:

- **مدیریت تطابق‌پذیری:** مدیریت تطابق‌پذیری، تمام فعالیت‌های مربوط به استخراج وضعیت تطابق‌پذیری امنیتی محیط فناوری اطلاعات را پوشش می‌دهد. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:

- *نظارت بر تطابق‌پذیری:* نظارت بر تطابق‌پذیری به ملاحظاتی از محیط جهت شناسایی اختلاف یا شکاف بین عملیات واقعی، سیاست‌ها و استانداردهای داخلی و نیازمندی‌ها اشاره دارد؛ به‌طوری‌که آن‌ها از مقررات، قوانین و دستورات صنعتی خارجی ناشی می‌شوند.
- *ممیزی تطابق‌پذیری:* ممیزی تطابق‌پذیری به قابلیتی برای مطابقت منبع (منشأ) رویداد و جریان رویدادهای آن با الزامات گزارش تطابق‌پذیری برای امنیت فناوری اطلاعات اشاره دارد و گزارش‌هایی براساس آن جریان‌های رویداد (یا به صورت دوره‌ای یا برحسب تقاضا) ارائه می‌کند. مدیریت ارتباط بین گزارش‌های منابع رویداد و الزامات گزارش تطابق‌پذیری یک قابلیت کلیدی این مؤلفه می‌باشد. همچنین، الزامات تطابق‌پذیری اغلب، الزامات نگهداری سوابق در مورد داده‌های ممیزی که ممکن است متفاوت از الزامات نگه‌داری جریان‌های رویداد در محیط فناوری اطلاعات باشد را نیز تحمیل می‌کند. از دید عملیات فناوری اطلاعات، جریان‌های رویداد بسیار کوتاه مدت هستند، در حالی که داده‌هایی که از ممیزی تطابق‌پذیری پشتیبانی می‌کنند ممکن است یک گستره عمر چندین ساله داشته باشند.
- *کنترل تطابق‌پذیری:* کنترل تطابق‌پذیری کار مداومی است که توسط متخصصین امنیت فناوری اطلاعات در سراسر بخش‌های مختلف یک سازمان صورت می‌پذیرد، و به شدت بر روی دو فعالیت پشتیبانی از تطابق‌پذیری و پیگیری (ردیابی) تطابق‌پذیری تمرکز می‌کند.

پشتیبانی از تطابق‌پذیری به ارائه مشاوره و راهنمایی به کاربرانی که لزوماً متخصص نیستند اما فعالیت‌های آن‌ها مرتبط با تطابق‌پذیری است، اشاره دارد. به‌عنوان مثال، متخصصان تطابق‌پذیری به یک واحد کسب‌وکار در انجام ممیزی‌ها کمک می‌کنند.

جنبه دیگر کنترل تطابق‌پذیری، پیگیری تطابق‌پذیری می‌باشد که مستندات ساخت‌یافته‌ای از پیگیری فعالیت‌ها پس از یک ممیزی و پیشرفت این فعالیت‌ها تا زمان خاتمه را پوشش می‌دهد. این فعالیت‌ها یا توسط حسابرس به صورت مستقیم تعیین می‌شوند یا براساس تجزیه و تحلیل نتایج ممیزی و آن دسته از اقداماتی که باید برای کاهش مشکلات امنیتی شناسایی شده، پیاده‌سازی شوند به‌دست می‌آیند. کنترل تطابق‌پذیری یک فرایند مداوم است (قبل، در طول و بعد از ممیزی) و از این رو نیاز به تلاش‌های مستمر و قابل توجهی در یک سازمان دارد.

- *گزارش تطابق‌پذیری:* گزارش تطابق‌پذیری به توانایی خلاصه‌سازی اطلاعات مربوط به رویدادهای تحلیل شده و دیگر اطلاعات مربوط به امنیت اشاره دارد. اغلب اوقات، گزارش برای ارزیابی پیروی از مقررات یا تطابق با توافق‌های سرویس امنیتی و در کل تطابق عملکرد محیط فناوری اطلاعات استفاده می‌شود. از دید امنیت داخلی، گزارش تطابق‌پذیری در اکثر موارد برای کنترل بر روی سیاست‌های امنیتی و شناسایی ضعف‌ها در تطابق‌پذیری امنیتی استفاده می‌شود.

- **مدیریت ریسک:** مدیریت ریسک تمام فعالیت‌های مربوط به استخراج وضعیت ریسک امنیتی محیط فناوری اطلاعات را پوشش می‌دهد. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:

  - *شناسایی ریسک:* شناسایی ریسک به قابلیت کشف، تشخیص و بررسی وجود ریسک‌های خاص اشاره دارد.

- *تجزیه و تحلیل ریسک:* تجزیه و تحلیل ریسک به فعالیت‌هایی اشاره دارد که به طبقه‌بندی، توصیف و یا تعیین احتمال و تأثیر ریسک‌ها مربوط می‌شود. همچنین تحقیقات درباره ارتباطات، وابستگی و همبستگی بین ریسک‌های مختلف را نیز پوشش می‌دهد.
- *کنترل ریسک:* کنترل ریسک فعالیت‌هایی که می‌توانند برای رسیدگی به ریسک‌ها استفاده شوند را تعیین می‌کند. محدوده فعالیت‌های معتبر می‌تواند از پذیرش ریسک با استفاده از روش‌های مختلف کاهش ریسک تا انتقال ریسک باشند. همچنین کنترل ریسک شامل تعیین هزینه برای چنین فعالیت‌هایی و شناسایی ریسک‌های بالقوه و بازیگران و مسئولین کاهش ریسک نیز می‌باشد. بخش مهم دیگر کنترل ریسک، پیگیری وضعیت فعالیت‌های کاهش‌دهنده ریسک‌های شناسایی شده تا زمان اتمام آن‌هاست.
- *گزارش ریسک:* مشابه گزارش تطابق‌پذیری، گزارش ریسک به توانایی خلاصه کردن داده‌های ریسک تحلیل شده و دیگر اطلاعات مربوط به ریسک و ارائه سطوح مختلفی از جزئیات درباره وضعیت ریسک‌های امنیتی برای بخش‌های مختلف سازمان به عنوان ورودی برای تجزیه و تحلیل و پردازش‌های بیشتر اشاره دارد.

گزارش ریسک به عنوان ورودی برای گزارش تطابق‌پذیری استفاده می‌شود زیرا مقررات خاصی ممکن است یک سازمان را ملزم کند که اطلاعاتی درباره رویدادهای ریسک کلیدی برای ذی‌نفعان خود ارائه کند (به‌عنوان مثال، بانک‌ها باید به مقامات نظارتی درباره ریسک‌های بالقوه خود که می‌تواند شامل وضعیت ریسک امنیتی آن‌ها باشد، گزارش دهند). از دید امنیت داخلی، گزارش ریسک به صورت متداول برای کمک به تصمیم‌گیری درست درباره سرمایه‌گذاری در فعالیت‌های کاهش ریسک و پیگیری روند پیشرفت این فعالیت‌ها استفاده می‌شود.

- **مدیریت شواهد:** مدیریت شواهد سرویس‌های مربوط به ثبت و ضبط و تأمین امنیت اطلاعات را به صورتی که این سرویس‌ها بتوانند به‌عنوان شواهد قانونی در دادگاه استفاده شده و یا بایستی به دلایل قانونی دیگری حفظ شوند را پوشش می‌دهد. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:
  - *جرم‌یابی دیجیتالی*[1]: جرم‌یابی دیجیتالی به توانایی بازیابی و حفظ وضعیت مؤلفه‌های فناوری اطلاعات که مورد هدف تحقیقات قانونی هستند، اشاره دارد. در موارد خاص، جرم‌یابی شامل حفظ وضعیت یک سیستم برای مراجعات بعدی است. در موارد دیگر، جرم‌یابی ملزم به بازسازی مجدد رویدادهایی است که باعث به وجود آمدن وضعیتی در یک مؤلفه خاص می‌شود.

    تحقیقات درمورد جرم‌یابی می‌تواند به صورت داخلی یا به عنوان بخشی از یک روند قانونی آغاز شود. زمانی که تحقیقات در مورد جرم‌یابی به عنوان بخشی از روند قانونی آغاز می‌شود، مسائل امنیتی بیشتری از جمله جامعیت[2]، دقت[3] و صحت داده‌های جمع‌آوری شده و نیز زنجیره نگهداری[4]، می‌تواند مدنظر قرار بگیرد. زنجیره نگهداری شرایطی را که در آن داده‌ها از یک مؤلفه فناوری اطلاعات به مؤلفه دیگر یا از یک فرد به فرد دیگری منتقل می‌شود را پوشش می‌دهد.
  - *تشخیص تقلب*[5]: تشخیص تقلب، تجزیه و تحلیل اطلاعات و رویدادهای درون محیط فناوری اطلاعات که به فعالیت‌های ناخواسته در سطح کسب وکار مربوط می‌شود را پوشش می‌دهد. معمولاً، تشخیص تقلب اطلاعات و رویدادهای امنیتی را برای ترکیب خاصی از وقایع بررسی و بازبینی می‌کند که نه تنها سوءاستفاده از حقوق کاربر یا دور زدن مکانیزم‌های کنترل

[1] Digital Forensics
[2] Completeness
[3] Accuracy
[4] Chain of custody
[5] Fraud Detection

دسترسی در زمینه یک سیاست را تشخیص می‌دهد؛ بلکه انجام فعالیت‌های جعلی در زمینه قانونی را نیز مشخص می‌کند.

- مدیریت سوابق: مدیریت سوابق الزامات قانونی را جهت ضبط و نگه‌داری سوابق خاصی در مورد تراکنش‌ها و ارتباطات کسب‌وکار جهت ارائه به عنوان شواهد پوشش می‌دهد.

- **سرویس‌های نظارتی:** سرویس‌های نظارتی در مدیریت ریسک و تطابق‌پذیری، نظارت، هشدار و تجزیه و تحلیل در تمام زمینه‌های مدیریت تطابق‌پذیری، ریسک و شواهد را فراهم می‌کنند. این مؤلفه شامل زیر مؤلفه‌های زیر می‌باشد:

- *داشبورد امنیت و تطابق‌پذیری:* مشابه دیگر داشبوردهای مربوط به کسب‌وکار، داشبورد امنیت و تطابق‌پذیری به یک مجموعه از واسط‌های تحت وب برای نمایش گزارش اطلاعات فعلی رویدادها و وضعیت امنیت فناوری اطلاعات اشاره دارد. داشبوردها بر مبنای جریان رویدادهایی هستند که در طی یک دوره جمع‌آوری می‌شوند.
- *سرویس‌های تحلیلی:* سرویس‌های تحلیلی به پیدا کردن روندهایی در رویدادهای وابسته و اتخاذ تصمیماتی بر مبنای روندهای پیدا شده، کمک می‌کنند. به‌عنوان مثال، یک موتور تحلیل رویداد ممکن است رویدادهای مجوزدهی را با سوابق کارمند به منظور تشخیص استفاده از حساب‌های کاربری غیرفعال[1] افرادی که سازمان را ترک کرده‌اند یا استفاده از یک شناسه مشترکی که بر اساس سیاست امنیتی سازمان مجاز نمی‌باشد، مطابقت بدهد.

۲-۵- حوزه‌های اصلی امنیت در مدل مرجع

۲-۵-۱- افراد

سازمان‌ها باید از دارایی‌ها و سرویس‌هایی که در خدمت کسب وکار آن‌هاست و از عملیات آن‌ها پشتیبانی می‌کنند، محافظت کنند. یک جنبه مهم از دستیابی به این حفاظت، از طریق مدیریت هویت و کنترل دسترسی

[1] Orphan Account

فراهم می‌شود. سازمان‌ها کاربران را ثبت‌نام می‌کنند و آن‌ها را به هویت‌ها یا حساب‌های کاربری نگاشت می‌کنند. روابط بین افراد و سازمان در نقش‌ها، مجوزها، سیاست‌های کسب وکار و قوانین بیان می‌شود. قابلیت ثبت افراد و توصیف ارتباط آن‌ها در داخل سازمان یک عامل امنیتی کلیدی برای دیگر دامنه‌ها و حوزه‌های امنیت است.

در عمل، به افرادی که در نقش‌های مجاز در یک سازمان فعالیت می‌کنند اجازه دسترسی به زیرساخت، داده، اطلاعات، برنامه‌های کاربردی و سرویس‌ها اعطا می‌شود. به همین ترتیب، افرادی که در نقش‌های غیرمجاز یا خارج از سیاست‌ها و قوانین کسب‌وکار فعالیت می‌کنند از دسترسی به زیرساخت، داده، اطلاعات، برنامه‌های کاربردی و سرویس‌ها منع می‌شوند.

در یک سیستم هویت، برای افراد یک گواهی‌نامه به منظور اثبات هویت آن‌ها در سیستم‌های فناوری اطلاعات صادر می‌شود. یک گواهی‌نامه می‌تواند به اشکال مختلفی وجود داشته باشد، مانند یک کارت هویت فیزیکی یا توکن منطقی. میزان اعتبار یک گواهی‌نامه یکی از جنبه‌های مهم سیاست کسب‌وکار و مدیریت ریسک است. توانایی مدیریت مؤثر و کارای چرخه حیات یک هویت، که عبارت است از ایجاد، حذف و تغییر نقش برای جمعیت پویای نیروی کار، مشتری یا جوامع کاربر، بسیار مهم است. به عنوان مثال، چرخه حیات هویت و گواهی‌نامه می‌تواند تحت تأثیر چرخه شغل، چرخه اشتغال و روابط مشتری قرار بگیرد.

اغلب، سیستم‌های هویت باید نقش، حقوق و امتیازات[1] کاربران را در یک محیط ناهمگن که از فناوری‌ها و معماری‌های متعددی در داخل یک زیر ساخت فناوری اطلاعات تشکیل شده است، مدیریت کنند. سیستم‌های هویت باید با مجموعه‌ای از کنترل دسترسی‌های مناسب یکپارچه شوند.

هر سازمانی باید فعالیت‌های دسترسی کاربران مجاز را به منظور اطمینان از این که هیچ دسترسی سطح بالایی برای اهداف مخرب مورد سوءاستفاده قرار نگرفته باشد، نگه‌داری کند. در این زمینه بسیار مهم است که دسترسی‌های مجاز و ویژگی تمام اقدامات افراد درون سازمان از نزدیک نظارت شود.

[1] Privileges

جدول (۲- ۵) خلاصه‌ای از جنبه‌هایی که در حوزه افراد پوشش داده می‌شود را نشان می‌دهد.

جدول (۲- ۲): حوزه افراد

افراد	
هدف	مدیریت و گسترش هویت فراسازمانی در تمام دامنه‌های امنیتی با هویت یکپارچه
مشکلات	• سربار هزینه مدیریت کردن کاربران و هویت‌ها در سراسر سیستم‌ها • ضعف در نظارت بر فعالیت کاربر مجاز • هویت‌های مشترک برای دسترسی به منابع به صورت نادرست استفاده می‌شود. • ناموفق بودن یک ممیزی، پاسخ به الزامات تطابق‌پذیری
مزایا	• کاهش هزینه، افزایش کارایی و فراهم کردن قابلیت ممیزی مدیریت ورود، استفاده و ترک سیستم‌های سازمانی توسط کاربران • کاهش دادن ریسک تقلب داخلی • پشتیبانی از جهانی شدن (گسترده شدن) عملیات • فراهم کردن توانایی تغییر جهت به مدل‌های کسب وکار جدید، به عنوان مثال، تحویل (محصول یا خدمت) به مشتری و شرکا با استفاده از سرویس‌های برخط • بهبود تجربه کاربر نهایی با فراهم کردن یکپارچگی و ورود یکپارچه[1]

۲-۵-۲- داده

سازمان‌ها باید از داده‌های خام و همچنین اطلاعات مفهومی که در محدوده کنترلی آن‌ها قرار دارد، محافظت کنند. سازمان باید دستورالعمل و راهنمایی‌هایی را در خصوص طبقه‌بندی و ارزش داده و اطلاعات و چگونگی مدیریت ریسک داده‌ها و اطلاعات را برای فناوری اطلاعات فراهم نماید. یک طرح مؤثر برای محافظت از داده و اطلاعات شامل تهیه و نگه‌داری فهرستی از این دارایی‌ها همراه با ویژگی‌ها، سیاست‌ها، مکانیزم‌های اجرایی و سرویس‌هایی که دسترسی، انتقال، گردش و موقعیت داده‌ها و اطلاعات را کنترل می‌کنند، می‌باشد.

این طرح محافظت از داده و اطلاعات می‌تواند به فرایندها و تراکنش‌های کسب‌وکار یا فرایندهای پشتیبانی از زیرساخت و کسب‌وکار اعمال شود. محافظت از داده و اطلاعات، چرخه حیات کامل اطلاعات از ایجاد تا

[1] Single Sign-on

تخریب تمام موقعیت‌ها، وضعیت‌ها و نمونه‌های مختلف آن و همچنین داده‌های بدون استفاده[1] و داده‌های قابل استفاده[2] را پوشش می‌دهد.

اصطلاح داده می‌تواند برای طیف وسیعی از دارایی‌های رمز شده به‌صورت الکترونیکی به‌کار رود. این دارایی‌ها شامل نرم‌افزار و سیستم‌عامل می‌باشند که باید در برابر ریسک‌های عملیاتی (جهت تضمین این که کدهای مخربی تولید نمی‌شوند) و ریسک‌های کسب‌وکار (جهت تضمین این که شرایط صدور مجوز نقض نمی‌شود) محافظت شوند. همچنین شامل انواع دیگری از مالکیت معنوی، از جمله برنامه‌ها و طرح‌ها و فرم‌های ساخت‌یافته و بدون ساختار نیز می‌باشد. نظارت بر دسترسی به داده‌ها و محافظت از داده‌ها در برابر نشت ناخواسته یا از دست دادن[3] اطلاعات حتی در محیط بسترهای محاسبات ابری متغیر امروزی بسیار پیچیده‌تر شده است.

اندازه‌گیری و گزارش‌دهی درباره تطابق‌پذیری یک سازمان در رابطه با حفاظت از داده و اطلاعات یک معیار ملموس از اثربخشی طرح امنیت سازمان می‌باشد. یک گزارش تطابق‌پذیری اطلاعات و داده، منعکس‌کننده قوت یا ضعف کنترل‌ها، سرویس‌ها و مکانیزم‌ها در تمام حوزه‌ها می‌باشد.

جدول (۲- ۲) خلاصه‌ای از جنبه‌هایی که در حوزه داده پوشش داده می‌شود را نشان می‌دهد.

جدول (۲- ۳): حوزه داده

داده	
هدف	کمک به امنیت حریم خصوصی و صحت دارایی‌های اطلاعاتی مورد اعتماد سازمان
مشکلات	• داده‌های ذخیره شده بر روی رسانه‌های قابل حمل می‌توانند مفقود یا سرقت شوند. • دسترسی به داده‌های ذخیره شده به صورت آشکار ساده است. • ناسازگاری (تناقض) در سیاست‌های مربوط به داده در کل سازمان • داده‌های بدون ساختاری که کشف، دسته‌بندی و نظارت بر آن‌ها دشوار می‌باشد.

[1] At rest
[2] In motion
[3] Loss

	• هزینه‌های نقض داده، اطلاع‌رسانی، ارزش نام تجاری
مزایا	• کاهش هزینه، افزایش قابلیت برخورداری از ممیزی و پیروی از الزامات • حصول اطمینان از این که داده در زمان مناسب در دسترس افراد مجاز قرار دارد. • کاهش ریسک فاش یا تخریب داده. • شناسایی فعالیت‌های غیرمجاز یا مشکوک بدون تأثیر برروی کارایی یا تغییر دادن پایگاه داده

۲-۵-۳- نرم‌افزار

این مساله ضروری است که یک رویکرد لایه‌ای برای امنیت وجود داشته باشد که تضمین کند تمام حوزه‌های امنیت به طور مناسب در یک زیرساخت امنیتی پوشش داده می‌شود. یکی از مؤثرترین راه‌ها برای دوری از نقض در برنامه‌های کاربردی، اطمینان از طراحی و پیاده‌سازی امن برنامه‌های کاربردی است که کاربران به آن‌ها دسترسی دارند.

سازمان‌ها باید از نرم‌افزارهای حیاتی کسب‌وکار خود در برابر تهدیدات داخلی و خارجی در سراسر چرخه حیات خود، از طراحی تا توسعه، آزمون و تولید، محافظت کنند. سیاست و رویه‌های امنیتی تعریف شده و واضح برای اطمینان از این که نرم‌افزار ریسک‌های بیشتری را برای کسب‌وکار به وجود نمی‌آورد، بسیار حیاتی است.

پویش خودکار کد منبع نرم‌افزار و همچنین آزمون آسیب‌پذیری سیستم‌های عملیاتی، می‌تواند قبل از وقوع یک حادثه امنیتی به شناسایی نقاط ضعفی که ممکن است توسط حمله‌کننده مورد استفاده قرار گیرد، کمک کند. جدول (۲- ۳) خلاصه‌ای از جنبه‌هایی که در حوزه نرم‌افزار پوشش داده می‌شود را نشان می‌دهد.

جدول (۲- ۴): حوزه نرم‌افزار

نرم‌افزار

هدف	کمک به کاهش هزینه‌ی توسعه برنامه‌های کاربردی امن‌تر
مشکلات	• برنامه‌های کاربردی وب اولین هدف هکرها است. • برنامه‌های کاربردی معمولاً دارای آسیب‌پذیری‌هایی هستند. • ۸۰ درصد از هزینه‌های توسعه، صرف شناسایی و رفع نواقص می‌شود. • داده‌های شخصی توسط فردی با دسترسی به محیط توسعه یا آزمون در معرض افشا قرار دارند، از جمله پیمانکاران.
مزایا	• کاهش خطر تغییر یا سرقت اطلاعات مربوط به برنامه‌های کاربردی وب • ارزیابی و نظارت بر پیروی از سیاست‌های امنیتی سازمان • بهبود تطابق‌پذیری با استاندارهای صنعتی و الزامات قانونی • آزمون و کنترل خودکار در سراسر چرخه حیات توسعه برنامه کاربردی

۲-۵-۴- زیرساخت

سازمان‌ها باید فعالانه بر عملکرد کسب‌وکار و زیرساخت فناوری اطلاعات به منظور شناسایی تهدیدات و آسیب‌پذیری‌ها جهت جلوگیری یا کاهش نقایض نظارت کنند. نظارت و مدیریت بر امنیت شبکه، سرویس‌دهنده‌ها و نقاط انتهایی یک سازمان به منظور جلوگیری از تهدیداتی که می‌توانند بر مؤلفه‌های سیستم، افراد و فرایندهای کسب وکار تأثیر سوء بگذارند، بسیار حیاتی است. تمرکز و شدت نظارت و مدیریت بر امنیت می‌تواند متأثر از نوع شبکه، سرویس‌دهنده‌ها و نقاط انتهایی موجود در زیرساخت فناوری اطلاعات و نحوه ایجاد، یکپارچگی، آزمون و نگه‌داری این مؤلفه‌ها باشد.

تأمین امنیت زیرساخت کلی یک سازمان می‌تواند به معنای اتخاذ اقدامات احتیاطی در برابر شکست یا از دست دادن دارایی‌های زیرساخت‌های فیزیکی باشد که ممکن است بر روی تداوم کسب‌وکار تأثیر بگذارد. این امنیت می‌تواند شامل محافظت در برابر تهدیدات و آسیب‌پذیری‌های غیرمستقیم، مانند تأثیر از دست دادن یک سرویس مفید، یک نقض در کنترل دسترسی فیزیکی یا از دست دادن دارایی‌های فیزیکی حیاتی باشد.

امنیت فیزیکی کارا به یک سیستم مدیریت متمرکز نیاز دارد که اجازه همبستگی (ارتباط) ورودی‌ها از منابع مختلف از جمله اموال، کارمندان، مشتریان، عموم مردم و شرایط محلی و منطقه‌ای را می‌دهد. تأمین امنیت دارایی‌های زیرساخت فیزیکی به اندازه تأمین امنیت دارایی‌های زیرساخت فناوری اطلاعات مهم است.

سازمان‌ها به صورت چشمگیری در حال استفاده از فناوری‌های مجازی‌سازی[1] به منظور پشتیبانی از اهداف خود در ارائه محصول در کمترین زمان و هزینه ممکن هستند. با ایجاد ساختاری از کنترل‌های امنیتی در داخل این محیط، سازمان‌ها می‌توانند به اهداف مجازی‌سازی از جمله استفاده بهینه از منابع فیزیکی، بهبود کارایی سخت‌افزار و کاهش هزینه‌های برق دست یابند، در حالی که تضمین می‌شود سیستم‌های مجازی با همان دقت سیستم‌های فیزیکی امن می‌شوند.

جدول (۲- ۴) خلاصه‌ای از جنبه‌هایی که در حوزه زیرساخت پوشش داده می‌شود را نشان می‌دهد.

جدول (۲- ۵): حوزه زیرساخت

زیرساخت	
هدف	کمک به محافظت در برابر حملات پیچیده با داشتن آگاهی نسبت به کاربران، محتوا و نرم‌افزار
مشکلات	• هدایت خودکار تهدیدات • ضعف دانش در خصوص ریسک‌های موجود در فناوری‌ها و برنامه‌های کاربردی جدید، از جمله مجازی‌سازی و فناوری ابر • ضعف در توانایی نظارت و مدیریت ورودی‌های امنیت • نقض‌ها و شکاف‌های کشف نشده ناشی از سوءاستفاده از دسترسی‌های مجاز و خرابی‌های ناشی از حادثه • کنترل ضعیف نرم‌افزاری
مزایا	• کاهش هزینه‌های جاری مدیریت عملیات امنیتی • بهبود قابلیت در دسترس‌پذیر بودن عملیات و تضمین مطابقت عملکرد با سرویس‌های مورد توافق • افزایش بهره‌وری با استفاده از کاهش ریسک بدافزارها[2]

[1] Virtualization Technology
[2] Malware

در ادامه جهت حرکت به سمت مجموعه مشترکی از قابلیت‌های امنیتی، این حوزه‌ها و لایه‌ها با جزئیات بیشتری شرح داده می‌شوند تا سازمان‌ها را جهت رسیدن به اهداف کسب‌وکار خود به صورت امن یاری نماید. این قابلیت‌های امنیتی اصلی تحت عنوان اصول پایه امنیت در بخش کنترل‌های امنیتی مطرح می‌شوند.

۲-۶-کنترل‌های امنیتی

یکی از راهکارها برای کاهش یا از بین بردن ریسک، استفاده از کنترل‌های امنیتی مناسب می‌باشد. کنترل‌ها، مکانیزم‌هایی هستند که تهدیدات را رفع نموده و آسیب‌پذیری‌ها را کاهش می‌دهند. در واقع هدف کنترل‌ها، پشتیبانی و کمک به طراحی و توسعه راه‌حل‌های امنیتی در سازمان و کاهش ریسک می‌باشد.

این بخش یک رویکرد بی‌طرف نسبت به محصول- و راه‌حل- برای دسته‌بندی و تعریف قابلیت‌ها و سرویس‌های امنیتی ارائه می‌دهد. چنین رویکردی برای پاسخگویی به نگرانی‌های کسب‌وکار در چارچوب مدل امنیتی مورد نیاز می‌باشد.

به طور کلی در انتخاب کنترل‌های امنیتی بایستی مواردی را مورد توجه قرار داد، ازجمله:

- ✓ مجموعه کنترل‌های پیاده‌سازی شده در داخل یک سازمان بایستی متناسب با نیازهای آن سازمان طراحی شود.
- ✓ نوع کنترل‌ها بایستی با تکنولوژی و زیرساخت سازمانی مطابقت داشته باشد.
- ✓ دامنه کنترل‌ها بایستی با اهمیت مأموریت مطابقت داشته باشد. (به‌عنوان مثال برای سیستمی با اهمیت کمتر، کنترل‌های کمتری استفاده شود.)
- ✓ کنترل‌ها بایستی با الزامات عملکرد هم‌راستا باشند.
- ✓ هریک از کنترل‌ها بایستی به منظور کاهش ریسک در یک سطح قابل قبول ارزیابی شوند.

- ✓ در هر پیاده‌سازی خاصی از کنترل‌ها در داخل سازمان یا سیستم، استراتژی کاهش ریسک بایستی یک رویکرد امنیتی لایه‌بندی شده را دنبال نماید. لایه‌بندی کنترل‌ها در حوزه‌های امنیتی مختلف، باعث بهبود وضعیت امنیت یک سازمان می‌شود.

در این بخش ابتدا اصول پایه امنیت که در واقع همان قابلیت‌های امنیتی اصلی هستند معرفی می‌شود و همچنین برای تمامی اصول معرفی شده، زیرساخت و سرویس‌های امنیتی موردنیاز مشخص می‌شود؛ که این کار به طراحان امنیت جهت تهیه و توسعه راه‌حل‌های امنیتی کمک می‌کند.

همچنین، در پیوست شماره ۱ و ۲، به منظور کاهش ریسک‌های امنیتی، راهنمایی بیشتر و سهولت کار طراحان امنیتی جهت در نظر گرفتن اصول پایه امنیت در تمامی حوزه‌های فناوری اطلاعات، این حوزه‌ها به چندین گروه اصلی تقسیم شده و استانداردهای امنیتی مربوط به هر گروه ارائه شده است.

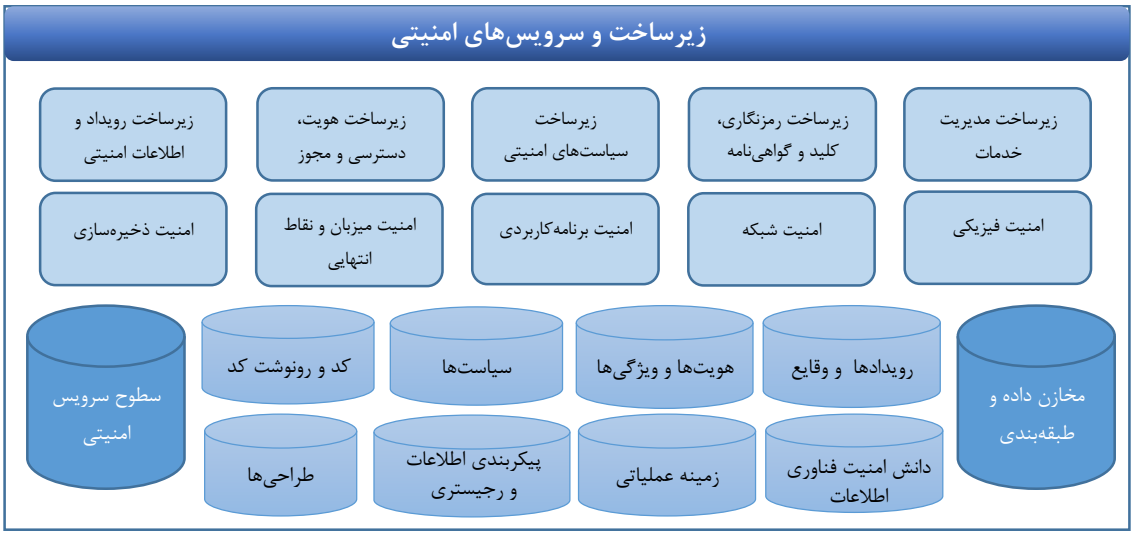
۲-۶-۱- اصول پایه امنیت

اصول پایه امنیت شامل مؤلفه‌های سطح بالایی است که برای هدایت و کنترل امنیت فناوری اطلاعات از دیدگاه مدیریت ریسک استفاده می‌شود. این مؤلفه‌ها در ذیل نام برده شده و در بخش بعدی با جزئیات بیشتر بیان می‌شوند.

- ➢ مدیریت هویت، دسترسی و مجوز
- ➢ مدیریت حفاظت از داده و اطلاعات
- ➢ تضمین نرم‌افزار، سیستم و سرویس
- ➢ مدیریت تهدید و آسیب‌پذیری
- ➢ مدیریت خدمات فناوری اطلاعات
- ➢ مدیریت دارایی‌های فیزیکی

۲-۶-۲- زیرساخت و سرویس‌های امنیتی

سرویس‌ها و زیرساخت‌های امنیتی شامل مؤلفه‌ها و زیرمؤلفه‌هایی است که توسط مؤلفه‌های اصول پایه امنیت در زمینه‌های مربوط به خود استفاده می‌شوند. در شکل (۲- ۶)، زیرمؤلفه‌های زیرساخت و سرویس‌های امنیتی آمده است.



شکل (۲- ۶): زیرساخت و سرویس‌های امنیتی

در ادامه مؤلفه‌های زیرساخت و سرویس‌های امنیتی شرح داده شده است:

- **زیرساخت رویداد و اطلاعات امنیتی** ساختاری را برای تجمیع، همبستگی و تجزیه و تحلیل خودکار وقایع فراهم می‌کند. همچنین یک سازمان را در تشخیص، بررسی و پاسخگویی خودکار به حوادث، تسهیل پیگیری و برطرف کردن حوادث، با هدف بهبود عملیات امنیتی و مدیریت ریسک اطلاعات یاری می‌کند.
- **زیرساخت هویت، دسترسی و مجوز** سرویس‌هایی را برای مدیریت تخصیص کاربر، رمزعبورها، ورود یکپارچه، کنترل دسترسی و همگام‌سازی اطلاعات کاربر در دایرکتوری‌ها ارائه می‌کند.
- **زیرساخت سیاست‌های امنیتی** سرویس‌هایی را برای مدیریت توسعه سیاست‌های امنیتی به شیوه‌ای سازگار و به‌کارگیری خودکار این سیاست‌ها در سیستم‌های فناوری اطلاعات فراهم می‌کند.

- **زیرساخت رمزنگاری، کلید و گواهی‌نامه** سرویس‌هایی را برای انجام مؤثر عملیات رمزنگاری و فرایندها و قابلیت‌های عملی و مؤثر برای مدیریت کلیدهای رمزنگاری ارائه می‌کند.
- **زیرساخت مدیریت خدمات** شامل خدمات زیرساختی به منظور رسیدگی به فرایندهای مدیریت خدمات مانند مدیریت حادثه، مشکل، تغییر و پیکربندی می‌باشد. کنترل خودکار فرایند، خدمات مبتنی بر چارچوب کلی جهت خودکارسازی اقدامات فناوری اطلاعات از جمله فعالیت‌های مربوط به امنیت می‌باشد.
- **امنیت ذخیره‌سازی** قابلیت‌های امنیتی داده محوری را برای محافظت از داده‌های درحال استفاده، در حال انتقال و بدون استفاده از طریق قابلیت‌هایی مانند رمزنگاری فراهم می‌کند. همچنین سرویس‌هایی برای دسته‌بندی دارایی‌های ذخیره‌سازی (انباره) و سیاست‌های کنترلی مربوط به آن‌ها نیز ارائه می‌کند.
- **امنیت میزبان و نقاط انتهایی** از سرویس‌دهنده‌ها و دستگاه‌های کاربر، مانند تلفن همراه، کامپیوترهای رومیزی و کامپیوترهای همراه با استفاده از هر دو تکنولوژی مبتنی‌بر شبکه و میزبان محافظت می‌کند. این محافظت در زیرساخت‌های مجازی به منظور تأمین امنیت برای محیط‌های مجازی ادغام و تجمیع می‌شود. این مؤلفه شامل گواهی مبتنی بر سخت‌افزار سیستم‌عامل‌های میزبان و منابع سیستمی به منظور محافظت در برابر حمله‌های مخرب می‌باشد.
- **امنیت برنامه‌کاربردی** زیرساختی را برای آزمون، نظارت و ممیزی برنامه‌های کاربردی استقرار یافته فراهم می‌کند.
- **امنیت شبکه** متشکل از امنیت چند لایه‌ای شبکه به منظور فراهم کردن دفاع در عمق[1]، بازرسی عمیق[2] و تجزیه و تحلیل پروتکل‌ها، محتوا[3]های سطح برنامه کاربردی جهت محافظت از تمام سطوح

[1] Defense in-Depth
[2] Deep Inspection
[3] Payload

پشته[1] شبکه می‌باشد. این مؤلفه در شبکه‌های مجازی به منظور ایجاد امنیت در محیط‌های مجازی مدرن نیز گسترده می‌شود.

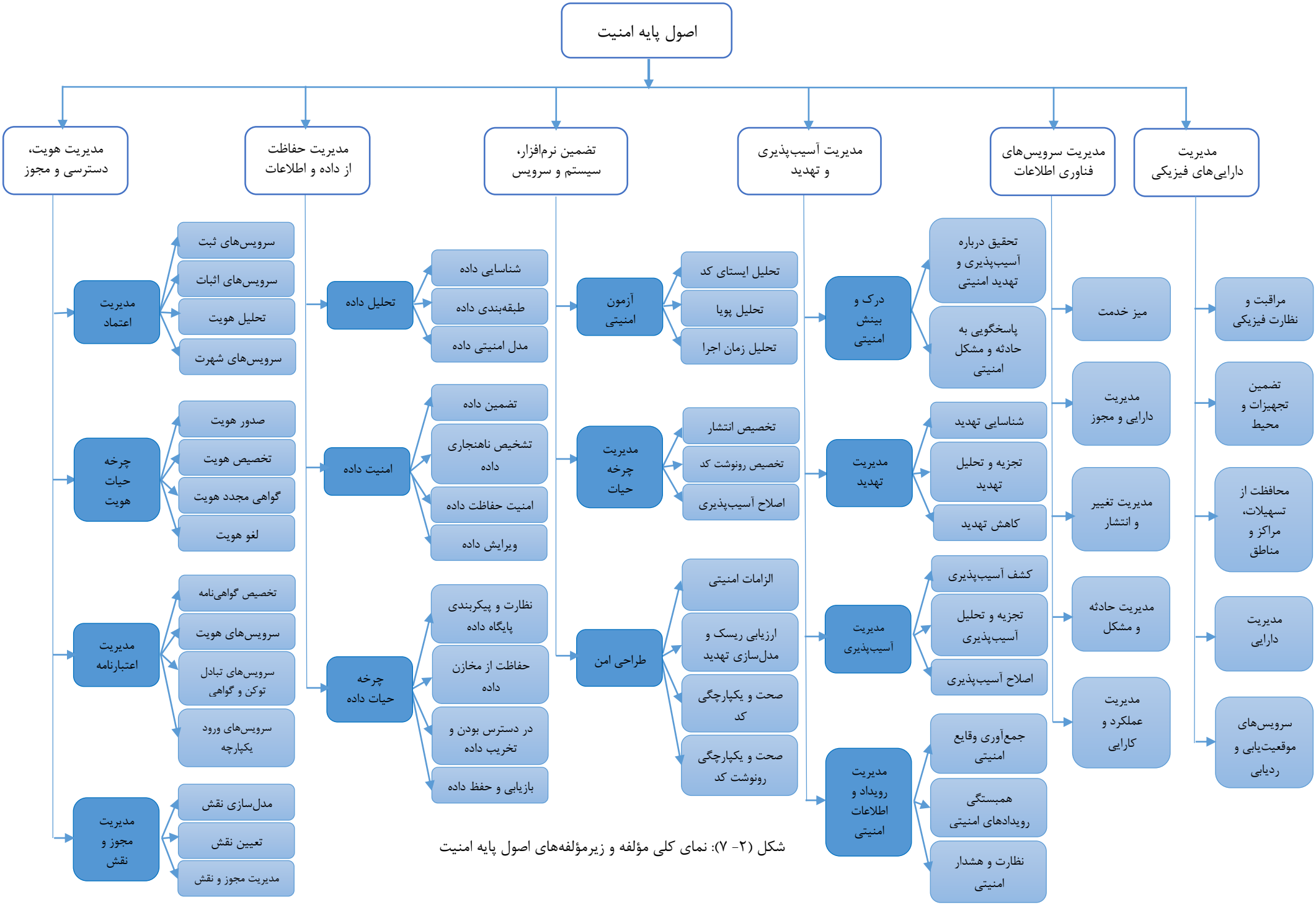
- **امنیت فیزیکی،** یک سرویس زیرساخت فناوری اطلاعات جهت فراهم کردن اطلاعاتی درباره امنیت فیزیکی و هماهنگی آن با امنیت فناوری اطلاعات است. این سرویس می‌تواند شامل نشان‌های[2] کارمندان، خوانندگان سامانه شناسایی با امواج رادیویی (RFID)[3]، سیستم‌های نظارتی و دارایی یا تکنولوژی مربوطه باشد. امنیت فیزیکی می‌تواند شامل نظارت، تشخیص حرکت، شناسایی و ردیابی اشیا و افراد، کنترل ورود، نظارت بر سیستم‌های محیطی، کنترل محیط و نظارت بر قدرت و بهره‌وری سیستم به صورت خودکار باشد.

۲-۶-۳- مؤلفه‌های اصول پایه امنیت

برای هریک از اصول امنیتی انتخابی، ویژگی‌ها، دامنه و قابلیت‌هایی تعریف می‌گردد. شکل (۲- ۷)، نمای کلی اصول پایه امنیت را به همراه زیرمؤلفه‌های آن‌ها نشان می‌دهد. مؤلفه‌های اصول پایه امنیت، قابلیت‌های امنیتی متداولی را توصیف می‌کنند که در هر محیط فناوری اطلاعات به منظور مدیریت ریسک‌های امنیتی موردنیاز هستند.

در ادامه جزئیات بیشتری درباره مؤلفه‌های اصول پایه امنیت با تقسیم‌بندی آن‌ها به زیرمؤلفه‌ها ارائه می‌شود.

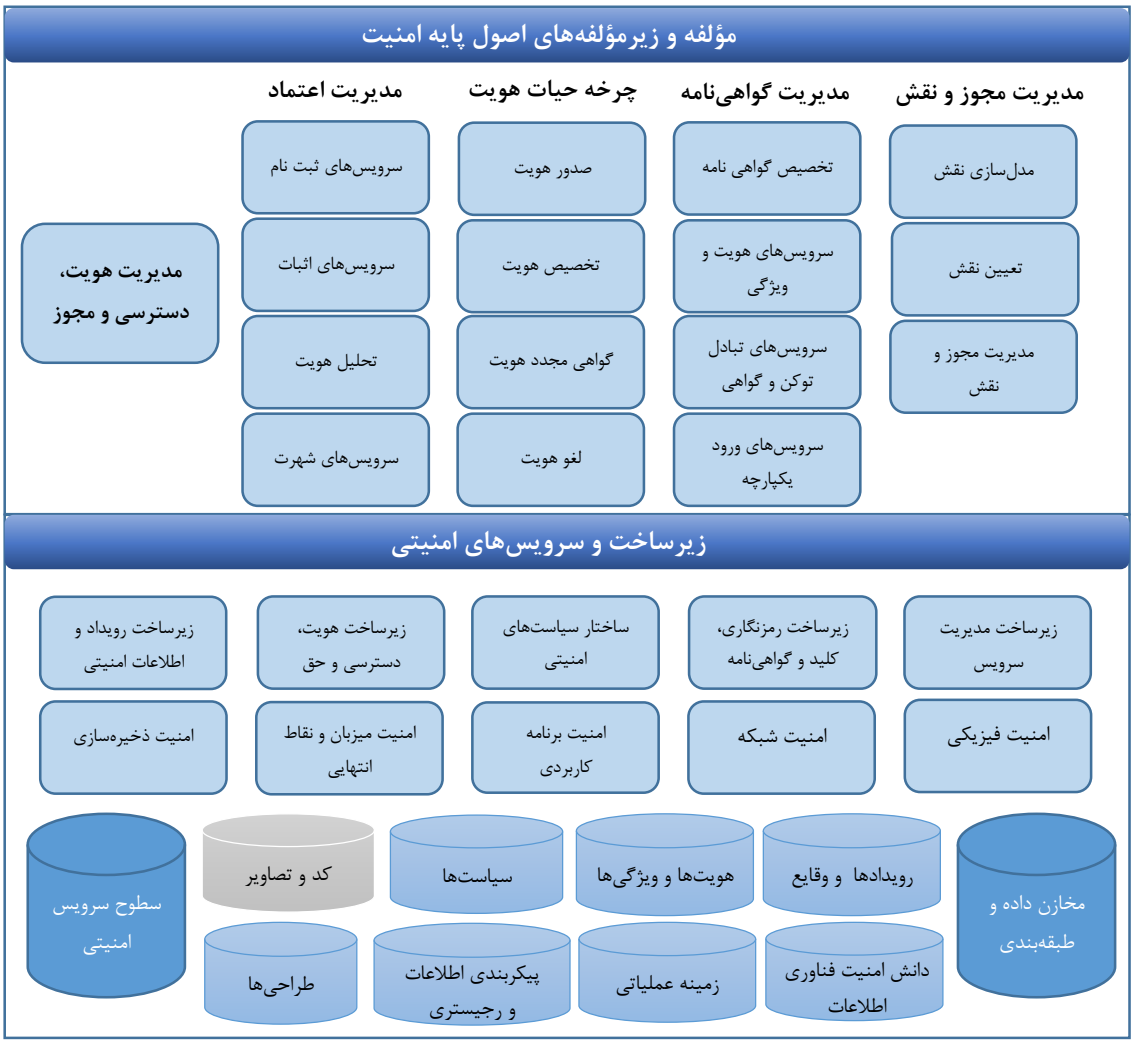
[1] Stack
[2] Badge
[3] Radio-Frequency Identification (RFID)



شکل (۲- ۷): نمای کلی مؤلفه و زیرمؤلفه‌های اصول پایه امنیت

۲-۶-۳-۱- مدیریت هویت، دسترسی و مجوز[1]

مدیریت هویت، دسترسی و مجوز سرویس‌هایی را ارائه می‌کند که به نقش‌ها و هویت‌ها، حقوق دسترسی و مجوزها وابسته هستند. استفاده صحیح از این سرویس‌ها می‌تواند تضمین کند که دسترسی به منابع برای هویت‌های صحیح، در زمان مناسب و برای اهداف مناسب اعطا شده است. همچنین این سرویس‌ها می‌توانند تضمین کنند که دسترسی به منابع برای کاربردهای غیرمجاز یا غیرقابل قبول، نظارت و ممیزی می‌شود. شکل (۲- ۸) دید کلی از زیرمؤلفه‌های مدیریت هویت، دسترسی و مجوز و نیز مؤلفه‌های مرتبط از مجموعه زیرساخت و سرویس‌های امنیتی را نشان می‌دهند.



شکل (۲- ۸): زیرمؤلفه‌های مدیریت هویت، دسترسی و مجوز به همراه زیرساخت و سرویس‌های امنیتی مربوطه

[1] Identity, Access, and Entitlement Management

توجه!

اشکال به رنگ خاکستری در شکل فوق و دیگر اشکال این بخش نشان‌دهنده سرویس‌ها یا مؤلفه‌هایی هستند که ممکن است برای وظایف مربوطه مورد نیاز نباشند.

مدیریت هویت، دسترسی و مجوز به چهار گروه مدیریت اعتماد، چرخه حیات هویت، مدیریت گواهی‌نامه و مدیریت مجوز و نقش تقسیم می‌شود:

- **مدیریت اعتماد:** مدیریت اعتماد به فعالیت‌هایی اشاره دارد که برای بهبود قابلیت اطمینان سیستم‌های مدیریت هویت به منظور تضمین صدور گواهی‌نامه برای افراد مجاز، مورد نیاز هستند. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
  - *سرویس‌های ثبت‌نام:* سرویس‌های ثبت‌نام عمل جمع‌آوری مستندات اولیه از افرادی که متقاضی صدور گواهی هستند را پوشش می‌دهد. این مؤلفه ممکن است شامل جمع‌آوری اطلاعات بیومتریک و بیوگرافی نیز باشد.
  - *خدمات تصدیق*[1]*:* خدمات تصدیق، فرایندها و فناوری‌هایی برای اعتبارسنجی تمام اطلاعاتی هستند که از افراد توسط سرویس‌های ثبت‌نام جمع‌آوری می‌شوند. علاوه‌بر تایید اطلاعات با مقایسه با منابع معتبر، این مؤلفه ممکن است از تجزیه و تحلیل هویت برای تشخیص نرم‌افزارهای تقلبی نیز استفاده کند.
  - *سرویس‌های تلفیق هویت*[2]*:* سرویس‌های تلفیق هویت، فرایندها و تکنیک‌هایی جهت شناسایی سوابق متعدد برای یک شخص، که ممکن است به صورت سهوی (تصادفی) یا تقلبی ایجاد شده باشد، را پوشش می‌دهد و آن‌ها را برای هر شخص در یک رکورد تلفیق می‌کند.

[1] Proofing Services
[2] Identity Resolution Services

- *سرویس‌های شهرت*[1]: سرویس‌های شهرت شامل پیگیری فعالیت‌ها و اقدامات یک فرد در طول زمان، جمع‌آوری نظرات دیگران (یا از افراد دیگر یا از سیستم‌های رتبه‌بندی) درخصوص این اقدامات و فعالیت‌ها و انتشار یک ارزیابی از نظرات (به صورت عمومی یا به صورت خصوصی به فرد مورد نظر) به عنوان یک مکانیزم بازخورد می‌باشد.

- **چرخه حیات هویت:** محدوده چرخه حیات هویت از اولین رویداد برای ایجاد آن تا در نهایت حذف یک هویت می‌باشد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
  - *تخصیص*[2] *هویت:* تخصیص هویت، فرایندها و فناوری‌های مربوط به ایجاد گواهی‌نامه‌ها را پوشش می‌دهد که این گواهی‌نامه‌ها در زمان صدور یک توکن هویت (به عنوان مثال، کارت هویت ملی) و نیز ثبت گواهی‌نامه در سیستم‌هایی که باید گواهی‌نامه را احرازهویت کنند، مورد استفاده قرار می‌گیرند.
  - *صدور هویت*[3]: صدور هویت فرآیندها و فناوری‌هایی را پوشش می‌دهد که برای ایجاد مؤلفه‌های فیزیکی گواهی‌نامه و تحویل امن آن به صاحبان آن‌ها استفاده می‌شود.
  - *گواهی مجدد هویت*[4]: گواهی مجدد هویت به فرایندها و فناوری‌هایی اشاره دارد که برای اعتبارسنجی مجدد یک گواهی‌نامه که در حال حاضر صادر شده است، استفاده می‌شود. در موارد خاص، این وضعیت بدان معنی است که شما فقط خود گواهی‌نامه را به‌روزرسانی می‌کنید. به عنوان مثال، یک گواهی‌نامه دیجیتالی منقضی شده است و باید یک گواهی‌نامه دیگر صادر شود. در موارد دیگر، گواهی مجدد شامل مجوزدهی مجدد و ارائه اطلاعاتی است که باید مجدداً اثبات شوند.

---

[1] Reputation Services
[2] Provisioning
تخصیص، فرایند هماهنگی ایجاد حساب‌های کاربری و کارهای دیگری مانند تخصیص منابع فیزیکی مربوط به فعال‌سازی کاربران جدید می‌باشد.
[3] Identity Issuing
[4] Identity Recertification

- *لغو هویت*[1]: لغو هویت فرایندها و فناوری‌های مورد استفاده جهت لغو اعتبار یک گواهی‌نامه را پوشش می‌دهد به‌طوری‌که دیگر به‌عنوان یک توکن شناسایی قابل استفاده نمی‌باشد. این وضعیت می‌تواند به وسیله یک رویداد محرک خارجی اتفاق بیفتد یا به طور طبیعی منقضی شود. به عنوان مثال، یک گواهی‌نامه دیجیتالی لغو شده ممکن است در یک لیست ابطال گواهی که توسط زیرساخت هویت بررسی می‌شود منتشر شود.

- **مدیریت گواهی‌نامه**: مدیریت هویت با مدیریت اطلاعات گواهی‌نامه و اطلاعات مربوط به هویت سروکار دارد. علاوه بر مدیریت کردن گواهی‌نامه‌ها در قالب الکترونیکی، مدیریت گواهی‌نامه شامل مدیریت گواهی‌نامه‌های فیزیکی، مانند توکن‌ها یا نشان‌ها، نیز می‌باشد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
  - *تخصیص گواهی‌نامه:* تخصیص گواهی‌نامه، فعال‌سازی گواهی‌نامه‌های صادر شده را پوشش می‌دهد به طوری که از آن می‌توان برای تصدیق هویت یک فرد و همچنین برای سرویس‌هایی جهت به‌روزرسانی، حذف و مدیریت گواهی‌نامه‌های هویت مورد اعتماد در تمام چرخه حیات استفاده کرد.
  - *خدمات هویت و ویژگی*[2]: خدمات هویت و ویژگی، دسترسی به رجیسترها[3] و پایگاه داده‌های محلی کاربر که ارائه‌دهنده اطلاعاتی درباره هویت می‌باشند را مدیریت می‌کنند. معمولاً خدمات هویت و ویژگی علاوه بر خواندن هویت، قادر به اضافه یا حذف اطلاعات مربوط به آن نیز هستند. این خدمات توسط سرویس‌های احرازهویت در هنگام ارزیابی مدارک احرازهویت ارائه شده و همچنین در زمان ایجاد مجوزهای مورد استفاده توسط سرویس‌های مدیریت نشست استفاده می‌شوند. امتیازات معمولاً بر اساس ویژگی‌های ذخیره شده کاربر

[1] Identity Revocation
[2] Identity and Attribute Services
[3] Register

در خدمات امنیتی هویت و ویژگی، مانند عضویت در گروه، نقش‌ها و ویژگی‌های فردی، می‌باشند.

- *سرویس‌های تبادل توکن و گواهی‌نامه:* سرویس‌های تبادل توکن و گواهی‌نامه، اعتبارسنجی و صدور توکن را جهت تبدیل یک نوع از توکن امنیتی به نوع دیگر انجام می‌دهند. توکن‌های امنیتی با روش‌های مختلفی مانند امضاء بر روی توکن، ساختار مورد انتظار و محتوای توکن تصدیق می‌شوند. صدور توکن شامل ایجاد یک توکن معتبر محلی و جدید براساس یک توکن دریافت شده معتبر می‌باشد. هنگامی که این توکن جدید به درخواست‌دهنده اصلی برمی‌گردد، این فرایند به عنوان یک فرایند تبادل توکن تلقی می‌گردد.
- *خدمات ورود یکپارچه*[1]*:* این قابلیت برای برطرف کردن مشکل ورود کاربر با نام‌های کاربری و رمزهای عبور متعدد به سیستم‌های مختلف برای دسترسی به منابع می‌باشد. معمولاً، یک ارائه‌دهنده هویت می‌تواند به عنوان یک واسط از طرف درخواست‌کننده عمل کرده و مدارک احرازهویت درخواست‌کننده را که مورد نیاز اشخاص ثالث می‌باشد، ارائه نماید.

- **مدیریت مجوز و نقش**: مدیریت مجوز و نقش در برگیرنده تمام سرویس‌های کاربردی است که مربوط به گروه‌بندی هویت‌ها و مدیریت دسترسی به اطلاعات و منابع در یک گروه می‌شوند.
  - *مدل‌سازی نقش:* مدل‌سازی نقش با طراحی ساختار نقش‌ها جهت برطرف کردن نیازمندی‌های به دست آمده از فعالیت‌های فناوری اطلاعات و کسب‌وکار سروکار دارد. هدف مدل‌سازی نقش کاهش پیچیدگی بازیگران با گروه‌بندی آن‌هاست به طوری که منجر به کاراتر شدن قابلیت ارائه و محدود کردن دسترسی به اطلاعات و دیگر منابع می‌شود. با استفاده از مدل‌سازی نقش، روش تفکیک وظایف کمتر دچار خطا خواهد شد.

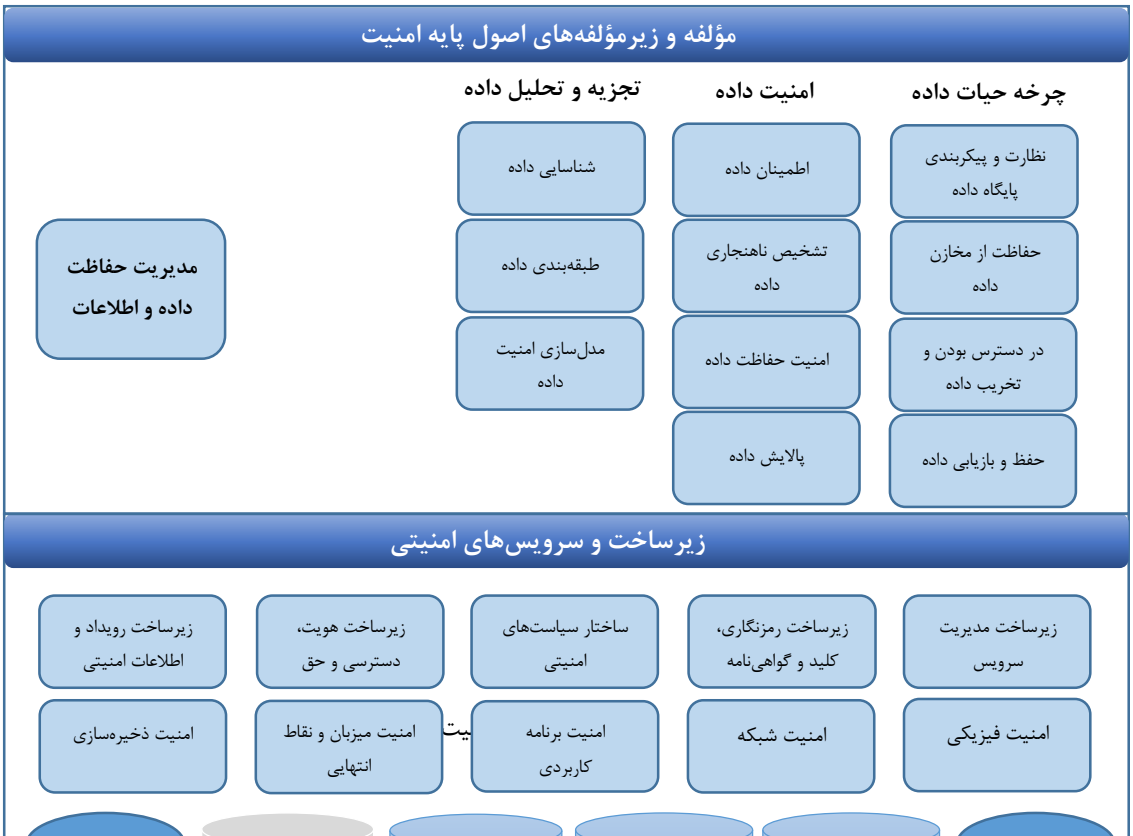
[1] Single Sign-on Services

- *شناسایی نقش:* این زیرمؤلفه به شناسایی نقش‌ها و مجوزهای مربوط به آن‌ها اشاره دارد. اطلاعات ضروری درباره نقش‌ها و مجوزها می‌تواند به صورت دستی با مشاهده و تجزیه و تحلیل فرایندها و مصاحبه با صاحبان فرایند جمع‌آوری شود.
- *مدیریت مجوز و نقش:* مدیریت مجوز و نقش به فعالیت‌های پیرامون نگه‌داری و به‌روزرسانی ساختارهای مجوز و نقش می‌پردازد. این مؤلفه بسیار شبیه به مؤلفه مدیریت هویت می‌باشد.

۲-۶-۳-۲- مدیریت حافظت از اطلاعات و داده

مدیریت حافظت از داده و اطلاعات سرویس‌هایی را فراهم می‌کند که از داده‌های ساخت یافته و بدون ساختار در برابر افشای غیرمجاز، تغییر و حذف، با توجه به طبیعت و ارزش کسب‌وکار اطلاعات محافظت می‌کنند. همچنین استفاده و دسترسی به سرویس‌های نظارتی و ممیزی را نیز ارائه می‌کند. امروزه فناوری اطلاعات عناصر اصلی اکثر فرایندهای کسب‌وکار از جمله تراکنش‌ها و داده‌ها را فراهم می‌کند. بنابراین مدیریت حافظت از داده‌ها و اطلاعات، از تراکنش‌ها و داده‌های سازمان به منظور اطمینان از این که داده‌ها (که شامل تراکنش‌ها نیز می‌شود) به طور کامل، دقیق و مناسب محافظت شده و در دسترس هستند، پشتیبانی می‌کند.

شکل (۲- ۹) دید کلی از زیرمؤلفه‌های محافظت از داده و اطلاعات و نیز مؤلفه‌های مرتبط از مجموعه زیرساخت و سرویس‌های امنیتی را نشان می‌دهد.



شکل (۲- ۹): زیرمؤلفه‌های مدیریت حافظت از داده و اطلاعات به همراه زیرساخت و سرویس‌های امنیتی مربوطه

مدیریت محافظت از داده و اطلاعات به سه زیرمؤلفه تجزیه و تحلیل داده، امنیت داده و چرخه حیات داده تقسیم می‌شود:

- **تجزیه و تحلیل داده:** تمرکز اصلی آن بر روی شناسایی داده، طبقه‌بندی داده و مدل‌سازی داده در سازمان می‌باشد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
- *شناسایی داده:* بخش مهمی از تجزیه و تحلیل داده، داشتن فهرست دقیقی از مخازن[1] داده سازمان و درک ریسک‌های امنیتی مربوط به آن‌ها می‌باشد. در واقع شناسایی داده، فرآیند شناسایی تمام مخازن داده در یک سازمان و تجزیه و تحلیل شِما[2] و ارزش داده و الگوی آن‌ها جهت شناسایی ارتباط بین عناصر پایگاه داده می‌باشد. یک سازمان بایستی آگاه باشد که چه اشخاصی و چگونه از داده‌ها استفاده می‌کنند، خواه داده‌هایی که از مرزهای کسب‌وکار خارج می‌شوند و خواه داده‌هایی که برای تولید یا آزمون استفاده می‌شوند. شناسایی داده شامل در نظر گرفتن روابط داده‌ها در تمام مخازن، درک ارتباط آن‌ها با هم و نحوه سازماندهی این روابط به منظور ارائه اهداف کسب و کار سازمان می‌باشد. همچنین شناسایی داده هنگام جابه‌جایی داده‌ها در بین مخازن، تغییرات و شرایط منطقی که بر روی داده‌ها اعمال می‌شوند را نیز تشخیص می‌دهد.

[1] Storages
[2] Schema

- *طبقه‌بندی داده*: طبقه‌بندی داده‌ها شامل ابزارها و فرآیندهایی است که برای ایجاد مجموعه مشترکی از برچسب‌های معنایی که توسط طراحان داده، تحلیل‌گران اطلاعات، تحلیل‌گران کسب‌وکار و معماران داده استفاده می‌شود، به کار می‌رود. طبقه‌بندی داده یک فاکتور مهم برای سیاست‌های امنیت و حریم خصوصی می‌باشد. طبقه‌بندی داده‌ها، دو سطح را مدیریت می‌کند که عبارتند از طبقه‌بندی سطح کسب‌وکار و طبقه‌بندی داده منطقی.

در سطح کسب‌وکار، مجموعه‌ای از طبقه‌بندی‌های کسب‌وکار، تعاریف آن‌ها و چگونگی ارتباط آن‌ها با مدل داده منطقی، فهرستی از واژگان مشترک کسب‌وکار را ایجاد می‌کنند که در سراسر سازمان جهت تضمین این که هر بخش از سازمان بر روی تعریف این واژگان توافق دارند، استفاده می‌شود. این وضعیت در واقع به کاهش سردرگمی و سوءتفاهم در سطح مذاکرات کسب‌وکار کمک می‌نماید و همچنین از طریق کاهش خطاها منجر به بهبود قابلیت همکاری در سراسر سازمان فناوری اطلاعات می‌گردد.

- *مدل‌سازی امنیت داده*[1]: مدل‌سازی امنیت داده به فعالیت‌های انجام شده توسط معمار داده برای تعریف مدل‌های داده منطقی، مدل‌های داده فیزیکی و مدل‌های اطلاعاتی خاص دامنه اشاره دارد. مدل‌سازی امنیت داده بر روی انواع داده تعریف شده توسط یک سازمان یا یک استاندارد صنعتی محدودیت‌هایی را اعمال می‌کند. این محدودیت‌ها، محدودیت‌های کسب و کار هستند که قابلیت همکاری بین سیستم‌ها و سازمان‌ها را فراهم می‌کنند. به عنوان مثال کدهای انتقال بانکی نشان‌دهنده یک رشته عددی هستند که قوانین خاصی را در فرمت خاص خود دنبال می‌کنند و برای انتقالات بین بانکی تفسیر می‌شوند. نوع دیگری از محدودیت می‌تواند مربوط به حریم خصوصی باشد. مدل‌های داده منطقی، نشان‌دهنده ساختار انتزاعی[2] یک دامنه از اطلاعات می‌باشد. مدل‌های داده منطقی بعضی مواقع در چرخه حیات توسعه نرم‌افزار نادیده گرفته

[1] Data Security Modeling
[2] Abstraction

می‌شوند اما این مدل‌ها به طور فزاینده‌ای در زمینه معماری سرویس‌گرا[1] مهم می‌باشند. مدل داده منطقی این قابلیت را برای معماران داده فراهم می‌کند که نمایی کلی از موجودیت‌های داده در یک نرم‌افزار یا فراسازمان را بدون داشتن جزئیات پیاده‌سازی ترسیم نمایند. مدل‌های داده منطقی اغلب به عنوان ورودی برای سایر فعالیت‌های معماری فراسازمانی مانند تعریف فرمت‌های پیام و واسط‌های سرویس استفاده می‌شوند.

مدل‌های داده فیزیکی، مدل‌های مخصوص پایگاه داده هستند که اشیای داده رابطه‌ای و ارتباط آن‌ها را ارائه می‌کنند (به عنوان مثال جدول‌ها، ستون‌ها، کلیدهای اصلی و خارجی). هریک از این لایه‌های مدل می‌توانند دارای محدودیت‌های امنیتی باشند که به آن‌ها پیوست می‌گردد و الزاماتی را برای محرمانگی و رمزنگاری، کنترل دسترسی و مبهم‌سازی تعریف می‌نمایند.

- **امنیت داده:** تمرکز امنیت داده جهت استفاده عملیاتی از اطلاعات در دو سطح ریز و کلان می‌باشد. امنیت داده دید بسیار جزئی از سیستم‌های پایگاه داده را به منظور حفاظت از صحت داده‌ها فراهم می‌نماید. این دید مستلزم قرار دادن ارزشی برای دارایی‌های داده و اجرای حفاظت امنیتی مناسب براساس این ارزش‌گذاری می‌باشد. این ارزیابی مستلزم استانداردسازی[2] تنظیمات، فرآیندها و شیوه‌هایی برای پایگاه داده‌ها در سراسر یک سازمان می‌باشد. همچنین امنیت داده از شناسایی و طبقه‌بندی داده به منظور دانستن نحوه استفاده از داده‌ها (توسط چه فرآیندی) و اطلاع از نوع داده‌ها (با استفاده از طبقه‌بندی)، استفاده می‌کند.

یک دید سطح کلان از داده و سیستم‌های پایگاه داده در سازمان نیز وجود دارد. این دیدگاه نه تنها شامل خود داده می‌شود بلکه شامل تعریف، تعیین مرجع داده و فراداده برای این داده‌ها نیز می‌گردد. در دیدگاه فراسازمانی داده‌ها، نحوه حفاظت، ذخیره‌سازی، ارزش‌گذاری و استفاده از داده‌ها توسعه می‌یابد. همچنین داده‌ها در سراسر سازمان تعریف و مرتبط می‌گردند و یک تصویر واضحی از داده و نحوه استفاده از آن ارائه می‌شود. امنیت داده در داده‌های قابل استفاده و بدون استفاده در نظر

[1] Service-oriented Architecture
[2] Standardizing

گرفته می‌شود. امنیت داده شامل تضمین داده[1]، تشخیص ناهنجاری داده، امنیت حفاظت از داده و ویرایش داده[2] می‌باشد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:

- *تضمین داده:* تضمین داده به ابزارها و فعالیت‌هایی اشاره دارد که به منظور اطمینان از اصلاح[3] و استانداردسازی داده‌ها قبل از استفاده برای یک مدل تعریف شده، به کار می‌روند. تضمین داده همچنین منبع داده را هنگامی که داده‌هایی از طریق قابلیت ممیزی دریافت می‌شوند، ردیابی می‌نماید. فرآیند تضمین داده یک نقطه بررسی[4] (ایستگاه بازرسی) برای الزامات تجمیع، ویرایش و مبهم‌سازی به منظور حصول اطمینان از محرمانه بودن و حفظ حریم خصوصی فراهم می‌کند.
- *تشخیص ناهنجاری داده:* تشخیص ناهنجاری داده، اقدامات حفاظتی موجود جهت شناسایی و جلوگیری از تقلب را توصیف می‌نماید. تکنیک‌های پیشگیری و تشخیص ناهنجاری داده به سرعت در چند سال اخیر با استفاده از شبکه‌های عصبی و تکنیک‌های داده‌کاوی گسترش یافته‌اند. روش تشخیص ناهنجاری تضمین می‌کند که سازمان‌ها، اطلاعات مبتنی بر استانداردهای تعریف شده را جمع‌آوری نمایند و همچنین یک رویکرد فراسازمانی در سازمان‌ها جهت تشخیص تقلب، همبستگی، تجزیه و تحلیل و مدیریت گزارشات وجود دارد. روش‌ها و رویکردها بایستی بر اساس استانداردها و معیارهای تعریف شده باشند. سازمان‌ها بایستی تشخیص تقلب را با سایر فرآیندهای دولتی، مدیریت حادثه[5] و مدیریت تغییر مشکلات، استفاده از مجوزهای پیشرفته، تبادل اطلاعات با اشخاص ثالث و سیاست‌های منتشر شده در رابطه با تقلب درنظر بگیرند و این به عنوان یک روش مناسب جهت ارائه موارد ذیل در نظر گرفته شده است:
    - فرآیندهایی به منظور ارائه و ثبت شواهدی برای پیگیری و ردیابی تقلب

[1] Data Assurance
[2] Data Redaction
[3] Cleansed
[4] Checkpoint
[5] Incident Management

- مهارت‌ها و تکنولوژی‌های اختصاصی
- آموزش و آگاهی کارمندان
- آگاهی برای اشخاص ثالث
- مکانیزم پاسخ بی‌درنگ به رویدادها
- بررسی فرآیند ممیزی سالانه برای تشخیص تقلب

○ *امنیت حفاظت از داده:* امنیت حفاظت از داده، صحت داده، رمزنگاری، احرازهویت، مجوزدهی و اقدامات ممیزی را برای داده‌های بدون استفاده و قابل استفاده که از سیاست‌های امنیتی و سرویس‌های زیرساخت رمزنگاری استفاده می‌کنند، ارائه می‌نماید.

رمزنگاری تضمین می‌کند که داده‌های بدون استفاده و قابل استفاده به درستی با استفاده از سرویس‌های رمزنگاری محافظت شده و همچنین از الزامات تعیین شده در سیاست امنیتی تبعیت می‌نمایند.

احرازهویت و مجوزدهی تضمین می‌نمایند که داده‌ها برای موجودیت‌ها و فرآیندهای غیرمجاز فاش نمی‌شوند. فرآیندهای احرازهویت، فرایند ممیزی واضحی را در مورد این که حق دسترسی به چه کسی یا چه فرآیندی اعطا گردد ایجاد می‌نمایند.

اقدامات ممیزی، امکان ردیابی و پیگیری این که چه شخصی یا چه فرآیندی به چه اطلاعاتی در هر لحظه از زمان دسترسی داشته است را فراهم می‌کنند.

○ *ویرایش داده:* به مجموعه ابزارها و روش‌هایی اشاره دارد که قبل از تحویل داده‌ها به گیرنده، داده‌های حساس یا محرمانه را بر اساس قوانین سیاست حذف می‌نمایند. روش‌های ویرایش داده می‌توانند برای داده‌های بدون ساختار مانند مجموعه‌ای از اسناد واژه‌پردازی یا داده‌های ساخت‌یافته در پایگاه داده استفاده شوند.

○ **چرخه حیات داده:** چرخه حیات داده، امنیت داده را در هر روشی و در هر زمانی که داده ذخیره شده، با توجه به چرخه حیات آن، در نظر می‌گیرد. همچنین از صحت، محرمانگی، حریم خصوصی و

دسترس‌پذیری داده‌ها با توجه به ذخیره‌سازی طولانی مدت داده‌ها محافظت می‌کند و کنترل‌هایی در خصوص دسترسی به داده‌ها، تا هنگامی که داده‌ها ذخیره شده‌اند، درنظر می‌گیرد. همچنین کیفیت ذخیره‌سازی داده را برای حصول اطمینان از این که هیچ‌گونه کمبودی در الزامات موردنیاز چرخه حیات ذخیره‌سازی، دسترسی و استفاده از داده‌ها وجود ندارد، پوشش می‌دهد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:

- *نظارت و پیکربندی پایگاه داده:* نظارت و پیکربندی مناسب پایگاه داده تضمین می‌نماید که دارایی‌های اطلاعاتی با توجه به حساسیت کسب‌وکار محافظت می‌شوند. هرچه داده‌های موجود در پایگاه داده بحرانی‌تر باشند؛ بایستی کنترل‌های مورد نیاز برای محرمانگی، صحت، حریم خصوصی و دسترس‌پذیری به صورت مناسب‌تری انتخاب شوند.
- *حافظت از مخازن داده:* اشاره به این دارد که چگونه اطلاعات در مخازن ذخیره می‌شوند. خواه مخزن یک رایانه قابل حمل، یک رایانه رومیزی، یک سرویس‌دهنده، یک انباره کمکی یا رسانه جداشدنی باشد. محافظت از محل ذخیره داده تضمین می‌کند که یک توافق گسترده سازمانی بر روی حفاظت، کنترل دسترسی به رسانه‌های قابل حمل، یک سیاست تعریف شده و اجرایی برای حفاظت از دستگاه‌های ذخیره‌سازی، استفاده از سیستم‌فایل رمزگذاری شده برای ذخیره‌سازی داده‌ها، قابلیت‌های مدیریت تهدید مانند محیط‌های عملیاتی استاندارد، امنیت پایگاه داده و صحت سیستم‌ها وجود دارد.
- *تخریب داده:* اشاره به ابزارها و فرآیندهایی دارد که داده‌های یک سیستم که برای طولانی مدت موردنیاز و استفاده نبوده و یا براساس قانون یا سیاست، لزومی به حفظ آن‌ها نمی‌باشد را حذف می‌کند. در واقع تخریب داده، روند به پایان رسیدن چرخه حیات اطلاعات و تخریب آن‌ها می‌باشد. در صورتی که فرآیندهای تخریب داده به صورت عمدی روشی را برای بازیابی داده‌های تخریب شده به کار ببرند، می‌توانند منجر به یک ریسک امنیتی شوند. فرآیندها و ابزارهای تخریب داده بر اساس ارزش، میزان حساسیت داده‌ها و تکنیک‌هایی که یک

حمله‌کننده ممکن است جهت بازیابی داده‌های تخریب شده به کار گیرد، تعیین می‌شوند و بایستی برای خنثی نمودن تهدیدات احتمالی در برابر بازیابی داده‌ها، طراحی گردند. تکنیک‌ها و فرآیندهای تخریب داده گاهی اوقات به وسیله قوانین و سیاست‌هایی مشخص می‌گردند. به عنوان مثال ممکن است جهت کاهش احتمال بازیابی داده‌ها در آینده قانونی نیاز باشد که داده‌ها چندین بار با اطلاعات تصادفی بازنویسی شوند.

- *حفظ و بازیابی داده:* قابلیت بازیابی داده ابزارها و فرآیندهای پشتیبانی[1] و بایگانی[2] را پوشش می‌دهد. پشتیبان‌گیری به ابزارها و فعالیت‌های مربوط به بازگردادن خدمات به یک نقطه شناخته شده هنگام رخ دادن واقعه‌ای در یک سیستم یا رسانه در صورت خرابی، اشاره دارد. بایگانی، به ابزارها و فرآیندهای مورد استفاده برای حذف تراکنش‌ها از سیستم فعالی که برای طولانی مدت موردنیاز نمی‌باشد اما برای الزامات قانونی بایستی حفظ گردند، اشاره دارد. اگرچه تکنیک‌های پشتیبان‌گیری برای رسانه‌ها و یا فعالیت در سطح فایل به کار برده می‌شوند، قابلیت‌های بایگانی بایستی اغلب از تراکنش‌ها مطلع باشند. به عنوان مثال یک رکورد کامل از یک تراکنش کسب وکار ممکن است نیاز به نگهداری داده‌ها از چندین جدول در پایگاه داده‌های متعدد و حتی حفظ اسناد غیرساخت‌یافته مختلف داشته باشد. در مجموع، مجموعه‌ای از داده‌های ساخت‌یافته و غیرساخت‌یافته برای حفظ یک تراکنش موردنیاز می‌باشند.

ابزارها و تکنیک‌های حفظ داده مؤلفه مهمی از یک سیستم مدیریت سوابق می‌باشند که قابلیت مدیریت تصمیم‌گیری در مورد آنچه که باید نگه داشته شود و در موارد خاص، آنچه که بایستی مطابق با سیاست حذف گردد را به فرآیندها اضافه می‌کنند. بازیابی داده به ملاحظات امنیتی درباره بازیابی طولانی مدت داده از مخزن یا بایگانی نیز اشاره دارد. این امر وجود یک رویکرد تعریف شده اجرایی و فرآیندها و استانداردهای فراسازمانی، تفکیک وظایف،

[1] Backup
[2] Archive

قابلیت ممیزی و یک رابط برای سایر فرآیندها را تضمین می‌کند. علاوه بر این تضمین می‌کند که سازمان‌ها امکان بازیابی داده‌ها را حفظ می‌کنند و از بازیابی کلید برای مخازن رمزگذاری شده از طریق استفاده از کلیدهای بلندمدت یا تغییرات کلید در طول بازیابی داده استفاده می‌کنند.

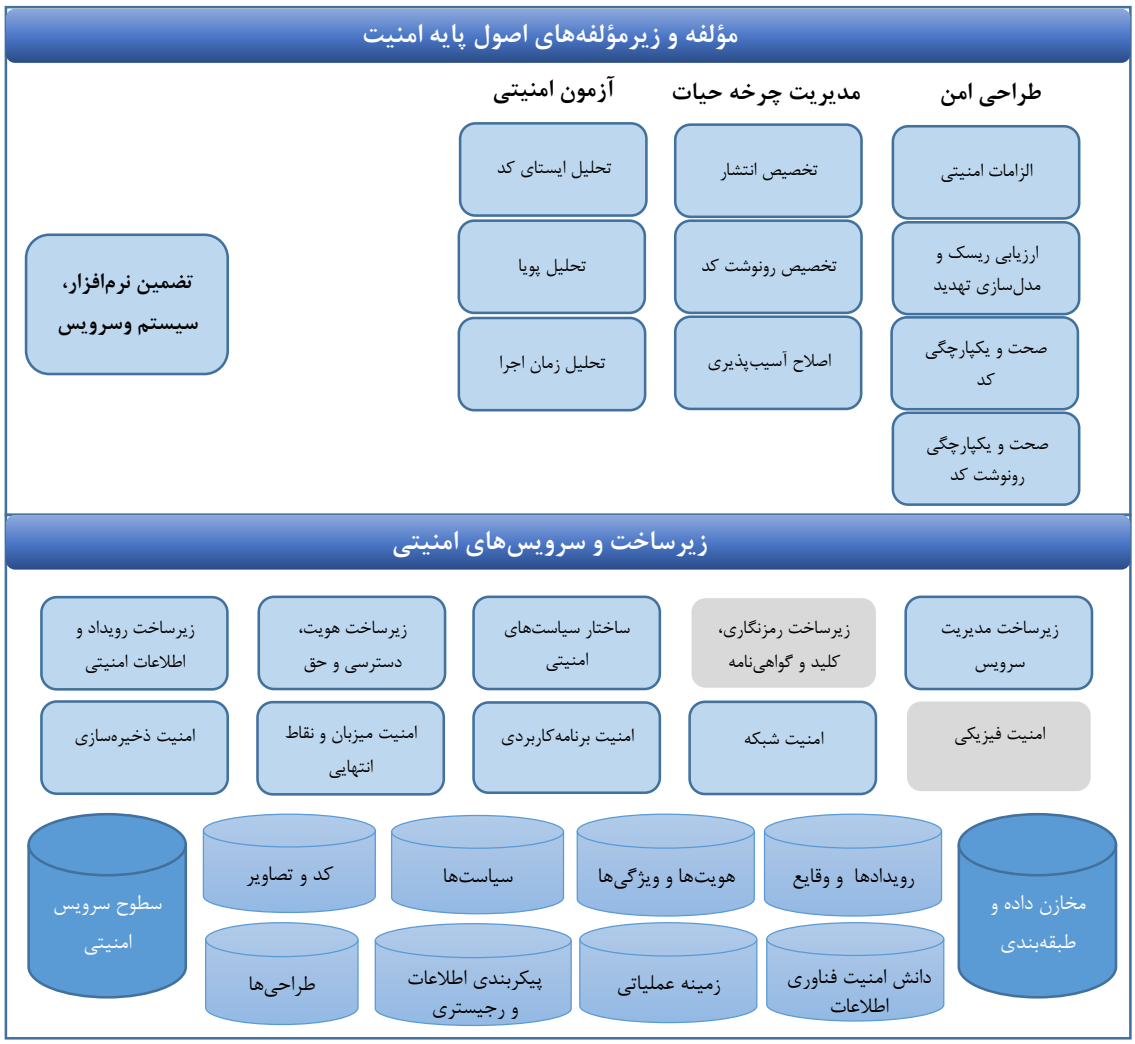
۲-۶-۳-۳- تضمین نرم‌افزار، سیستم و سرویس[1]

تضمین نرم‌افزار، سیستم و سرویس بیان می‌کند که نرم‌افزار، سیستم‌ها و سرویس‌ها در طی چرخه حیات نرم‌افزار جهت ایجاد نرم‌افزار امن، چگونه طراحی، توسعه، آزمون، اجرا و نگه‌داری شوند. این مؤلفه طراحی ساخت‌یافته، مدل‌سازی تهدید، ارزیابی ریسک نرم‌افزار، بازبینی طراحی برای امنیت، بازبینی و تحلیل کد منبع، تجزیه و تحلیل پویای برنامه کاربردی، کنترل کد منبع و نظارت بر دسترسی، امضاء و تایید کد یا بسته[2]، آزمون تضمین کیفیت و اعتبارسنجی کد شخص ثالث و تأمین‌کننده را پوشش می‌دهند.

انواع مؤلفه‌های مورد نیاز بر اساس این که در چه بخشی از چرخه حیات توسعه نرم‌افزار یک سازمان حضور دارند و نحوه توسعه نرم‌افزار، سیستم و سرویس‌ها متفاوت هستند. به عنوان مثال، نرم‌افزار می‌تواند به‌صورت داخلی توسعه یابد یا می‌تواند خریداری و نصب شود. همچنین ممکن است توسط یک ارائه‌دهنده‌ی ابر عمومی[3] ارائه شود. در صورتی که نرم‌افزار به صورت داخلی توسعه یابد (حتی اگر بخشی از توسعه برون‌سپاری شود)، تمام زیرمؤلفه‌های آن قابل اجرا هستند. هنگامی که نرم‌افزار خریداری گردد، تمرکز باید بر روی زیرمؤلفه‌های مدیریت چرخه حیات و آزمون امنیت باشد، اما همچنان این موضوع مهم است که اطمینان حاصل شود که یک توسعه‌دهنده نرم‌افزار از شیوه‌های طراحی امن استفاده کند. اگر یک برنامه کاربردی یا سرویسی در یک ابر عمومی ارائه شود، ارائه‌دهنده سرویس باید مسئول اکثر زیرمؤلفه‌ها باشد.

[1] Software, System, and Service Assurance
[2] Package
[3] public cloud provider

شکل (۲- ۱۰) دید کلی از زیرمؤلفه‌های تضمین نرم‌افزار، سیستم و سرویس و نیز مؤلفه‌های مرتبط از مجموعه زیرساخت و سرویس‌های امنیتی را نشان می‌دهد.



شکل (۲- ۱۰): زیرمؤلفه‌های تضمین نرم‌افزار، سیستم و سرویس به همراه زیرساخت و سرویس‌های امنیتی مربوطه

تضمین نرم‌افزار، سیستم و سرویس به سه گروه طراحی امن، مدیریت چرخه حیات و آزمون امنیتی تقسیم می‌شود:

- **طراحی امن**[1]: شامل سیاست‌ها و فرآیندهایی است که برای توسعه و استقرار نرم‌افزار، سیستم‌ها و سرویس‌ها موردنیاز هستند. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
  - *الزامات امنیتی*[2]: مانند الزامات عملیاتی و اجرایی، الزامات امنیتی جهت تضمین این که امنیت از همان ابتدا برای نرم‌افزار در نظر گرفته می‌شود، ضروری می‌باشند. الزامات امنیتی مشخص

[1] Secure Design
[2] Security Requirements

می‌نمایند که چه ویژگی‌های امنیتی موردنیاز هستند و چگونه این ویژگی‌ها بایستی تغییر یابند تا شامل ویژگی‌های امنیتی ضروری شوند. هدف از الزامات امنیتی تضمین حفاظت برنامه‌های کاربردی در برابر حملات می‌باشد. به عنوان مثال، موضوعات ذیل نمونه‌هایی از الزامات امنیتی هستند که شامل امنیت انتها به انتها برای یک برنامه کاربردی می‌باشند:

- ممیزی و ثبت وقایع
- احرازهویت و مجوزدهی
- مدیریت نشست[1]
- اعتبارسنجی ورودی و رمزنگاری خروجی[2]
- مدیریت استثنا[3]
- صحت و رمزنگاری
- داده‌های بدون استفاده
- داده‌های قابل استفاده
- مدیریت پیکربندی

○ *ارزیابی ریسک و مدل‌سازی تهدید:* مدل‌سازی تهدید اجازه می‌دهد تا گروه‌های توسعه، ریسک‌ها و حملات بالقوه علیه یک برنامه کاربردی را قبل از وقوع آن‌ها و یا تصمیم‌گیری در مورد آن‌ها، شناسایی نمایند. پس از شناسایی، تهدیدات بر حسب اهمیت رتبه‌بندی شده و مطابق با مشخصات ریسک، بررسی می‌شوند. برخی تهدیدات بایستی در طراحی داخلی مؤلفه، محصول یا راه‌حل رسیدگی شوند. با این حال برخی تهدیدات می‌توانند به وسیله پیکربندی و یکپارچه‌سازی مناسب رسیدگی شوند و یا ممکن است به مؤلفه‌ها یا فرآیندهای مدیریتی بیشتری برای کنترل ریسک‌ها نیاز باشد.

[1] Session Management
[2] Input Validation and Output Encoding
[3] Exception management

- *صحت و یکپارچگی کد*[1]: صحت کد به حفاظت از دارایی‌هایی اشاره دارد که برای ساخت و اجرای کد نرم‌افزار مورد استفاده قرار می‌گیرند و تضمین می‌کند که آن‌چه به مدیریت خدمات جهت استقرار تحویل داده می‌شود، دستکاری و یا با کد ناشناخته‌ای ترکیب نشده است. صحت کد شامل محرمانگی کد منبع در برابر رقبا و سایر افراد غیرمجاز نیز می‌باشد. صحت کد همچنین تضمین می‌کند که تمامی مجوزهای صحیح برای اجرای نمونه‌ای از کد دریافت شده و تطابق‌پذیری با هرگونه محدودیت تعیین شده از سوی تیم توسعه را نیز تضمین می‌نماید.
- *صحت و یکپارچگی رونوشت کد*[2]: صحت و یکپارچگی رونوشت کد، پشته‌های زمان اجرا[3] از پشته‌های سیستم‌عامل تا مؤلفه‌های میان‌افزار[4] و بسترهای کاربردی که جهت اجرای یک برنامه یا سرویس موردنیاز هستند را پوشش می‌دهد. رونوشت کد ممکن است شامل تعاریفی از وابستگی‌های زمان اجرا باشد که در طول فرآیند استقرار اعمال می‌شوند یا اینکه ممکن است پشته کامل نرم‌افزاری از پیش ساخته شده‌ای باشد که به عنوان یک رونوشت ماشین مجازی بسته‌بندی شده است. صحت و یکپارچگی کد تضمین می‌کند که رونوشت کد در طول و پس از تجمیع دستکاری نمی‌شود.

- **مدیریت چرخه حیات:** مدیریت مؤثر چرخه حیات به منظور اطمینان از استقرار امن نرم‌افزار، سیستم‌ها و سرویس‌ها و حذف هرگونه آسیب‌پذیری کشف شده با بیشترین سرعت ممکن ضروری می‌باشد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
  - *تخصیص انتشار*[5]: تخصیص امن تضمین می‌کند که توزیع کد[6] در مدیریت انتشار به منظور نصب و پیکربندی زیرساخت‌های نرم‌افزاری وابسته، مطابق با سیاست‌های امنیتی و در برخی موارد براساس قرارداد با مشتری انجام می‌شود. به عنوان مثال تخصیص انتشار ممکن است شامل

[1] Code Integrity
[2] Image Integrity
[3] Runtime Stack
[4] Middleware
[5] Release Provisioning
[6] Handing over Code

نگاشتی از نقش‌ها و اشخاص سازمانی به نقش‌های حقوقی تعریف شده در برنامه کاربردی جهت تضمین این که به اشخاص مجاز در سازمان دسترسی به نقش‌های درستی از برنامه کاربردی اعطا شده است، باشد.

- *تخصیص رونوشت کد*[1]: دسترسی به محتویات رونوشت کد را مدیریت می‌نماید. به عنوان مثال مدیران ممکن است مجاز به مشاهده اطلاعات یا کد محرمانه درون رونوشت کد نباشند. تخصیص رونوشت کد همچنین سطح دسترسی را برای استقرار و تعیین این‌که چه کسانی اجازه دسترسی داشته و می‌توانند نمونه‌هایی از رونوشت کد را در یک محیط تولید گسترش دهند، مدیریت می‌نماید. در نهایت این که تخصیص رونوشت کد ممکن است محدودیت‌هایی، به‌خصوص محدودیت‌های مربوط به امنیت را بر روی فرآیندهای توسعه سرویس تحمیل نماید.
- *اصلاح آسیب‌پذیری*[2]: هنگامی که یک آسیب‌پذیری در یک برنامه کاربردی شناسایی و اعتبارسنجی می‌شود، بایستی یک فرآیند پاسخ به حادثه تعریف گردد که شامل ارائه یک راه ترمیم[3] برای آسیب‌پذیری باشد. فرآیند پاسخ به حادثه بایستی اطلاع‌رسانی به سایر تیم‌های برنامه کاربردی که ممکن است تحت تأثیر آسیب پذیری قرار گیرند را نیز دربرگیرد.

- **آزمون امنیت:** روش‌های مختلفی برای تحلیل برنامه‌های کاربردی جهت مشخص نمودن و یافتن آسیب‌پذیری‌هایی که می‌توانند مورد سوءاستفاده قرار گیرند، وجود دارد. تمامی این روش‌ها بایستی در هنگام توسعه برنامه‌های کاربردی مورد استفاده قرار گیرند. در هنگام استفاده از برنامه‌های شخص ثالث و در زمانی که دسترسی به کد منبع وجود ندارد، تحلیل‌های پویا و بی‌درنگ بایستی استفاده گردند. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
- *تجزیه و تحلیل ایستای کد*[4]: شامل ابزارها و فرآیندهای ایجاد شده‌ای است که توسط تیم توسعه نرم‌افزار و یا تیم ساخت به منظور بررسی تمامی مصنوعات و مؤلفه‌ها برای ساخت یک برنامه

[1] Image Provisioning
[2] Vulnerability Remediation
[3] Fix
[4] Static Code Analysis

کاربردی استفاده می‌شوند. این تجزیه و تحلیل‌ها به‌دنبال شناسایی آسیب‌پذیری‌های امنیتی و روش‌های برنامه‌نویسی ضعیفی هستند که می‌توانند مشکلاتی در زمینه‌های امنیت، کارایی یا سایر زمینه‌ها ایجاد نمایند. تجزیه و تحلیل ایستای کد معمولاً به ابزارهای خودکاری اشاره دارد که کد منبع را پویش می‌کنند و مشکلات بالقوه را گزارش می‌دهند.

- *تجزیه و تحلیل پویا*[1]: شامل ابزارهایی است که تحلیل نرم‌افزار را مانند جعبه سیاه[2] بدون اطلاع از کد منبع و عملیات داخلی آن انجام می‌دهند. ابزارهای تحلیل پویا به صورت خودکار نرم‌افزار، نقاط ورودی و خروجی آن را بررسی و همچنین تلاش صورت گرفته برای تزریق ورودی که منجر به نقض[3] نرم‌افزار شده یا باعث خطایی در منطق آن می‌گردد را تحلیل می‌نماید. تحلیل پویا می‌تواند برای ارائه دقت و پوشش بهتر با استفاده از یک روش تحلیل ترکیبی توسعه یابد. اگرچه یک پویش تحلیل پویا بیشتر متکی به پاسخ سرویس‌دهنده برای مشخص نمودن وجود آسیب‌پذیری می‌باشد، اما یک تحلیل ترکیبی می‌تواند عملیات داخلی و ساختار برنامه‌های وب را نیز پویش نماید. در نتیجه این نوع تحلیل کامل بوده و می‌تواند آسیب‌پذیری‌های پیچیده‌تر را شناسایی و مکان دقیق آسیب‌پذیری‌ها را در کد منبع گزارش دهد.
- *تجزیه و تحلیل در زمان اجرا*: تجزیه و تحلیل در زمان اجرا یا توصیف مشخصات نرم‌افزار[4]، اشاره به قابلیتی برای مشاهده یک سیستم نرم‌افزاری در حال اجرا و تحلیل آن جهت تشخیص آسیب‌پذیری‌های کد دارد. این رویکرد نظارت مستمری را برروی نرم‌افزار ارائه می‌نماید در حالی که تحلیل ایستا و پویای کد، وضعیت نرم‌افزار را در لحظه‌ای از زمان ارائه می‌نماید. اگرچه تجزیه و تحلیل در زمان اجرا، اغلب برای بررسی مشکلات استفاده از حافظه، استفاده از شبکه یا سایر منابع در زمان اجرا به کار می‌رود، می‌تواند برای شناسایی مشکلات امنیتی بالقوه نیز استفاده گردد. تجزیه و تحلیل زمان اجرا یک دید داخلی از برنامه در حال اجرا را فراهم می‌نماید، در

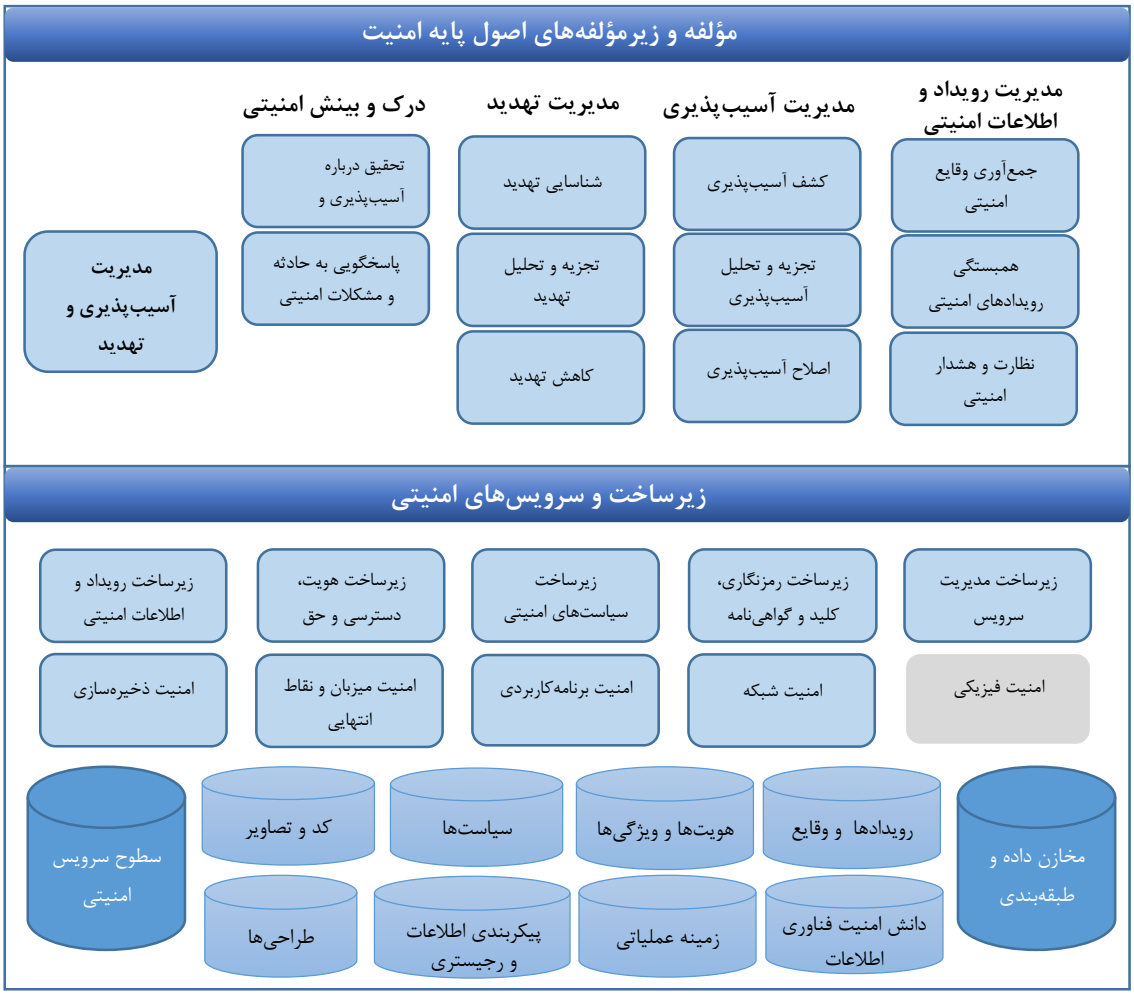
[1] Dynamic Analysis
[2] Black Box
[3] Breaks
[4] Software Profiling

حالی که تحلیل پویا، یک برنامه در حال اجرا را از طریق تعامل با آن از یک دید خارجی به همان شیوه‌ای که یک کاربر یا مشتری نرم‌افزار با آن تعامل دارد، بررسی می‌نماید.

۲-۶-۳-۴- مدیریت تهدید و آسیب‌پذیری

مدیریت تهدید و آسیب‌پذیری سرویس‌هایی را فراهم می‌کند که می‌توانند در مواردی مانند تعیین تهدیدات امنیتی و شناسایی آسیب‌پذیری‌ها در سیستم‌های توسعه یافته، جمع‌آوری اطلاعات مربوط به امنیت از منابع مختلف داخلی و خارجی و تعیین پاسخ مناسب کمک کنند.

شکل (۲- ۱۱) دید کلی از زیرمؤلفه‌های مدیریت آسیب‌پذیری و تهدید و نیز مؤلفه‌های مرتبط از مجموعه زیرساخت و سرویس‌های امنیتی را نشان می‌دهد.



شکل (۲- ۱۱): زیرمؤلفه‌های مدیریت آسیب پذیری و تهدید به همراه مؤلفه‌های زیرساخت و سرویس‌های امنیتی مربوطه

مدیریت آسیب‌پذیری و تهدید به چهار گروه زیر تقسیم می‌شود:

- **درک و بینش امنیتی**[1]: اطلاعات امنیتی درباره تهدیدات و آسیب‌پذیری‌ها فراهم می‌کند. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:
  - *تحقیقات درمورد آسیب‌پذیری و تهدید امنیتی*[2]: نشان‌دهنده قابلیتی برای جمع‌آوری، تحلیل و انتشار اطلاعات مرتبط با امنیت رایانه از طریق بررسی و ردیابی طیف وسیعی از منابع اطلاعاتی در دسترس در مورد تهدیدات و آسیب‌پذیری‌های بالقوه به منظور تعیین قابلیت اجرا در محیط‌های فناوری‌اطلاعات سازمانی می‌باشد. در یک اجرای بسیار پیچیده، تحقیقات آسیب‌پذیری و تهدید امنیتی شامل مشاهده، دستکاری و تجزیه و تحلیل دقیقی از رفتار عوامل تهدید و ترکیب شرایط آسیب‌پذیری با سناریوهای حمله به منظور ایجاد و ارائه اطلاعاتی درباره حملات بالقوه‌ای که در آینده رخ می‌دهند، با استفاده از اطلاعاتی که جمع‌آوری می‌شود، می‌باشد. افراد و فرآیندهایی که با این مؤلفه مرتبط هستند، مسئول جمع‌آوری اطلاعاتی از تهدیدات و آسیب‌پذیری‌ها جهت کمک به سازمان‌های مجری قانون، سازمان‌های نظارتی و گروه‌های تجاری صنعتی می‌باشند.
  - *پاسخگویی به حادثه و مشکلات امنیتی*[3]: پاسخگویی به حادثه و مشکلات امنیتی، مدیریت مشکلات و مدیریت حوادث مرتبط با سرویس‌های امنیتی را پشتیبانی می‌کند. این مؤلفه این امر را به وسیله ارائه دانش تخصصی امنیت درباره حملات شناسایی شده و ناهنجاری‌های مربوط به امنیت و همچنین توصیه‌هایی برای مدیریت حوادث و مشکلات امنیتی فراهم می‌نماید و شامل مهار نمودن حادثه امنیتی، بازیابی حادثه، تحلیل مشکلات امنیتی و حل مشکلات می‌باشد.
- **مدیریت تهدید:** سرویس‌های مدیریت تهدید با شناسایی و درک تهدیدات خاصی که ممکن است برای یک محیط فناوری اطلاعات وجود داشته باشد، سر و کار دارند. یک تهدید به معنای تصمیم یک

[1] Security Intelligence
[2] Security Threat and Vulnerability Research
[3] Security Incident and Problem Response

عامل تهدید برای انجام یک عمل تهدیدآمیز به منظور سوءاستفاده از یک آسیب‌پذیری خاص می‌باشد. همچنین صرفا وقوع تهدید و آسیب‌پذیری با هم، احتمال وقوع یک ریسک را مشخص می‌نمایند. در صورتی که تهدید یا آسیب‌پذیری وجود نداشته باشد، احتمال ریسک صفر می‌باشد (هیچ ریسکی وجود ندارد). این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:

- *شناسایی تهدید:* شناسایی تهدید، شامل فعالیت‌هایی جهت کمک به کشف بازیگران و اقداماتی است که در محیط فناوری اطلاعات ممکن است برروی دارایی‌ها و اطلاعاتی که بر روی آن‌ها ذخیره و پردازش شده‌اند، اثرات سوء داشته باشند. شناسایی تهدید می‌تواند صرفاً به صورت دستی انجام شود، اما امروزه معمولاً بر اساس تشخیص خودکار و همچنین براساس میزان انحراف از عملیات معمول در یک محیط فناوری اطلاعات انجام می‌گیرد. هرگونه ناهنجاری‌های کشف شده می‌تواند برای تهدیدات بالقوه مورد بررسی قرار گیرد.
- *تجزیه و تحلیل تهدید:* تجزیه و تحلیل تهدید، در واقع آزمون مداوم اطلاعات در دسترس است که با عوامل تهدید (که اغلب با عنوان مهاجم نامگذاری می‌شوند) و اقدامات تهدیدآمیز احتمالی آن‌ها به منظور ارزیابی شدت تهدید شناسایی شده مرتبط می‌باشد.
- *کاهش تهدید*[1]: شامل تلاش‌هایی جهت تأثیر بر روی عوامل تهدید و یا برای دستکاری اقدامات تهدید به منظور کاهش شدت یک تهدید انجام می‌شود. کاهش تهدید شامل کنترل‌هایی مانند استقرار سیستم‌های تشخیص بدافزارها، تشخیص نفوذ و تله عسل[2] می‌باشد.

- **مدیریت آسیب‌پذیری:** سرویس‌های مدیریت آسیب‌پذیری با کشف، درک و کاهش آسیب‌پذیری‌های خاصی که ممکن است برای یک محیط فناوری اطلاعات وجود داشته باشد، سروکار دارند. آسیب‌پذیری ضعفی است که می‌تواند برای به خطر افتادن امنیت مورد سوءاستفاده قرار بگیرد. این مؤلفه شامل زیرمؤلفه‌های زیر می‌باشد:

[1] Threat Mitigation
[2] Honeypot

- *کشف آسیب‌پذیری:* شناسایی آسیب‌پذیری‌ها با تشخیص آسیب‌پذیری‌ها سروکار دارد. روش‌های شناخته شده‌ای برای کشف آسیب‌پذیری‌ها وجود دارد که شامل موارد ذیل می‌باشند:

➢ تحلیل پویای کد: تحلیل پویای کد، جهت ارزیابی برنامه‌های کاربردی از نظر آسیب‌پذیری که ممکن است از سمت کاربر مورد سوءاستفاده قرار بگیرد، به‌کار می‌رود.

➢ پویش آسیب‌پذیری شبکه: پویش آسیب‌پذیری شبکه به منظور بررسی مواردی همچون سیستم‌عامل‌ها، پایگاه‌های داده، میان‌افزارها و دیواره‌های آتش[1] صورت می‌گیرد که از تمامی سرویس‌های فناوری اطلاعات مستقر در برابر آسیب‌پذیری‌هایی که از طریق اینترنت قابل دسترسی هستند، محافظت می‌نماید. تفاوت بین تحلیل پویای کد و پویش آسیب‌پذیری شبکه در این است که پویش آسیب‌پذیری شبکه بیشتر بر روی بسته‌های نرم‌افزاری عمومی[2] تمرکز می‌کند در حالی که تمرکز تحلیل پویای کد بیشتر بر روی برنامه‌های کاربردی سفارشی ساخته شده[3] می‌باشد.

➢ بررسی سلامت امنیت[4]: بررسی سلامت امنیت، سیستم‌ها را به وسیله اسکریپت‌ها یا از طریق یک عامل محلی داخلی بررسی نموده و پیکربندی سرویس‌های محلی و شبکه‌ای سیستم‌عامل‌ها، پایگاه های‌داده و برنامه‌های کاربردی را جهت شناسایی خطاهایی که می‌تواند منجر به سوءاستفاده از آسیب‌پذیری‌های بالقوه گردد، ارزیابی می‌کند.

➢ هک اخلاقی[5]: شامل استفاده از ابزارها و تکنیک‌هایی است که توسط آن‌ها نقاط آسیب‌پذیر شبکه یا نرم‌افزار یا سیستم اطلاعاتی کشف می‌گردد. در واقع هک اخلاقی به سازمان‌ها کمک می‌کند که بتوانند بهتر از همیشه سیستم‌های امنیتی را درک کنند و ریسک‌هایی که وجود دارد را شناسایی و فرآیندهای مقابله با ریسک‌ها را انجام دهند. این کار در نهایت باعث

---

[1] Firewall
[2] off-the-shelf Software Packages
[3] Custom-Built
[4] Security Healthchecking
[5] Ethical Hacking

کاهش هزینه‌های سازمان می‌شود زیرا از بروز ریسک‌هایی که ممکن است بعدها هزینه‌های سنگینی برای سازمان داشته باشند جلوگیری می‌نماید.

- *تجزیه و تحلیل آسیب پذیری:* تجزیه و تحلیل آسیب‌پذیری، بررسی و بازبینی آسیب‌پذیری‌ها را به‌وسیله از بین بردن خطای مثبت کاذب پوشش می‌دهد و همچنین گروه‌بندی آسیب‌پذیری‌ها را در شرایط بحرانی (به‌عنوان مثال بر اساس سهولت کشف و پیچیدگی سوءاستفاده از آن‌ها برای حمله‌کنندگان) پوشش می‌دهد.
- *اصلاح آسیب‌پذیری:* اصلاح آسیب‌پذیری شامل ترکیبی از کنترل‌های امنیتی اصلاحی، بازدارنده و پیشگیرانه به منظور کاهش آسیب‌پذیری‌های شناسایی و تایید شده می‌باشد. متداول‌ترین روش‌های کاهش برای از بین بردن یک آسیب‌پذیری شامل اقدامات زیر می‌باشد:
  - رفع نواقص کد مربوطه از طریق وصله‌ها[1]
  - تغییر پیکربندی سرویس آسیب‌پذیر
  - استفاده از بیشترین کنترل‌های امنیتی پیشگیرانه مانند دیواره آتش و سیستم‌های تشخیص نفوذ با قابلیت‌های وصله مجازی
  - به‌کارگیری اقدامات اصلاحی بیشتر مانند افزایش تعداد دفعات بررسی سیستم، پشتیبان‌گیری از داده‌ها برای بازیابی سریع‌تر و بهبود روش پاسخ اضطراری.
- **مدیریت رویداد و اطلاعات امنیتی:** مدیریت رویداد و اطلاعات امنیتی شامل جمع‌آوری وقایع امنیتی، همبستگی رویدادهای امنیتی و نظارت‌بر امنیت و هشدار می‌باشد.
- *جمع‌آوری وقایع امنیتی:* به قابلیتی برای جمع‌آوری رویدادهای مربوط به امنیت از مجموعه نقاط مختلف در محیط فناوری اطلاعات (معمولاً از سیستم‌ها، شبکه‌ها، وقایع امنیتی و داده‌های هشدار) و ذخیره آن‌ها به روشی ساخت‌یافته به منظور داشتن یک نسخه اضافه جهت بازیابی و

[1] Patching

تحلیل آن‌ها در طول وقوع حوادث و مشکلات امنیتی در مورد فایل‌های ثبت وقایعی که در معرض خطر هستند، اشاره می‌نماید.

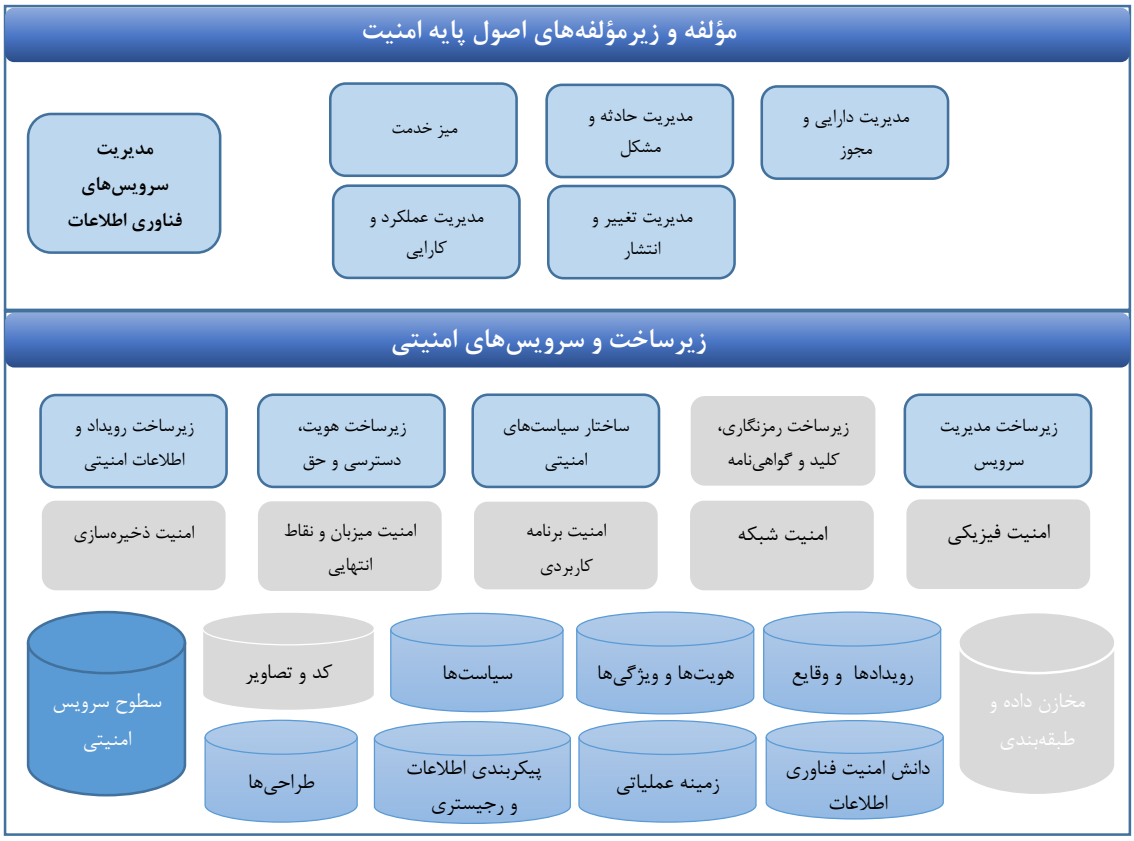
- *همبستگی رویدادهای امنیتی*[1]: همبستگی رویدادهای امنیتی بر اساس جمع‌آوری وقایع امنیت ایجاد می‌شود. پس از این که داده‌های وقایع به صورت متمرکز جمع‌آوری شد، داده‌ها می‌توانند به‌منظور استخراج اطلاعات امنیتی قابل درکی ادغام، استاندارد، ساخت‌یافته، همبسته و نرمال گردند.
- *نظارت بر امنیت و هشدار*[2]: نظارت‌بر امنیت و هشدار به تمامی فعالیت‌های مربوط به ملاحظات مکرر و مداوم بر روی زیرساخت فنی به منظور تعیین میزان انحراف از عملیات استاندارد اشاره دارد که نشان‌دهنده تأثیر آن‌ها بر امنیت می‌باشد.

۲-۶-۳-۵- مدیریت سرویس‌های فناوری اطلاعات

مدیریت سرویس‌های فناوری اطلاعات، خودکارسازی فرآیند و روند جریان‌کاری[3] را برای تمام فعالیت‌های تحویلی فناوری اطلاعات، از جمله مدیریت امنیت فراهم می‌کند. به طور خاص، فرایندهای مدیریت تغییر و مدیریت حادثه نقش مهمی را در مدیریت امنیت ایفا می‌کنند. این بخش یک توصیف کاملی از تمام حوزه‌های مدیریت سرویس فناوری اطلاعات ارائه نمی‌کند. تمرکز این بخش بر روی مؤلفه‌های کلیدی مدیریت خدمات فناوری اطلاعات است که به امنیت کمک می‌کند.

شکل (۲- ۱۲) دید کلی از زیرمؤلفه‌های مدیریت سرویس فناوری اطلاعات و نیز مؤلفه‌های مرتبط از مجموعه زیرساخت و سرویس‌های امنیتی را نشان می‌دهد.

[1] Security Event Correlation
[2] Security Monitoring and Alerting
[3] Workflow



شکل (۲- ۱۲): زیرمؤلفه‌های مدیریت سرویس فناوری اطلاعات به همراه مؤلفه‌های زیرساخت و سرویس‌های امنیتی مربوطه

مدیریت سرویس فناوری اطلاعات شامل زیرمؤلفه‌های زیر می‌باشد:

- **میز خدمت**[1]: میز خدمت به عنوان یک مرکز ارتباطات در سازمان است که تک نقطه تماس[2] میان سازمان و مشتریان داخلی و خارجی به شمار می‌رود. هدف این مرکز ارائه خدمات به‌هنگام و کارآمد به مشتریان سازمان در هر لحظه و زمان و همسو با توافق‌نامه‌ها و تفاهم‌نامه‌های میان آن‌ها و سازمان می‌باشد.
- **مدیریت مشکلات و حوادث:** مدیریت مشکلات و حوادث روش‌ها و فرآیندهایی را مدیریت می‌کند که جهت بازیابی خدمات از هر نوع اختلالی که به دلیل حوادث و مشکلات ایجاد شده، مورد نیاز

[1] Service Desk
[2] Single point of contact

می‌باشند. یک حادثه، یک رویداد واحد یا گروهی از رویدادها در نظر گرفته می‌شود که به صورت موازی یا در یک دوره زمانی کوتاه رخ می‌دهند و تأثیر منفی بر سطح خدمات دارند. یک مشکل به عنوان نتیجه‌ای از حوادث تکراری مشابه یا با الگوی مشابه و یا به‌عنوان نتیجه تشدید یک حادثه درنظر گرفته می‌شود که تأثیر چشمگیری برروی سطح خدمت داشته و نیاز به تلاش زیادی جهت بازگشت به عملیات عادی دارد.

- **مدیریت مجوز و دارایی‌های فناوری اطلاعات:** مدیریت مجوز و دارایی، مجموعه‌ای از قابلیت‌ها را به‌منظور نظارت بر دارایی‌های فناوری اطلاعات مستقر از دید مالی، فهرست اموال و غیره پوشش می‌دهد. از دیدگاه نرم‌افزار، مدیریت مجوز و دارایی شامل مدیریت مجوزها، جنبه‌های خاصی از مدیریت پیکربندی (برای لیستی از اهداف مدیریتی) و گزارشی برای اهداف نظارتی می‌باشد. مدیریت مجوز شامل حفظ لیستی از نرم‌افزارهای مستقر شده و مدیریت مجوزها برای نرم‌افزارهای مجاز می‌باشد.

مدیریت دارایی سخت‌افزاری شامل ویژگی‌های فیزیکی مؤلفه‌های سخت‌افزاری استقرار یافته در محیط فناوری اطلاعات از قبیل شماره مدل آن‌ها، شماره سریال، مکان‌های فیزیکی و نقش آن‌ها در شبکه می‌باشد. مدیریت دارایی‌های سخت‌افزاری شامل ردیابی منظمی از دارایی‌های سخت‌افزاری، ردیابی تاریخچه‌ای از شکست‌های فیزیکی و غیره می‌باشد و اغلب درگیر ضبط و ردیابی دیدگاه مالی از دارایی می‌باشد.

- **مدیریت ظرفیت و عملکرد:** مدیریت ظرفیت و عملکرد با برنامه‌ریزی، تخصیص و بهینه‌سازی منابع فناوری اطلاعاتی که مورد نیاز سرویس‌های فناوری اطلاعات می‌باشند، سروکار دارد. در حالت کلی، این مؤلفه بیشتر به جزئیاتی مانند قدرت پردازش و حافظه، سیستم پشتیبان‌گیری و بایگانی داده و سرعت شبکه یا پهنای باند اشاره دارد. در یک زمینه گسترده‌تر، مدیریت ظرفیت و عملکرد می‌تواند شامل منابع انسانی و منابع دارایی فیزیکی باشد. این حوزه برای امنیت مهم می‌باشد، به‌دلیل اینکه

سرویس‌های امنیتی و اجزای زیرساخت مربوطه آن‌ها در یک محیط فناوری اطلاعات می‌توانند مقدار قابل توجهی از منابع را استفاده نمایند و در نتیجه این می‌تواند بر روی عملکرد تأثیرگذار باشد.

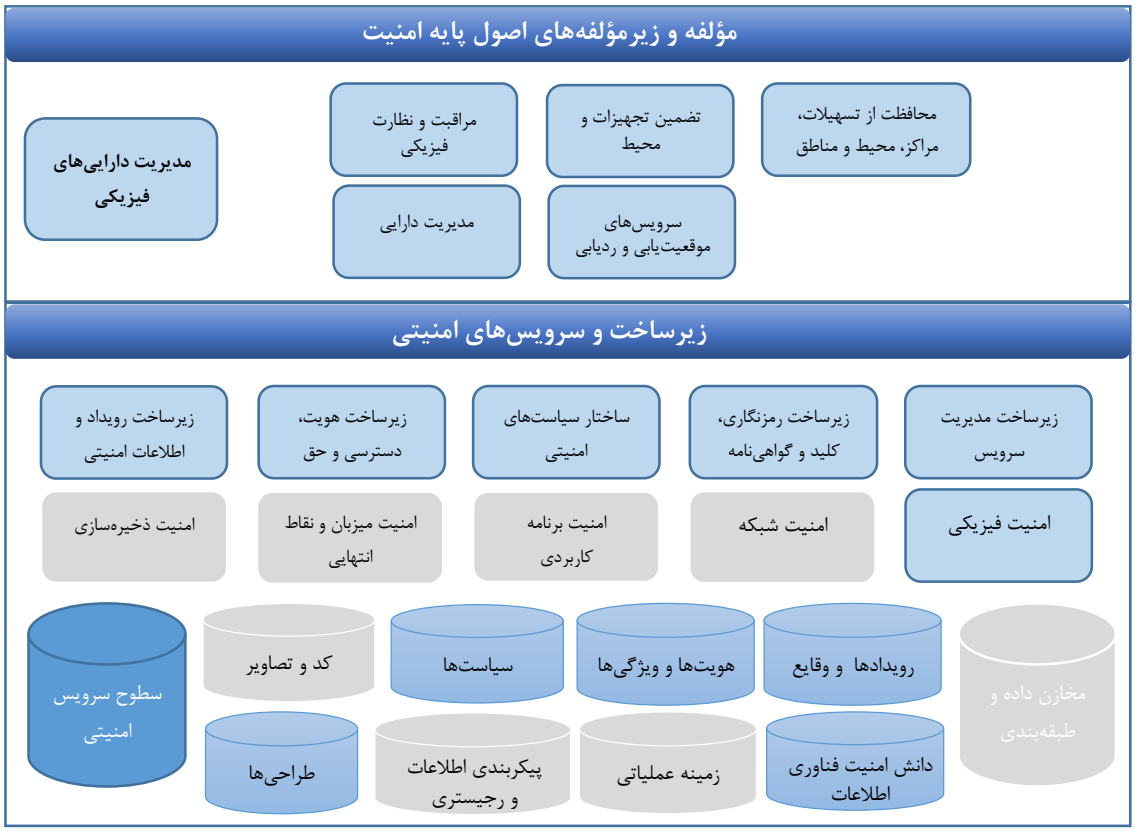
- **مدیریت تغییر و انتشار:** مدیریت تغییر و انتشار، استانداری از روش‌ها و فرآیندهای کاری را برای مدیریت نمودن پیکربندی دارایی‌های فناوری اطلاعات استقرار یافته و ارتقاء مؤلفه‌های نرم‌افزاری توسعه‌یافته موجود و استقرار مؤلفه‌های نرم‌افزاری جدید، پوشش می‌دهد. هدف این استانداردسازی به حداقل رساندن اختلال در سرویس‌ها می‌باشد و همچنین برای اینکه اطمینان حاصل شود که مؤلفه‌های سخت‌افزاری و نرم‌افزاری در روش‌هایی که جنبه‌های امنیت یا صحت را به خطر می‌اندازند، استقرار نیافته‌اند.

۲-۶-۳-۶- مدیریت دارایی‌های فیزیکی

مدیریت دارایی‌های فیزیکی اطلاعاتی از موقعیت و وضعیت دارایی‌های فیزیکی و نیز اطلاعاتی درباره کنترل‌های امنیت فیزیکی ارائه می‌کند و برای سیستم‌های فیزیکی، اطلاعات امنیتی را با استفاده از کنترل‌های امنیت فناوری اطلاعات هماهنگ می‌کند. این بخش تمام حوزه‌های مدیریت دارایی فیزیکی را دربرنمی‌گیرد و صرفاً برروی مؤلفه‌های کلیدی مدیریت دارایی فیزیکی که به تأمین امنیت کمک می‌کنند، تمرکز می‌کند.

شکل (۲- ۱۳) دیدکلی از زیرمؤلفه‌های مدیریت دارایی‌های فیزیکی و نیز مؤلفه‌های مرتبط از مجموعه زیرساخت و سرویس‌های امنیتی را نشان می‌دهد.

از آنجا که همگرایی امنیت فناوری اطلاعات و امنیت فیزیکی در حال پیشرفت است، مدیریت دارایی‌های فیزیکی به یک نگرانی مهم و عمده تبدیل شده است. مدیریت دارایی فیزیکی شامل زیرمؤلفه‌های مراقبت و نظارت فیزیکی، تضمین تجهیزات و محیط، محافظت از تسهیلات، مراکز، محیط و مناطق، مدیریت دارایی و سرویس‌های موقعیت‌یابی و ردیابی می‌باشد.



شکل (۲- ۱۳): زیرمؤلفه‌های مدیریت دارایی فیزیکی به همراه مؤلفه‌های زیرساخت و سرویس‌های امنیتی مربوطه

- **مراقبت و نظارت فیزیکی**[1]: مراقبت و نظارت فیزیکی تمامی تحقیقات درباره کنترل‌های امنیتی فیزیکی را پوشش می‌دهد و معادل نظارت فنی فناوری اطلاعات (از جمله مشاهده بی‌درنگ دارایی‌های فیزیکی به منظور تشخیص حملات فیزیکی، سرقت، سوءاستفاده و سایر وقایع غیرعادی و مشکوک) می‌باشد. مراقبت و نظارت فیزیکی می‌تواند با استفاده از نظارت مستقیم یا غیرمستقیم انسان یا سیستم‌های خودکار صورت گیرد. مراقبت و نظارت فیزیکی می‌تواند شواهد را در طول دوره‌ای طولانی مدت به منظور بررسی موقعیت‌های مربوط به امنیت در گذشته ثبت نماید.
- **تضمین تجهیزات و محیط:** تضمین تجهیزات و محیط، تأمین برق و سایر کنترل‌های اقلیمی و تدارکات مربوط به صنایع همگانی مانند سیستم‌های نظارتی گاز و آب را پوشش می‌دهد. تضمین

[1] Surveillance and Physical Monitoring

تجهیزات و محیط بخشی از مدیریت امکانات می‌باشد که می‌تواند تأثیر قابل توجهی را برروی دسترس‌پذیری سرویس‌های فناوری اطلاعات و امنیت داشته باشد.

- **حفاظت از تسهیلات (مراکز)، محیط پیرامون و حوزه:** این زیرمؤلفه تخصیص و مدیریت کنترل‌های امنیت فیزیکی دستی یا خودکار را به‌صورت بازدارنده، پیشگیرانه و یا واکنشی پوشش می‌دهد. این سرویس شامل فعالیت‌های برنامه‌ریزی برای محیط به‌منظور رسیدگی به خطرات شناخته شده از بلایای طبیعی، رویدادهای سیاسی و سایر تهدیدات خارجی می‌باشد. سیستم‌های اطفاءحریق و نظارتی[1] شامل این سرویس می‌باشند.
- **سرویس تعیین موقعیت و ردیابی:** سرویس‌های تعیین موقعیت و ردیابی مربوط به شناسایی موقعیت و تغییر مکان دارایی‌های فیزیکی ملموس می‌باشد که این دارایی‌های حاوی اطلاعات با ارزش بایستی محافظت گردند. این مؤلفه می‌تواند شامل ردیابی برد کوتاه و بلند تا یک مقیاس جهانی باشد.
- **مدیریت دارایی[2]:** مدیریت دارایی فعالیت‌های مربوط به تأمین، ساخت و تهیه، نگهداری و به‌روزرسانی، انهدام و تخریب دارایی‌های فیزیکی ملموس و همچنین دارایی‌های غیرملموس را پوشش می‌دهد. این دارایی‌ها فراتر از دارایی‌های محض فناوری اطلاعات می‌باشند اما اغلب تمرکز اصلی برروی دارایی‌هایی است که تأثیر مستقیم یا مهمی برروی امنیت اطلاعات دارند.

در بخش‌های قبلی چارچوب معماری مرجع امنیت و زیر حوزه‌های امنیتی به طور کامل و جامع بیان گردیدند. در ادامه نگاه کلی و اجمالی بر این فرایند، که در شکل (۲-۱۴) نیز آمده است، خواهیم داشت.

همان‌طور که در شکل مشاهده می‌شود، در تعریف و اعتبارسنجی نیازمندی‌ها، بایستی نیازمندی‌ها و الزامات کسب‌وکار، ریسک کسب‌وکار، ذینفعان، ساختار سازمانی، جوامع درگیر، هزینه‌ها و غیره شناسایی و مورد بررسی و تحلیل قرار گیرد. در واقع با تحلیل و بررسی الزامات و نیازها می‌توان استراتژی و سطح اهداف امنیتی و همچنین سیاست‌ها و قوانین امنیتی موردنیاز را مشخص نمود. الزامات و نیازها به عنوان ورودی برای

[1] suppression and monitoring systems
[2] Asset Administration

سیاست‌ها و قوانین امنیتی در نظر گرفته می‌شوند که با استفاده از آن‌ها می‌توان استراتژی کلی امنیت و سطح اهداف امنیتی که می‌بایست به آن دست یافت را مشخص نمود.

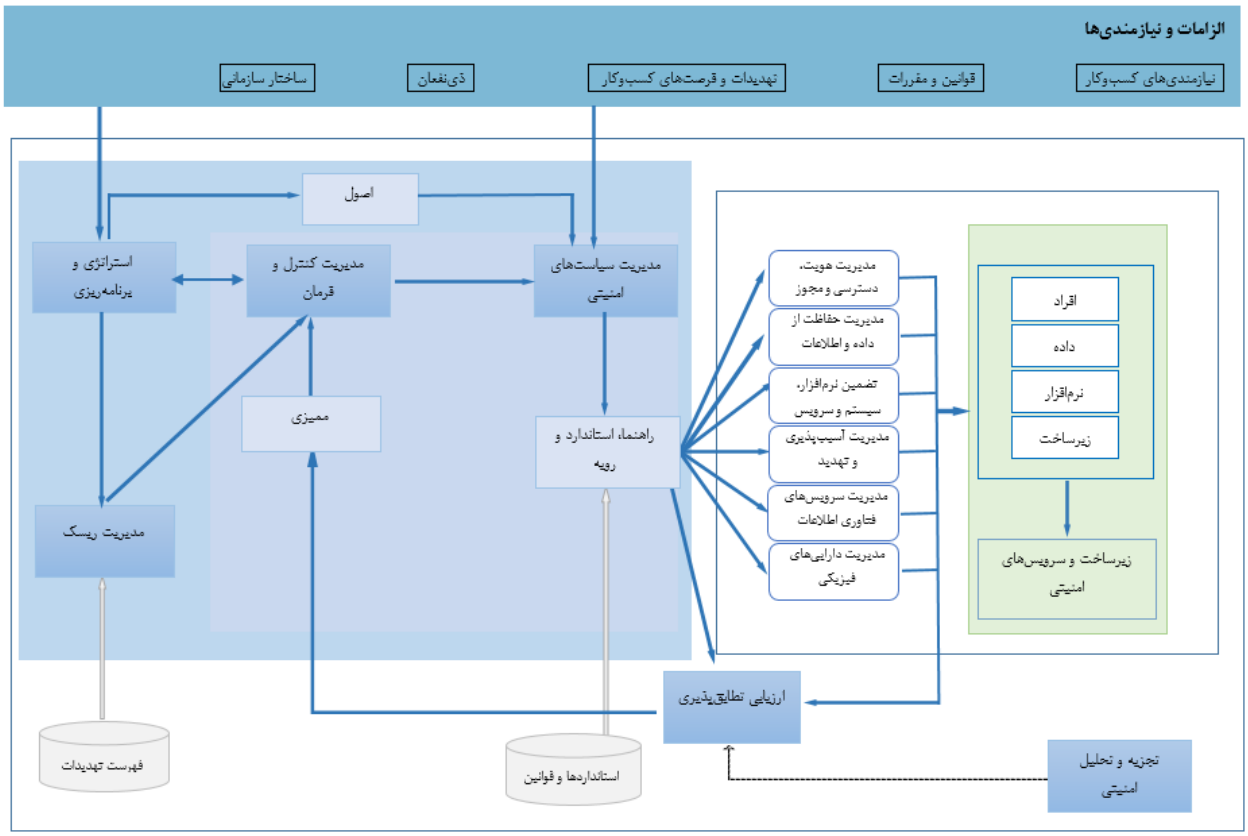
پس از تعیین و تحلیل الزامات و مشخص شدن هدف کلی امنیتی، بایستی اصول، سیاست‌ها و قوانین امنیتی مشخص گردد. هر سازمانی سیاست‌ها و قوانین امنیتی خاص خود را دارد که بایستی در راستای آن‌ها اقدامات امنیتی را انجام دهد در واقع به منظور کاهش ریسک‌های امنیتی، سازمان بایستی از سیاست‌ها و قوانین امنیتی خاص در حوزه‌های مختلف استفاده نماید. (به عنوان مثال سیاست کنترل دسترسی، امنیت محیطی و فیزیکی، کنترل و طبقه‌بندی دارایی و ...). لازم به ذکر است که هر سازمان در هنگام تدوین اصول، سیاست‌ها و قوانین امنیتی باید سیاست‌ها و قوانین کلی کشور را مدنظر قرار دهد.

مولفه مدیریت سیاست امنیتی، رویه، راهنما و استانداردهایی را با استفاده از خروجی مراحل قبلی در حوزه‌های اصلی تحت عنوان اصول امنیتی پایه که در واقع همان قابلیت‌های امنیتی اصلی در این سند می‌باشند، را مشخص می‌کند که این اصول امنیتی در حوزه‌های مختلف مدل، به منظور برقراری امنیت در آن‌ها بایستی به کار گرفته شوند. این مولفه همچنین برنگاشت و ترجمه صحیح سیاست‌ها به استانداردها و راهنماها نظارت می‌کند.

علاوه بر شناسایی ریسک کسب و کار در مرحله الزامات، مدیریت ریسک عملیاتی نیز بایستی در کل چرخه حیات توسعه سیستم در نظر گرفته شود. در واقع مدیریت ریسک‌های امنیتی، اجرای منظمی از سیاست‌های امنیتی، فرآیندها و روش‌هایی است که به مدیر سازمان در شناسایی ریسک‌های امنیتی، تحلیل، ارزیابی و طبقه‌بندی آن‌ها کمک می‌کند و این فرآیند بایستی به طور مداوم در تمامی حوزه‌های مختلف مدل انجام شود.

به منظور ارزیابی و نظارت بر کنترل‌های امنیتی، نیز بایستی یک مرکز کنترل جهت مدیریت ثبت وقایع، مدل‌سازی ریسک، اولویت‌بندی آسیب‌پذیری، تشخیص حادثه و تجزیه و تحلیل تأثیر وظایف وجود داشته

باشد که در مدل با نام مرکز تجزیه و تحلیل امنیتی ارایه شده است و از اطلاعات فراهم شده توسط این مرکز جهت ارزیابی تطابق‌پذیری و مدیریت ریسک استفاده می‌شود.



شکل (۲- ۱۴): ارتباط سایر مدل‌های مرجع با مدل مرجع امنیت

۲-۷- ارتباط مدل مرجع امنیت با سایرمدل‌های مرجع

مدل مرجع امنیت ارتباط بسیار نزدیکی با پنج مدل مرجع دیگر از چارچوب مدل مرجع تلفیقی دارد به گونه‌ای که کنترل‌های امنیتی و حریم خصوصی باید در کسب و کار، جریان‌های داده، سیستم‌های اطلاعاتی، برنامه‌های کاربردی و زیرساخت پوشش داده شود.

ارتباط امنیت و حریم خصوصی با معماری فراسازمانی، از جمله اهداف عملکرد سازمان، فرایندهای کسب‌وکار، جریان‌های داده، برنامه‌کاربردی و فناوری زیرساخت، تضمین می‌کند که هر کدام از جنبه‌های کسب‌وکار ملاحظات امنیتی و حریم خصوصی مناسبی را دریافت می‌کنند. به‌علاوه، پوشش دادن امنیت و حریم خصوصی از طریق معماری فراسازمانی قابلیت همکاری را ترویج می‌دهد و به استانداردسازی و تثبیت قابلیت‌های امنیتی و حریم خصوصی کمک می‌کند.

مدل مرجع عملکرد، دربردارنده طبقه‌بندی کاملی از سنجه‌های عملکرد در دستگاه‌ها است که تصویری منسجم و جامع را از مولفه‌های کسب‌وکار و ارتباط آن‌ها با اهداف و نتایج راهبردی ارایه می‌دهد. استفاده از این مدل مرجع باعث ایجاد یک چارچوب مشترک برای انتخاب، اندازگیری و پایش شاخص‌های عملکرد می‌شود و به دولت امکان می‌دهد که در دوره‌های زمانی مختلف، ارزیابی عملکرد دستگاه‌های اجرایی را براساس این سنجه‌ها جمع‌آوری نموده و ارزیابی نماید. از این رو این مدل معیارهای هدف برای اندازه‌گیری کارایی و اثربخشی امنیت و حریم خصوصی را فراهم می‌کند. در مقابل، مدل مرجع امنیت، محدودیت‌های امنیتی و حریم خصوصی را برای کنترل و اندازه‌گیری عملکرد ارایه می‌کند.

مدل مرجع خدمات دربردارنده ساختار، طبقه‌بندی و الگوهای کارکردهای (خدمات) دولت، مستقل از دستگاه ارایه‌دهنده آن است. این مدل تصویر کلان معماری کارکردهای (خدمات) دولت را ترسیم می‌کند تا در مرحله بعد هر دستگاه اجرایی جزییات و نحوه پیاده‌سازی این نقشه کلان را در قالب جزییات معماری سازمانی خود، تدوین و پیاده‌سازی نماید. این مدل همچنین مشتریان و کانال‌های مختلفی که آن‌ها برای تعامل با دولت استفاده می‌کنند، سرویس‌ها و خدمات مشترک ارایه شده به شهروندان و... را توصیف می‌کند. این مدل با

دسته‌بندی کارکردها و خدمات دولت، ورودی‌هایی برای فرایند دسته‌بندی امنیتی اطلاعات و سیستم‌های اطلاعاتی فراهم می‌کند؛ عناصر کسب و کار که نیاز به حفاظت امنیتی و حریم خصوصی دارند و همچنین الزامات کسب و کار برای مدیریت هویت و دسترسی را مشخص می‌کند. در مقابل، مدل مرجع امنیت استانداردها و اطلاعاتی را برای حفظ امنیت و حریم خصوصی ارایه می‌کند که جهت امن کردن کانال‌ها، خدمات و فرآیندهای کسب‌وکار استفاده می‌گردد و با تعیین ریسک‌های کسب‌وکار، تدوین استراتژی و قوانین امنیتی تضمین می‌کند که مدل مرجع خدمات بر روی مسایل امنیتی نیز تمرکز دارد.

مدل مرجع داده، یک پشتیبان پایه برای کل مدل مرجع است و بر دو سوال اصلی تمرکز دارد:

- چه اطلاعاتی برای به اشتراک‌گذاری و استفاده مجدد در دسترس می‌باشد.
- چه شکاف‌های اطلاعاتی نیاز به اصلاح دارند.

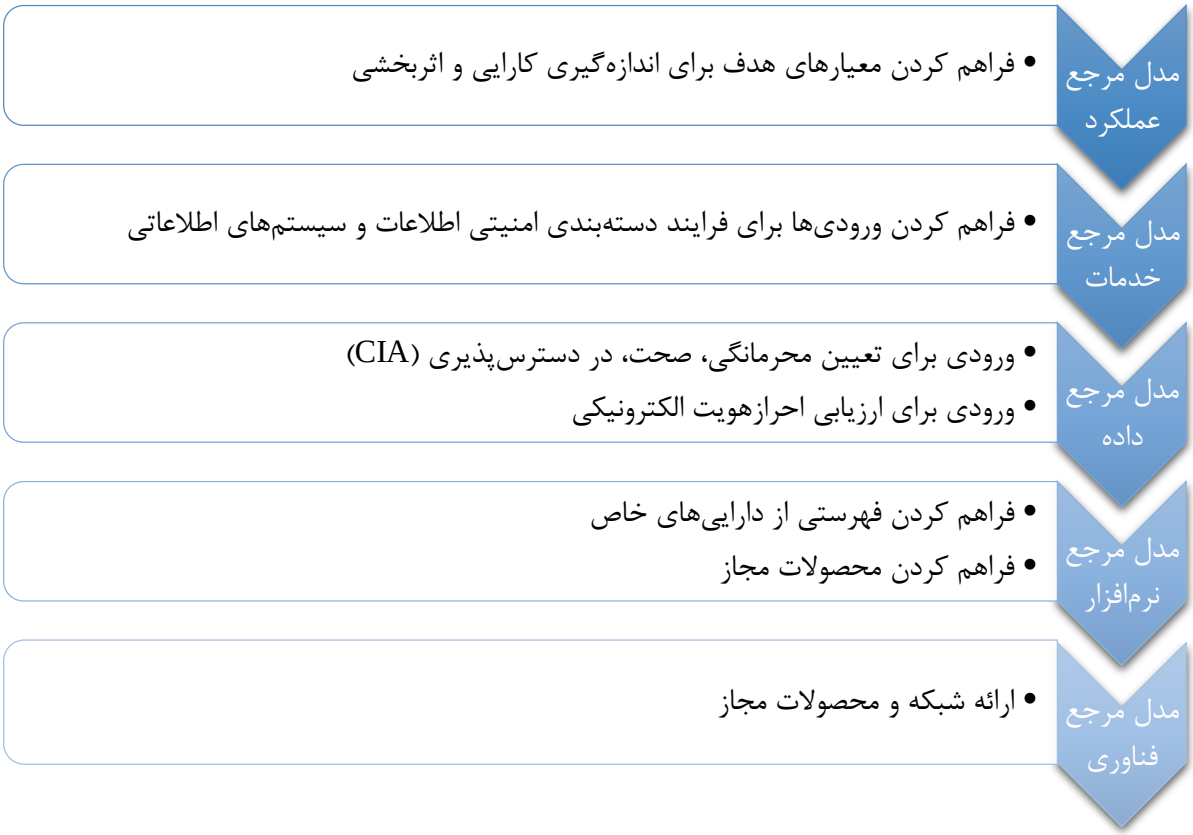
مدل مرجع داده به منظور ارایه یک چارچوب مشترک انعطاف‌پذیر برای به اشتراک‌گذاری موثر اطلاعات دولتی در سراسر سازمان‌ها، افزایش یکپارچگی و نیز استفاده مجدد از فرصت‌ها و پشتیبانی از قابلیت همکاری با درنظر گرفتن امنیت، حفظ حریم خصوصی و استفاده مناسب از اطلاعات، طراحی شده است. مدل مرجع داده ابزاری استاندارد را ارایه می‌کند که می‌تواند داده‌ها را توصیف، طبقه‌بندی و به اشتراک بگذارد. این مدل، داده‌ها و اطلاعات و نیز مدل‌های موردنیاز برای برقراری امنیت و حفظ حریم خصوصی (به عنوان مثال تعیین محرمانگی، صحت و دسترس‌پذیری) و ورودی‌های لازم برای ارزیابی احرازهویت الکترونیکی را فراهم می‌کند. در مقابل، مدل مرجع امنیت الزامات، نیازمندی‌ها، محدودیت‌ها و کنترل‌های امنیتی مناسب برای حفاظت از داده‌ها (جمع‌آوری، ذخیره‌سازی و تبادل اطلاعات) را ارایه می‌نماید.

مدل مرجع نرم‌افزار، یک طبقه‌بندی مبتنی بر مولفه است که استانداردها و فناوری‌های مربوط به نرم‌افزار و سیستم‌هایی را دسته‌بندی می‌کند و قابلیت‌های خدمت را پشتیبانی و فراهم می‌کند و همچنین از یکپارچه‌سازی برنامه‌های کاربردی موجود سازمان و نیز استانداردسازی و استفاده مجدد از فناوری و مولفه‌های خدمت پشتیبانی می‌کند.

در مقابل، مدل مرجع امنیت، اطلاعات، استانداردها و آزمون‌های امنیتی را جهت امن نمودن سرویس‌ها و برنامه‌های کاربردی فراهم می‌کند.

مدل مرجع فناوری، دربردارنده ساختار طبقه‌بندی فناوری‌ها، استانداردها و ابزارهای فناوری اطلاعات در راستای ارایه سرویس‌های فاوا به ذینفعان است. این مدل، طبقه‌بندی همه فناوری‌ها و استانداردهای فناوری اطلاعات را با نگاه سرویس محور ارایه نموده و اصول و رهنمون‌هایی برای استفاده از آن در سطح دستگاه‌های اجرایی ارایه می‌نماید. در واقع این مدل تصویر کلان معماری فناوری دولت را ترسیم می‌نماید تا در مرحله بعد هر دستگاه اجرایی جزییات و نحوه پیاده‌سازی این نقشه کلان را در قالب جزییات معماری سازمانی خود تدوین و پیاده‌سازی نماید. این مدل استانداردها و کنترل‌های فناوری و نیز محصولات مجاز موردنیاز جهت پشتیبانی از الزامات امنیتی و حریم خصوصی را ارایه می‌کند. در مقابل، مدل مرجع امنیت، استانداردها و اطلاعات امنیتی جهت امن نمودن فناوری و زیرساخت را ارایه می‌کند.

در سطح بالا، ارتباط بین سایر مدل‌های مرجع با مدل امنیت و ارتباط مدل مرجع امنیت با سایر مدل‌ها به ترتیب در اشکال (۲- ۱۵) و (۲- ۱۶) بیان شده است.



شکل (۲- ۱۵): ارتباط سایر مدل‌های مرجع با مدل مرجع امنیت

شکل (۲- ۱۶): ارتباط مدل مرجع امنیت با سایر مدل‌های مرجع

۲-۸- مدل بلوغ امنیت

چارچوب امنیتی، یک مدل مرجع برای دامنه‌های امنیت ارائه می‌کند که توسط آن یک سازمان می‌تواند از افراد، داده‌ها، نرم‌افزار و زیرساخت خود محافظت کند. در هر دامنه، می‌تواند درجه‌های حفاظتی مختلفی، از پایه تا ویژه و بهینه وجود داشته باشد. سازمان‌ها در قابلیت‌ها یا مقاصد خود برای توسعه راه‌حل‌های امنیتی بسته به بودجه، تجربه، مجموعه مهارت‌ها و ریسک‌پذیری‌شان متفاوت هستند. به عنوان مثال، سازمانی ممکن است چندین سال تجربه درباره کنترل‌های دسترسی کاربر داشته باشد، مانند کنترل دسترسی با فناوری پیشرفته خودکاری که در سطح حفاظتی بهینه در دامنه افراد مستقر می‌شود. در همان زمان، ممکن است سازمان در اولین مرحله پیاده‌سازی از یک نرم‌افزار نظارتی باشد، بنابراین احتمالاً در سطح حفاظتی اولیه از امنیت در آن دامنه هستند.

جهت کمک به روشن شدن کنترل‌های امنیتی نشان‌دهنده سطوح بلوغ در داخل هر دامنه، مدل بلوغ امنیت در شکل (۲- ۱۶) آمده است.

به عنوان مثال، رمزنگاری و کنترل دسترسی پایگاه داده نماینده یک سطح پایه به‌منظور حفاظت از داده می‌باشند. برای داشتن یک سطح بهینه از امنیت داده، سازمان باید راه‌حل‌های امنیتی را توسعه دهد که کنترل‌ها در سطوح پایه، ویژه و بهینه که در شکل (۲- ۱۷) نشان داده شده‌اند، را فراهم نماید.

درک امنیتی:
تحلیل جریان
مدیریت رویداد و اطلاعات امنیتی
مدیریت ثبت وقایع

درک امنیتی

	افراد	زیرساخت	نرم‌افزار	داده
بهینه	- هویت دولتی - مدیریت کاربر مجاز - تعیین مجوزها و نقش‌ها به صورت جزئی	- محافظت چندوجهی از شبکه - تشخیص ناهنجاری - امن کردن و مقام‌سازی سیستم‌ها	- تشخیص جعل - همبستگی آسیب‌پذیری‌ها - پویش ترکیبی	- تحلیل جریان داده - داده‌های دولتی - مدیریت کلید رمزنگاری
ویژه	- تخصیص کاربر - مدیریت دسترسی - احرازهویت قوی	- امنیت مجازی‌سازی - مدیریت دارایی - مدیریت امنیت شبکه/ نقاط انتهایی	-حفاظت از برنامه‌های کاربردی وب -پویش کد منبع	- پنهان‌سازی داده - نظارت بر فعالیت پایگاه‌داده - جلوگیری از گم شدن داده
پایه	- مدیریت دایرکتوری	- امنیت محیط - ضد ویروس	- پویش نرم‌افزار	- رمزنگاری - کنترل دسترسی به پایگاه‌داده

شکل (۲- ۱۷): مدل بلوغ امنیت

مدل مرجع امنیت

فصل سوم

اصول طراحی معماری امنیت

۳- اصول طراحی معماری امنیتی

یک سازمان بایستی هنگام طراحی معماری امنیت خود اصولی را در تمام سطوح چارچوب معماری در نظر داشته باشد که عبارتند از:

- **باز بودن**[1]

باز بودن یکی از اولویت‌های اصلی در یک محیط سازمانی است. باز بودن شامل پشتیبانی از تمام پلتفرم‌های اصلی، زمان‌های اجرا و زبان‌ها، پشتیبانی از استانداردهای اصلی (مهم) صنعت، الگوریتم‌ها و رابط‌های منتشر شده، اجتناب از امنیت با ابهام، مدل‌های تهدید و اعتماد مستند شده و پشتیبانی از معیارهای مشترک و غیره می‌باشد.

- **امنیت به طور پیش‌فرض**[2]

امنیت نباید به‌عنوان یک ضمیمه به راه‌حل‌های فناوری اطلاعات اضافه شود (یا به آن فکر شود). این وضعیت به وسیله تعریف و مدیریت منسجم پیکربندی‌ها، یک مجموعه سازگار و منسجم از نقش‌های امنیتی در تمام محصولات و یک رابط کاربری مدیریت امنیت منسجم امکان‌پذیر می‌شود.

- **طراحی پاسخگویی**[3]

با وجود نیازمندی‌های زیاد در زمینه تطابق‌پذیری، این مساله مهم است که تمام اقدامات مربوط به امنیت بتواند ذخیره (ثبت) و ممیزی شود، زیرساخت ممیزی و حسابرسی به منظور رسیدگی به این رویدادها بایستی مقیاس‌پذیر بوده و اطلاعات ممیزی تغییرناپذیر باشد.

- **طراحی مقررات**[4]

مقررات، اکثر الزامات و نیازمندی‌ها را در پروژه‌های امنیت فناوری اطلاعات بیان کرده و در طول زمان تغییر می‌کنند. رسیدگی و بررسی این وضعیت نیازمند پشتیبانی منعطف از محدودیت‌هایی است که

---

[1] Openness
[2] Security by Default
[3] Design for Accountability
[4] Design for Regulations

توسط قوانین و مقررات دولتی و استانداردهای صنعتی وضع می‌شوند و همچنین نیازمند پشتیبانی از قابلیت‌های پیگیری مقررات، استانداردها و سیاست‌های کسب‌و کار و امنیتی مورد استفاده در پیاده‌سازی می‌باشد.

- **طراحی حفظ حریم خصوصی[1]**

در حال حاضر در اشتراک‌گذاری داده، حریم خصوصی بسیار مهم است. راه‌حل‌ها بایستی موارد استفاده از اطلاعات شناسایی شخصی و مکانیزم‌های حفاظت از داده‌ها را مشخص کنند و اصول اطلاع‌رسانی، حق انتخاب و دسترسی را فراهم نمایند.

- **طراحی با قابلیت توسعه[2]**

راه‌حل‌های خوب مبتنی بر مؤلفه هستند و به منظور پشتیبانی از مکانیزم‌های مختلف در چارچوب‌های مشابه، مدیریت مکانیزم‌ها را از خود مکانیزم‌ها جدا می‌کنند. سیستم‌های توسعه‌یافته باید امکان افزایش و گسترش مکانیزم‌های جدید در داخل چارچوب مدیریتی موجود را داشته باشند.

- **طراحی مشترک[3]**

راه‌حل‌های متعددی می‌توانند از یک محیط فناوری اطلاعات بهره ببرند، مانند یک مرکز سرویس مشترک. برای دستیابی به این هدف، سرویس‌های امنیتی و مدیریتی باید قادر به پوشش چندین دامنه باشند که هر دامنه به‌طور بالقوه مجموعه سیاست‌های امنیتی، هویت‌ها، مدل‌ها و غیره را به‌صورت مستقل برای خودش ارائه می‌کند.

- **طراحی با هدف قابلیت استفاده[4]**

تمام سرویس‌های امنیتی باید به آسانی و راحتی توسط مخاطبان مختلف قابل استفاده باشند. این مخاطبان شامل برنامه‌نویسانی هستند که برنامه‌های کاربردی را با سرویس‌های امنیتی، سیستم‌های مدیریتی که سیاست‌های امنیتی را ایجاد، به‌روزرسانی و مدیریت می‌کنند و دیگر مصنوعات امنیتی،

[1] Design for Privacy
[2] Design for Extensibility
[3] Design for Sharing
[4] Design for Consumability

توسعه و یکپارچه می‌سازند و همچنین شامل افرادی می‌باشند که فعالیت‌های امنیتی را مدیریت، فعالیت‌های امنیتی و دسترسی به منابع محافظت شده را ممیزی می‌کنند.

- **محافظت چند سطحی (سطوح مختلف محافظت)[1]**

دفاع در عمق یک اصل کلی است که با افزایش تعداد لایه‌های دفاعی، مسیر دسترسی نفوذگر به منطقه حساس و کلیدی را دشوار می‌سازد.

- **تفکیک مدیریت و اجرای امنیت[2]**

سرویس‌های مدیریت امنیت (هویت، مجوزدهی، حسابرسی و غیره) از طریق یک زیرساخت امنیتی اختصاصی و به اشتراک گذاشته شده، ارائه می‌شوند و امکان نظارت و اجرای سازگار و منسجم را فراهم می‌کنند. اجرا نیز خود از طریق رمزنگاری، اجرای سیاست‌ها یا جداسازی فیزیکی انجام می‌شود و محدود به منابع نگه‌داری می‌شود.

- **منابع امنیتی و آگاهی از زمینه‌های امنیتی آن‌ها[3]**

منابع و بازیگران همیشه باید از محیط خودشان (از جمله مکان‌های فیزیکی و یا منطقی) و وضعیت امنیتی آن‌ها آگاه باشند.

- **سازگاری در رویکردها، مکانیزم‌ها و مؤلفه‌های نرم‌افزار[4]**

دو لایه محافظتی مستقل برای یک منبع، می‌تواند امنیت را بهبود بخشد. اما استفاده از دو مکانیسم مختلف برای یک هدف مشابه برای دو منبع، احتمال این که حداقل یکی از آن‌ها با شکست مواجه شود را افزایش می‌دهد (به‌علاوه مدیریت را نیز تحت تأثیر قرار می‌دهد).

---

[1] Multiple levels of protection
[2] Separation of security management, enforcement
[3] Security-critical resources and awareness of their security context
[4] Consistency in approaches, mechanisms, and software components

فصل چهارم

انواع چارچوب‌های معماری امنیتی

۴-۱- مدل امنیتی SABSA

یک چارچوب معماری و روشی برای ایجاد معماری امنیتی است که برای نیازهای کسب‌وکار و مشخصات ریسک سازمان ساخته شده و برای اولین بار توسط John Sherwood در سال ۱۹۹۵ توسعه‌یافته و در سال ۱۹۹۶ به عنوان SABSA "روشی برای توسعه استراتژی و معماری امنیتی فراسازمانی" منتشر شده است. مدل SABSA شامل شش لایه است و شامل موارد معماری امنیتی زمینه‌ای (Contextual)، معماری امنیتی مفهومی، معماری امنیتی منطقی، معماری امنیتی فیزیکی، معماری امنیتی مؤلفه‌ای، معماری امنیتی عملیاتی می‌شود. از ویژگی‌های مدل امنیتی SABSA می‌توان به موارد زیر اشاره کرد:

- مدل SABSA تمامی دیدگاه‌ها یا دامنه‌ها را پوشش می‌دهد (کسب‌و کار، اطلاعات، کاربردی، تکنولوژی)
- SABSA مستقل از چارچوب Zachman توسعه داده شده اما دارای ساختاری مشابه می‌باشد.

۴-۲- معماری امنیتی باز[1] (OSA):

OSA یک معماری امنیتی فراسازمانی است که در آن کسب‌وکار (استراتژی و فرآیندها)، برنامه‌های کاربردی، اطلاعات (مخزن داده) و تکنولوژی (معماری شبکه) پوشش داده شده‌اند. چارچوب OSA یک مجموعه اطلاعات کلی را ارائه می‌نماید. اساسی‌ترین بخش این اطلاعات، چشم‌انداز معماری امنیتی می‌باشد که محدوده مشخص شده‌ای را برای چارچوب OSA تعریف می‌کند.

معماری OSA به دلیل این‌که دستورالعمل‌های کمی را برای پیاده‌سازی ارائه می‌نماید، نمی‌تواند به‌عنوان یک متدولوژی درنظر گرفته شود. اگرچه هریک از الگوها در کتابخانه الگو دارای برخی از توضیحات می‌باشند و تعدادی دستورالعمل را نیز ارائه می‌نمایند، اما هیچ دستورالعمل کلی برای معماری وجود ندارد.

[1] Open Security Architecture

۳-۴- معماری امنیت فراسازمانی باز[1] (O-ESA):

O-ESA، برای اولین بار به عنوان معماری امنیت فراسازمانی کنسرسیوم برنامه‌های کاربردی شبکه در سال ۲۰۰۴ معرفی شد. اعضای این کنسرسیوم یک معماری امنیتی فراسازمانی سیاست محور را مطرح کردند که این معماری قادر به مقابله با پیچیدگی و تغییرات سریع در داخل سازمان می‌باشد.

معماری O-ESA، چندین حوزه از معماری امنیت فراسازمانی را شرح می‌دهد. این حوزه‌ها عبارتند از: محرک‌های کسب‌وکار[2]، مدیریت برنامه امنیت، کنترل امنیت، فناوری امنیت، عملیات امنیت.

تمرکز اصلی O-ESA بر روی حوزه فناوری می‌باشد. در نتیجه این امر باعث می‌شود که معماری امنیتی، یک معماری امنیتی تک‌منظوره (برخلاف یک معماری امنیتی عمومی مانند SABSA) باشد.

اگرچه O-ESA به دلیل عدم تعریف اقدامات و الزامات ذی‌نفعان برای ایجاد یک معماری، نمی‌تواند به‌عنوان متدولوژی برای معماری امنیتی در نظر گرفته شود، اما می‌تواند به‌عنوان یک چارچوب درنظر گرفته شود.

۴-۴- معماری امنیت اطلاعات فراسازمانی گارتنر

گارتنر یک روش تعیین شده برای ارزیابی و توسعه معماری امنیت جامع فناوری اطلاعات و توسعه استراتژی‌هایی از جمله معماری مدیریت هویت و دسترسی می‌باشد. گارتنر یک طبقه‌بندی مشابه چارچوب Zachman، یک فرآیند مشابه TOGAF و یک متدولوژی مشابه معماری فراسازمانی فدرال می‌باشد.

این مدل برای انتقال برخی اصول مهم از معماری امنیتی به کار می‌رود:

- چارچوب معماری امنیتی باید قادر به برنامه‌ریزی و طراحی از طریق تکرارهای متعدد باشد. (سطوح انتزاعی یا جداسازی سطوح)
- مصنوعات معماری امنیتی شامل مدل‌ها، اصول و الزامات مستند شده‌ای از سطوح مختلف انتزاعی می‌باشد.

[1] Open Enterprise Security Architecture
[2] Business drivers

- معماری بایستی حداقل، دیدگاه‌های اطلاعات، کسب‌وکار و فنی را پوشش دهد.
- نقطه شروع برای تمام برنامه‌ریزی‌های امنیتی بایستی زمینه کسب‌وکار باشد.

در معماری گارتنر سه سطح مفهومی، منطقی و پیاده‌سازی و سه دیدگاه مختلف کسب‌وکار، اطلاعات و فنی وجود دارد.

۴-۵- معماری فراسازمانی فدرال[1]:

در سال ۱۹۹۶ قانونی موسوم به کلینگر کوهن در کنگره آمریکا به تصویب رسید که مطابق آن، همه وزارتخانه‌ها و سازمان‌های فدرال آمریکا ملزم شدند معماری فناوری اطلاعات خود را ایجاد کنند. مسئولیت تدوین، اصلاح و اجرای معماری فناوری اطلاعات یکپارچه در هر سازمان بر عهده مدیر ارشد اطلاعاتی آن سازمان قرار گرفت. در سال ۱۹۹۸ بر اساس همین قانون شورای مدیران ارشد اطلاعاتی موظف شدند که جهت توسعه، پشتیبانی و تسهیل پیاده‌سازی معماری اطلاعات سیستم‌های دولتی، راهکار واحدی را ارائه دهد. چارچوب معماری سازمان فدرال در سپتامبر سال ۱۹۹۹ توسط شورای مدیران ارشد اطلاعاتی دولت ایالات متحده آمریکا تهیه و تنظیم شد و آخرین به‌روزرسانی آن در سال ۲۰۱۳ انجام شده است.

این معماری دارای مدل‌های معماری مرجع عملکرد، کسب‌وکار، داده، برنامه کاربردی، زیرساخت و امنیت می‌باشد. مدل مرجع امنیتی به طراحان اجازه می‌دهد که معماری امنیت را در تمام سطوح معماری فدرال (فدرال، ملی، سازمان، مؤلفه، سامانه، برنامه کاربردی و غیره) به کار ببرند. مدل مرجع امنیت فدرال دارای سه بعد اهداف، ریسک و کنترل می‌باشد و ورودی خود را از سایر مدل‌های مرجع فوق می‌گیرد.

۴-۶- مدل TOGAF 9.1:

TOGAF یک چارچوب معماری سازمانی است. چارچوب معماری سازمانی که توسط Open Group ارائه شده است. TOGAF ابزاری برای کمک به پذیرش، تولید، استفاده و نگهداری طرح‌های معماری سازمانی

[1] Federal Enterprise Architecture Framework

می‌باشد. TOGAF بر پایه یک مدل فرآیندی تکرارپذیر می‌باشد که توسط بهترین راهکارهای عملی و مجموعه‌ای از اجزای معماری با قابلیت استفاده مجدد، پشتیبانی می‌گردد.

اولین نسخه TOGAF، در سال ۱۹۹۵ بر پایه چارچوب معماری فنی وزارت دفاع ایالات متحده آمریکا برای مدیریت اطلاعات (TAFIM[1]) ایجاد شد. با شروع کردن از این پایه، انجمن معماری Open Group نسخه‌های موفقی از TOGAF را در دوره‌های زمانی معین ایجاد کرد. آخرین نسخه TOGAF 9.1 در دسامبر سال ۲۰۱۱ منتشر شد.

TOGAF توسعه چهار حوزه معماری را پوشش می‌دهد: معماری کسب‌وکار، معماری داده، معماری برنامه کاربردی و معماری فناوری. این حوزه‌ها به‌عنوان زیرمجموعه‌هایی از یک معماری سازمانی کلی پذیرفته می‌شوند.

در مدل مرجع، راهنمایی برای کمک به طراحان فراسازمانی و مسئولین امنیت به منظور اجتناب از نادیده گرفته شدن ملاحظات امنیتی حیاتی در نظر گرفته شده است. این راهنما، معمار (طراح) فراسازمان را از آنچه معمار امنیت در طول اجرای معماری امنیت نیاز خواهد داشت، آگاه می‌کند. در طول مراحل توسعه معماری، دستورالعمل‌هایی در مورد اطلاعات خاص امنیتی که باید جمع‌آوری شود و مراحلی که باید انجام شود، ارائه شده است.

۷-۴- مدل معماری فراسازمانی NIST:

یک مدل مرجع برای معماری فراسازمانی است که در سال ۱۹۸۸ در جهت مدیریت اطلاعات آغاز شده و توسط مؤسسه ملی استاندارد و فناوری (NIST) با همکاری ACM، انجمن کامپیوتر IEEE و گروه کاربران مدیریت داده فدرال تدوین شده است. این مدل از پنج لایه تشکیل شده است: معماری کسب‌وکار، معماری اطلاعات، معماری سیستم‌های اطلاعاتی، معماری داده و سامانه‌های تحویل داده که معماری داده را پشتیبانی

[1]TAFIM: Technical Architecture Framework for Information Management

می‌نمایند. در این مدل معماری امنیت به‌صورت حوزه جدا در نظر گرفته نشده و در سطح معماری اطلاعات باید اصول، اهداف و ملزومات امنیتی در نظر گرفته شود.

۸-۴- چارچوب معماری فراسازمانی خزانه‌داری[1]:

TEAF یک چارچوب معماری فراسازمانی خزانه‌داری بوده که فرآیندهای کسب و کار خزانه‌داری را از نظر محصولات پشتیبانی می‌نماید و بر اساس چارچوب Zachman، فدرال و C4ISR ساخته شده است. این چارچوب توسط بخش ایالت متحده خزانه‌داری توسعه داده شده و در جولای سال ۲۰۰۰ منتشر شده است که مناسب سامانه‌های خزانه‌داری، مدیریت بودجه و مدیریت مالی می‌باشد.

ماتریس TEAF که جهت تدوین یک ساختار ساده و یکسان برای کل چارچوب استفاده می‌شود، شامل چهار جنبه (عملکرد، اطلاعات، سازمان و زیربنا) به‌عنوان ستون و چهار دیدگاه (برنامه‌ریز، مالک، طراح و سازنده) به‌عنوان سطرهای ماتریس می‌باشد. در این معماری، امنیت به‌عنوان یک لایه جدا در نظرگرفته نشده است، اما به‌عنوان یک دیدگاه عرضی بر روی تمام دیدگاه اعمال می‌شود.

[1] Treasury Enterprise Architecture Framework

پیوست شماره ۱

سازمان‌های امنیت فضای تبادل اطلاعات

و استانداردهای امنیتی ملی

سازمان‌های امنیت فضای تبادل اطلاعات

➢ مرکز امداد و هماهنگی رایانه‌ای کشور (ماهر)

امروزه اطلاع‌رسانی، آموزش و هماهنگی‌های مختلف در زمینه امنیت فضای تبادل داده، امری اجتناب‌ناپذیر قلمداد می‌شود. لذا شرکت فناوری اطلاعات، در راستای ایجاد یک نقطه کانونی در سطح وزارت ارتباطات و فناوری اطلاعات، برای انجام فعالیت‌های هماهنگ راهبری رخدادهای فضای تبادل داده، اقدام به ایجاد یک مرکز با عنوان "مرکز مدیریت امداد و هماهنگی عملیات رخداد رایانه‌ای" یا به اختصار "ماهر" نموده است. این مرکز با ایجاد هماهنگی با سایر تیم‌های فوریت‌های امنیتی و مراکز امداد رایانه‌ای در سطح کشور، اطلاعات ارزشمند خود را به‌صورت یکسان در اختیار سایر گروه‌ها قرارداده و به‌روز بودن این دانش را تضمین می‌نماید. در واقع خدمات و پشتیبانی‌های لازم را از یک قلمرو تعریف شده برای جلوگیری، بررسی و پاسخگویی به حوادث امنیت رایانه به عمل می‌آورد. هنگامی که یک حادثه امنیتی رخ دهد، داشتن یک راه کار مؤثر برای پاسخ به حادثه، بسیار حیاتی است. سرعت عمل سازمان در تشخیص، تحلیل و پاسخ به یک حادثه، باعث می‌شود که میزان خسارت و هزینه بازیابی سامانه کاهش یابد. تیم امداد، پاسخ سریع به یک حادثه امنیتی را هدایت کرده و سامانه را بازیابی می‌کند. این تیم با حوادث امنیتی و سامانه‌های مورد حمله آشنا بوده و در نتیجه می‌تواند به خوبی عملیات بازیابی و استراتژی‌های پاسخ به حمله را هماهنگی کند. همچنین تیم‌های امداد با یکدیگر و دیگر سازمان‌های امنیتی مرتبط، در ارتباط هستند و اخطارهای امنیتی را بسیار سریع مبادله کرده و حتی‌الامکان قبل از وقوع حملات، از آن‌ها پیشگیری می‌کنند. این تیم‌ها کارمندان سازمان را مورد آموزش و آگاهی‌رسانی قرار می‌دهند و با ارائه مشاوره امنیتی موجب پیشگیری از حملات آینده می‌شوند.

در واقع اهداف مرکز، متناسب با اهداف سازمان و جامعه قلمرو آن تعیین می‌گردد. در اکثر موارد محافظت از سرمایه‌های حیاتی اطلاعات به‌عنوان هدف بنیادین مورد قبول بوده و لذا در صورت وقوع حادثه، حداقل‌کردن خرابی‌ها و کنترل آن، پاسخ مؤثر، بازیابی اطلاعات و جلوگیری از حوادث مشابه در آینده، به عنوان اهداف اساسی مورد اجماع می‌باشد.

این مرکز جهت تحقق اهداف فوق، اطلاعات جامعی از حوادث، ضعف‌های امنیتی و آسیب‌پذیری‌های سامانه‌ها و نرم‌افزارهای مورد استفاده در زیرساخت‌های سازمانی و جامعه قلمرو را جمع‌آوری می‌نماید و به یک نقطه کانونی و منبعی قابل اعتماد تبدیل می‌گردد. همچنین این مرکز به عنوان یک پایگاه مرکزی اطلاعات، اجازه می‌یابد که کلیه موارد مرتبط با امنیت را در سطح سازمان جمع‌آوری و ساماندهی نماید. این امر فرصتی جهت تجزیه و تحلیل و ارتباط‌دهی کلیه وقایع که هر یک به تنهایی مرتبط به نظر نمی‌رسند را فراهم آورده و نقش آن را به عنوان یک عنصر کلیدی در کاهش تلفات و مخاطرات ارتقاء می‌بخشد.

➢ مرکز مدیریت راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا) ریاست جمهوری

در جمهوری اسلامی ایران به‌منظور ایفای نقش حاکمیت در تأمین امنیت فضای مجازی و حفظ زیرساخت‌های حیاتی کشور در مقابل حملات الکترونیکی، مرکز مدیریت راهبردی افتای ریاست جمهوری مأموریت یافته است در تعامل با دستگاه‌های ذیربط، نسبت به امن‌سازی زیرساخت‌های دستگاه‌های حیاتی اقدام کند.

این مرکز نقش حلقه واسط بین سه بخش اصلی یعنی مراجع حاکمیتی، دستگاه‌های اجرایی و بخش خصوصی را در حوزه افتا برعهده دارد. در زمینه هماهنگی با بخش حاکمیتی، این مرکز با شورای عالی و مرکز ملی فضای مجازی و نیز شورای عالی امنیت ملی مرتبط است. از سوی دیگر، کلیه دستگاه‌های اجرایی کشور، به‌عنوان حوزه مصرف محصولات فتا و خدمات افتا و بخش خصوصی نیز به‌عنوان حوزه تولید محصولات و خدمات مذکور با این مرکز مرتبط می‌باشند.

سیاست‌های کلی این مرکز را می‌توان در محورهای ذیل دسته‌بندی نمود:

- اشراف بر فناوری‌های نوین و بهره‌گیری از آن‌ها
- انجام امور رگولاتوری (تنظیم مقررات)، ساماندهی، نظارت و هماهنگی حوزه افتا در سطح کشور
- بهره‌گیری از تدابیر صحیح و فنی، جهت پیشگیری از مخاطرات امنیتی، تشخیص به‌موقع، مقابله صحیح و هوشمندانه با مخاطرات
- توجه اکید به رویکردهای ایجابی در انجام ماموریت‌ها و در حد امکان دوری از رویکردهای سلبی
- امن‌سازی مدبرانه فضای تولید و تبادل اطلاعات به منظور عدم توقف استمرار ارائه خدمات

- انجام اقدامات حمایتی از صنعت افتا بومی کشور
- تأسیس مراکز افتا در استان‌ها با رویکرد نظارتی و کنترلی

و همچنین مأموریت مرکز افتا عبارت است از:

❖ ماموریت‌های راهبردی- تدوین راهبردها، راهکارها و سیاست‌های اجرایی مورد نظر در چارچوب سیاست‌های حاکمیتی

- تدوین و ابلاغ طرح امن‌سازی زیرساخت‌های حیاتی
- تدوین نظام ارزیابی امنیتی محصولات فتا و خدمات افتا
- بومی‌سازی استانداردهای ارزیابی امنیتی
- تدوین بخشنامه‌ها، دستورالعمل‌ها و آئین‌نامه‌های ارتقاء امنیت
- تدوین نظام پیشگیری و مقابله با حوادث فضای مجازی
- ارزیابی راهبردی سیاست‌های کلی نظام در حوزه افتا

❖ نظارتی- نظارت بر حسن اجرای بخشنامه‌ها، دستورالعمل‌ها و راهکارهای ابلاغی

- ممیزی سامانه‌های مدیریت امنیت اطلاعات (ISMS)
- نظارت در اجرای طرح امن‌سازی زیرساخت‌های حیاتی
- نظارت بر عملکرد آزمایشگاه‌های ارزیابی امنیتی و شرکت‌ها

❖ عملیاتی- پیشگیری و مدیریت حوادث سایبری در دستگاه‌های اجرایی کشور

- راه‌اندازی تیم امداد رایانه برای زیرساخت‌ها
- اجرای عملیات ارزیابی امنیتی و رصد آسیب‌پذیری زیرساخت‌ها
- ارایه خدمات تخصصی فارنزیکی و تحلیلی حوزه بدافزار برای زیرساخت‌ها
- ارتقا توان شناسایی و مقابله با بدافزارهای ناشناخته در زیرساخت‌ها

❖ حمایتی و فرهنگ سازی- با هدف تکیه بر فناوری بومی و توانمندی‌های تخصصی داخلی

- برگزاری همایش‌ها، کارگاه‌های آموزشی و جلسات توجیهی برای مدیران بخش خصوصی و نیز مدیران دستگاه‌ها در سطح کشور به منظور فرهنگ‌سازی
- برگزاری دوره‌های توجیهی امنیتی برای صیانت از مدیران و کارشناسان بخش خصوصی
- آگاهی‌رسانی از طریق تهیه و توزیع خبرنامه و سامانه پیام‌رسان
- مشارکت در تأمین هزینه‌های آزمایشگاهی ارزیابی امنیتی محصولات
- تسهیل فرایند اداری برای بخش خصوصی جهت انجام پروژههای فاوایی
- تاسیس مراکز استانی جهت حمایت از ظرفیت‌های استانی

➢ **سازمان پدافند غیرعامل کشور**

پدافند غیرعامل به معنای کاهش آسیب‌پذیری در هنگام بحران، بدون استفاده از اقدامات نظامی و صرفاً با بهره‌گیری از فعالیت‌های غیرنظامی، فنی و مدیریتی است. اقدامات پدافند غیرعامل شامل پوشش، پراکندگی، تفرقه و جابجایی، فریب، مکان‌یابی، اعلام خبر، قابلیت بقا، استحکامات، استتار، اختفاء و سازه‌های امن می‌باشد. در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری ایفا کنند در حالی که در پدافند عامل مانند سامانه‌های ضدهوایی و هواپیماهای رهگیر، تنها نیروهای مسلح مسئولیت برعهده دارند.

سازمان پدافند غیرعامل کشور یک سازمان (نهاد) حاکمیتی (لشکری و کشوری) به منظور افزایش بازدارندگی، کاهش آسیب‌پذیری و تداوم فعالیت‌های ضروری می‌باشد.

➢ قرارگاه پدافند سایبری کشور

در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، مؤسسات غیردولتی و نهادهای دولتی و حاکمیتی، در فضای سایبری انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا، شکل گرفته است. عمده فعالیت‌های رسانه‌ای به این فضا منتقل شده و بیشتر مبادلات مالی از طریق این فضا انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. سهم درآمد حاصل از کسب‌وکارهای فضای سایبر در تولید ناخالص ملی افزایش چشم‌گیر یافته و از میان شاخص‌های تعیین شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه سایبر، سهم عمده‌ای را به خود اختصاص داده‌اند. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تأثیر عمده می‌پذیرد. به عبارت دیگر، وجوه مختلف زندگی شهروندان، به معنای واقعی، با این فضا در آمیخته و هرگونه بی‌ثباتی، ناامنی و چالش در این حوزه، مستقیماً وجوه مختلف زندگی شهروندان را به مخاطره خواهد انداخت.

ضرورت و اهمیت صیانت از فضای سایبری کشور، در مقابل انواع تهدیدات و تهاجمات سایبری و به‌ویژه جنگ سایبری، موجب گردید تا قرارگاه پدافند سایبری کشور با هدف تمرکز بر دفاع از زیرساخت‌های حیاتی، حساس و مهم کشور در مقابل انواع تهدیدات و تهاجمات سایبری ایجاد شود. قرارگاه پدافند سایبری کشور وظیفه صیانت از مرزهای سایبری کشور در حوزه غیرنظامی و به‌ویژه در حوزه ایمن‌سازی زیرساخت‌های حیاتی و حساس واقع شده در این فضای سایبری را بر عهده خواهد داشت.

وظایف قرارگاه پدافند سایبری کشور

۱) پایش تهدیدات سایبری کشور

۲) تهیه، تدوین و تصویب دستورالعمل تخصصی آمادگی دستگاه‌ها در برابر تهدیدات سایبری و نظارت‌بر حسن اجرای آن

۳) راه‌اندازی مرکز پدافند سایبری کشور به‌منظور تولید محصولات امنیتی و دفاعی کشور

۴) تعامل و هماهنگی‌های لازم با کمیته پدافند غیرعامل دستگاه‌ها، استان‌ها، مناطق ویژه در تعیین فرضیه‌ها و سناریوهای محتمل درحوزه پدافند سایبری

۵) هدایت، نظارت و ارزیابی اجرای طرح‌های پدافند غیرعامل حوزه سایبری

۶) برنامه‌ریزی لازم برای تعیین و اجرای طرح‌های اجرایی پدافند غیر عامل حوزه سایبری

۷) برقراری ارتباط با مراکز پدافند سایبری دستگاه‌های کشور به منظور تبادل اطلاعات و هماهنگی و هدایت کلی آن‌ها

وظایف مراکز پدافند سایبری

- شناسایی اهداف امنیت اطلاعات مرتبط با زیرساخت
- شناسایی تهدیدهای مرتبط با زیرساخت‌های مبتنی‌بر فضای سایبری با توجه به اهداف امنیتی
- شناسایی آسیب‌پذیری‌های مرتبط با زیرساخت‌های مبتنی بر فضای سایبری با توجه به اهداف و تهدیدها
- تحلیل مخاطرات مرتبط با هر آسیب‌پذیری
- شناسایی نیازمندی‌های امنیتی موردنیاز در جهت مقابله با مخاطرات و ارائه گزارش به کمیته پدافند غیرعامل دستگاه، استان، منطقه ویژه و قرارگاه پدافند سایبری کشور
- نظارت بر تأمین نیازمندی‌های امنیتی شناسایی شده در دستگاه، استان، منطقه ویژه
- تحلیل و بررسی زیرساخت‌های موجود در جهت تحقق راهبرد امنیتی دفاع در عمق
- آماده‌سازی و اعزام تیم واکنش سریع در مواقع وقوع رخداد در جهت مدیریت آن
- کسب آشنایی با آخرین رخدادهای امنیتی فضای سایبری در سطح جهان
- اطلاع‌رسانی‌های عمومی و مدیریتی در زمینه امنیت فضای سایبری

- برگزاری دوره‌های آموزشی پدافند سایبری برای کارکنان متناسب با نیاز دستگاه
- گزارش موارد کشف بدافزارها و آسیب پذیری‌ها به قرارگاه پدافند سایبری کشور
- گزارش هرگونه حادثه سایبری از جمله سرقت هویت افراد مجاز و ورود غیرمجاز به شبکه‌ها و قطع خدمات به قرارگاه پدافند سایبری

➢ **پلیس فضای تولید و تبادل اطلاعات ناجا**

توسعه روزافزون زیرساخت‌های فناوری اطلاعات و ارتباطات در کشور و افزایش کاربران و استفاده‌کنندگان از اینترنت و سایر فناوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتا کشوری و محلی، ارتباطات ماهواره‌ای از جمله دلایلی است که لزوم ایجاد و توسعه سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطلاعات جمهوری اسلامی ایران را توجیه می‌کند. همچنین توسعه خدمات الکترونیک در کشور نظیر دولت الکترونیک، بانکداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سایر خدمات از این دست، نیز لزوم ایجاد پلیسی تخصصی در مجموعه نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند.

از سوی دیگر، با گسترش جرایم در حوزه فضای تولید و تبادل اطلاعات کشور (فتا) مثل کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری[1] و جرایم اخلاقی و برخی جرایم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصصی که توان پی‌جویی و رسیدگی به جرایم سطح بالای فناورانه داشته باشد، به‌وجود آید.

پلیس فضای تولید و تبادل اطلاعات ایران یا پلیس سایبری ایران با نام مختصر فتا، که یک واحد تخصصی نیروی انتظامی جمهوری اسلامی ایران است که وظیفه آن جلوگیری و مبارزه با ایجاد کلاهبرداری اینترنتی[2]

[1] Pornography
[2] Phishing

و جعل، سرقت اینترنتی، هک و نفوذ، جرایم سازمان یافته رایانه‌ای، هرزه‌نگاری و به‌خصوص تجاوز به حریم خصوصی افراد است. همچنین دسترسی غیرمجاز، برداشت اینترنتی غیرمجاز از حساب‌های بانکی اشخاص، شنود غیرمجاز، جعل رایانه‌ای، تخریب و اخلال در داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، استفاده غیرمجاز از پهنای باند بین‌المللی برای برقراری ارتباطات مخابراتی، تولید و آموزش بدافزارها یا نرم‌افزارهای ارتکاب جرایم سایبری و گذرواژه و اطلاعات کاربران از جمله موضوعاتی است که مورد پیگیری پلیس فتا قرار می‌گیرد. بر پایه اظهارات رئیس پلیس فتا، این پلیس مسئولیت تأمین نظم و امنیت و آسایش عمومی و فردی در فضای مجازی را بر عهده دارد.

استانداردهای ملی

مؤسسه استاندارد و تحقیقات صنعتی ایران به موجب بند یک ماده ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد و استانداردهایی را در حوزه‌های مختلف تدوین نموده است. لیست استانداردهای حوزه امنیت منتشر شده از سوی این مؤسسه در جدول (۱) و همچنین لیست اسناد بالادستی مرتبط با حوزه امنیت در جدول (۲) آمده است.

جدول (۱): لیست استانداردهای حوزه امنیت مؤسسه استاندارد و تحقیقات صنعتی ایران

شماره استاندارد	موضوع	سال تصویب
۱-۱۰۸۲۲	فناوری اطلاعات- فنون امنیتی- مدیریت کلید- قسمت ۱- چارچوب	۱۳۹۲
۵-۱۰۸۲۲	فناوری اطلاعات- فنون امنیتی- مدیریت کلید- قسمت ۵- مدیریت کلید گروهی	۱۳۹۲
۱-۱۰۸۲۵	فناوری اطلاعات- فنون امنیتی- احراز هویت هستار قسمت ۱- کلیات	۱۳۹۱
۲-۱۰۸۲۵	فناوری اطلاعات- فنون امنیتی- احراز هویت هستار قسمت ۲- سازوکارهای استفاده‌کننده از الگوریتم‌های پوشیده‌سازی متقارن	۱۳۹۱
۳-۱۰۸۲۵	فناوری اطلاعات- فنون امنیتی- احراز هویت هستار قسمت ۳- سازوکارهای استفاده‌کننده از فنون امضای رقمی (دیجیتال)	۱۳۹۱
۵-۱۰۸۲۵	فناوری اطلاعات– فنون امنیتی– احراز هویت هستار- قسمت ۵: سازوکارهای استفاده‌کننده از فنون دانش- صفر	۱۳۹۲
۶-۱۰۸۲۵	فناوری اطلاعات- فنون امنیتی- احراز هویت هستار قسمت ۶- سازوکارهای استفاده از انتقال دستی داده‌ها	۱۳۹۱
۳-۱۱۲۱۰	فناوری اطلاعات- فنون امنیتی- امنیت شبکه فناوری اطلاعات- قسمت ۳- امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی	۱۳۹۳
۴-۱۱۲۱۰	فناوری اطلاعات- فنون امنیتی- امنیت شبکه فناوری اطلاعات- قسمت ۴- ایمنی دسترسی از راه دور	۱۳۹۳
۱-۱۱۳۱۰	فناوری اطلاعات- فنون امنیتی- خدمات مهر زمانی- قسمت اول- چارچوب	۱۳۹۴
۴-۱۱۳۱۰	فناوری اطلاعات- فنون امنیت- خدمت‌های مهر زمانی- قسمت ۴- قابلیت ردیابی منابع زمانی	۱۳۹۴
۱-۱۴۸۶۶	فناوری اطلاعات- فنون امنیتی- امنیت شبکه- قسمت ۱- مرور کلی و مفاهیم	۱۳۹۱

شماره استاندارد	موضوع	سال تصویب
۲-۱۶۱۹۶	فناوری اطلاعات– فنون امنیتی– طرح‌های امضای رقمی (دیجیتال) با بازیابی پیام- قسمت ۲: سازوکار-های مبتنی بر تجزیه اعداد صحیح	۱۳۹۲
INSO-ISO-IEC 27033-5	فناوری اطلاعات- فنون امنیتی- امنیت شبکه- قسمت ۵- ارتباطات امن ساز سرتاسر شبکه ها با استفاده از شبکه‌های خصوصی مجازی(VPNs)	۱۳۹۲
INSO-ISO-IEC 27037	فناوری اطلاعات- فنون امنیتی- راهنماهایی برای شناسایی، جمع‌آوری، اکتساب و حفاظت از شواهد رقمی (دیجیتال)	۱۳۹۳
INSO-ISO-IEC 27038	فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت ۴- امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی	۱۳۹۳
INSO-ISO-IEC 27039	فناوری اطلاعات- فنون امنیتی- انتخاب، استقرار و عملیات سامانه‌های آشکارسازی و پیش‌گیری نفوذ (IDPS)	۱۳۹۵
INSO-ISO-IEC 27042	فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تحلیل و تفسیر شواهد رقمی (دیجیتالی)	۱۳۹۵
INSO-ISO-IEC 9797-1	فناوری اطلاعات- فنون امنیتی- کدهای احراز هویت پیام (MAC قسمت ۱ – سازوکارهای استفاده از رمزگذاری بلوکی)	۱۳۹۰
INSO-ISO-IEC13888-1	فنون امنیتی فناوری اطلاعات- سلب انکار- قسمت ۱- کلیات	۱۳۹۰
INSO-ISO-IEC13888-2	فناوری اطلاعات فنون امنیتی- سلب انکار- قسمت ۲- سازوکارهای به‌کارگیری فنون متقارن	۱۳۹۰
INSO-ISO-IEC13888-3	فناوری اطلاعات فنون امنیتی- سلب انکار- قسمت ۳- سازوکارهای به‌کارگیری فنون نامتقارن	۱۳۹۰
۱۶۲۲۰	فناوری اطلاعات- مدل مرجع مدیریت داده	۱۳۹۱
۲-۱۶۲۷۴	سامانه‌های پردازش اطلاعات- اتصال متقابل سامانه‌های باز- مدل مرجع پایه- قسمت ۲- معماری امنیتی	۱۳۹۱
۱۶۲۷۵	فناوری اطلاعات- اتصال متقابل سامانه‌های باز- پروتکل امنیتی لایه شبکه	۱۳۹۱
۱-۱۶۳۰۰	فناوری اطلاعات- اتصال متقابل سامانه‌های باز- چارچوب‌های کاری امنیتی برای سامانه‌های باز- مرورکلی	۱۳۹۱
۷-۱۶۳۰۰	فناوری اطلاعات- اتصال متقابل سامانه‌های باز- چارچوب‌های کاری امنیتی برای سامانه‌های باز- چارچوب کاری ممیزی امنیت و هشدارها	۱۳۹۱
۱۶۳۰۲	فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها- پروتکل امنیت لایه انتقال	۱۳۹۱
۱۶۳۴۵	تنش‌پذیری سازمانی– سامانه‌های مدیریت امنیتـ آمادگی و استمرار- الزامات به همراه راهنمای استفاده	۱۳۹۱
۱۷۱۱۴	الزامات پروتکل درخواست صدور گواهی در زیر ساخت کلید عمومی ایران	۱۳۹۳

شماره استاندارد	موضوع	سال تصویب
۱۷۱۱۵	فناوری اطلاعات- الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی	۱۳۹۴
۱-۱۷۲۵۳	فناوری اطلاعات- فنون امنیتی- اصالت سنجی هستار ناشناس- قسمت ۱- عمومی	۱۳۹۲
۲-۱۷۲۵۳	فناوری اطلاعات- فنون امنیتی- اصالت سنجی هستار ناشناس- قسمت ۲- سازوکارهایی براساس امضاهایی که از یک کلید عمومی گروهی استفاده می‌کنند.	۱۳۹۳
۱۷۵۲۰	سری x شبکه‌های داده‌ها، امنیت و ارتباطات سامانه باز خدمات و کاربردهای ایمن -امنیت شبکه حسگر همه جاگاه - الزامات امنیتی برای مسیریابی شبکه حسگر بی سیم	۱۳۹۳
INSO-ISO-IEC 15408-1	فناوری اطلاعات- فنون امنیتی- معیارهای ارزیابی امنیت فناوری اطلاعات -قسمت ۱- معرف و مدل عمومی	۱۳۹۱
INSO-ISO-IEC 15408-2	فناوری اطلاعات- فنون امنیتی- معیارهای ارزیابی امنیت فناوری اطلاعات- قسمت ۲- مؤلفه‌های کارکردی امنیت	۱۳۹۱
INSO-ISO-IEC 15944-8	فناوری اطلاعات- دیدگاه عملکردی کسب و کار- قسمت۸- شناسایی الزامات حفاظت از حریم خصوصی به‌عنوان محدودیت‌های خارجی در تراکنش‌های کسب‌وکار	۱۳۹۲
INSO-ISO-IEC 23005-3	فناوری اطلاعات-کنترل و محتوی رسانه- قسمت ۳- اطلاعات حسی	۱۳۹۲
INSO-ISO-IEC 23005-4	فناوری اطلاعات -کنترل و محتوی رسانه- قسمت ۴- مشخصه‌های شی دنیای مجازی	۱۳۹۲
INSO-ISO-IEC 24767-2	فناوری اطلاعات- امنیت شبکه خانگی- قسمت ۲- خدمات امنیت داخلی- پروتکل ارتباطی امن برای میان افزار(SCPM)	۱۳۹۰
INSO-ISO-IEC -27000	فناوری اطلاعات- فنون امنیتی- سیستم‌های (سامانه‌های) مدیریت امنیت اطلاعات- مرور کلی و واژگان	۱۳۹۴
INSO-ISO-IEC 27007	فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزی سامانه‌های مدیریت امنیت اطلاعات	۱۳۹۱
INSO-ISO-IEC 27010	فناوری اطلاعات -فنون امنیتی- مدیریت امنیت اطلاعات برای ارتباطات درون بخشی و درون سازمانی	۱۳۹۲
INSO-ISO-IEC 27013	فناوری اطلاعات- فنون امنیتی- راهنمای پیاده‌سازی یکپارچه استانداردهای ISO-IEC27001,ISO-IEC20000-1	۱۳۹۳
INSO-ISO-IEC 27014	فناوری اطلاعات- فنون امنیتی- حاکمیت امنیت اطلاعات	۱۳۹۲
INSO-ISO-IEC 27033-3	فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت ۳- فرانامه‌های شبکه‌بندی مرجع- تهدیدها- فنون طراحی و مسائل کنترلی	۱۳۹۳
INSO-ISO-IEC 27033-4	فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت ۴- امن‌سازی ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی	۱۳۹۳
۴-۱۷۶۰۶	فناوری اطلاعات- پروتکل کنترل شبکه قسمت ۴- ارتباط IP	۱۳۹۱

شماره استاندارد	موضوع	سال تصویب
۱۷۶۰۷	فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها- اتصال متقابل سامانه‌های باز- سازوکار شناسایی پروتکل انتقال	۱۳۹۲
۱۷۶۴۱	فناوری اطلاعات- فنون امنیتی- تصدیق پروتکل‌های رمز نگاشتی	۱۳۹۱
۱-۱۷۶۴۲	فناوری اطلاعات- فنون امنیتی- چارچوب کاری برای مدیریت هویت- قسمت ۱- واژگان و مفاهیم	۱۳۹۲
۲-۱۷۶۴۲	فناوری اطلاعات- فنون امنیتی- چارچوبی برای مدیریت هویت- قسمت ۲- الزامات و معماری مرجع	۱۳۹۴
۱۷۶۴۳	فناوری اطلاعات- فنون امنیتی- چارچوب کاری حریم خصوصی	۱۳۹۲
۱۷۷۴۸	فناوری اطلاعات- فنون امنیتی- الزامات برای اصالت‌سنجی تا حدودی گمنام تا حدودی غیر پیوندپذیر	۱۳۹۳
۱۷۹۱۳	فناوری اطلاعات- فنون امنیتی- چارچوب تضمین اصالت سنجی هستار	۱۳۹۳
۲-۱۷۹۱۴	فناوری اطلاعات- فنون امنیتی- کدهای اصالت سنجی پیام (MACs) قسمت۲- سازوکارهای استفاده کننده از تابع در هم‌ساز اختصاصی	۱۳۹۳
۱-۱۸۴۷۷	فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک (قسمت ۱- پروتکل و خدمات امنیتی ارتباط میدان نزدیک امن (NFC-SEC) - پروتکل و واسط ارتباط میدان نزدیک (NFCIP-1)	۱۳۹۳
۲-۱۸۴۷۷	فناوری اطلاعات- مخابرات و تبادل اطلاعات بین سامانه‌ها- امنیت ارتباط میدان نزدیک- قسمت ۲- استاندارد رمزنگاری ارتباط میدان نزدیک امن (NFC-SEC) با به‌کارگیری منحنی‌های بیضوی دیفی- هلمن (ECDH) و استاندارد رمزبندی پیشرفته (AES)	۱۳۹۳
۱۸۷۱۹	فناوری اطلاعات- شناسایی و مدیریت اقلام سیار- پروتکل حفظ حریم مصرف‌کننده برای خدمات شناسایی بسامد رادیویی (RFID) سیار	۱۳۹۳
۱۸۷۲۱	فناوری اطلاعات- فنون امنیت- الزامات امنیت برای پودمان‌های رمزنگاری	۱۳۹۳
۱-۱۸۷۲۲	فناوری اطلاعات- فنون امنیتی- امضاهای رقمی (دیجیتالی) ناشناس- قسمت ۱-کلیات	۱۳۹۴
۲-۱۸۷۲۲	فناوری اطلاعات- فنون امنیت- امضاهای رقمی (دیجیتالی) ناشناس- قسمت ۲- سازوکارهایی با استفاده از یک کلید عمومی گروهی	۱۳۹۳
۱۸۹۱۴	فناوری اطلاعات- فنون امنیتی- مرزگذاری اصالت‌سنجی شده	۱۳۹۳
۱-۱۹۰۴۳	مهندسی نرم‌افزار و سامانه‌ها- آزمون نرم‌افزار- قسمت ۱- مفاهیم و تعاریف	۱۳۹۳
۲-۱۹۰۴۳	مهندسی نرم‌افزار و سامانه‌ها- آزمون نرم‌افزار- قسمت ۲- فرایندهای آزمون	۱۳۹۳

شماره استاندارد	موضوع	سال تصویب
۳-۱۹۰۴۳	مهندسی نرم‌افزار و سامانه‌ها- آزمون نرم‌افزار- قسمت ۳- مستندسازی آزمون	۱۳۹۴
۱۹۰۵۴	فناوری اطلاعات- فنون امنیتی- چارچوب کاری معماری حریم	۱۳۹۳
۱۹۰۵۵	فناوری اطلاعات- فنون امنیتی- افشای آسیب‌پذیری	۱۳۹۳
۴-۱۹۲۶۷	فناوری اطلاعات- فنون امنیتی- رمزنگاری سبک- قسمت ۴- سازوکارهای استفاده از فنون نامتقارن	۱۳۹۳
۱-۱۹۵۱۶	فناوری اطلاعات- امنیت شبکه خانگی قسمت ۱- الزامات امنیتی	۱۳۹۱
۲۱۰۷۸	فناوری اطلاعات- فنون امنیتی- فرایندهای ساماندهی آسیب‌پذیری	۱۳۹۵
۲۱۲۱۶	فناوری اطلاعات- فنون امنیتی- حفاظت اطلاعات زیست‌سنجشی	۱۳۹۵
۱-۵۲۳۳	تجهیزات فناوری اطلاعات- ایمنی قسمت اول- الزامات عمومی	۱۳۹۱
۲۱-۵۲۳۳	تجهیزات فناوری اطلاعات- ایمنی- قسمت ۲۱- تغذیه توان از دور	۱۳۹۳
۲۲-۵۲۳۳	تجهیزات فناوری اطلاعات- ایمنی- قسمت ۲۲- تجهیزاتی که در فضای باز نصب می‌شوند	۱۳۹۲
۲۳-۵۲۳۳	تجهیزات فناوری اطلاعات- ایمنی- قسمت ۲۳- تجهیزات در اندازه بزرگ برای ذخیره‌سازی داده‌ها	۱۳۹۲
۳-۹۵۹۸	فناوری اطلاعات- فنون امنیتی- توابع درهم‌ساز- قسمت ۳- توابع درهم‌ساز اختصاصی	۱۳۹۱
INO-ISO-IEC 27032	فناوری اطلاعات- فنون امنیتی-راهنماهایی برای امنیت فضای مجازی	۱۳۹۳
INSO - ISO-IEC 27041	فناوری اطلاعات- فنون امنیتی- راهنماهایی برای تضمین مناسب بودن و کفایت روش تحقیقات رخداد	۱۳۹۵
INSO ISO IEC 27036-2	فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط با تأمین‌کننده- قسمت ۲- الزامات	۱۳۹۵
INSO -ISO-IEC -27001	فناوری اطلاعات- فنون امنیتی- سامانه (سیستم) مدیریت امنیت اطلاعات- الزامات	۱۳۹۴
INSO-IEC-18045	فناوری اطلاعات- فنون امنیتی- روشگان برای ارزشیابی امنیت فناوری اطلاعات	۱۳۹۱
INSO-IEC 27005	فناوری اطلاعات- فنون امنیتی- مدیریت مخاطرات امنیت اطلاعات	۱۳۹۲

شماره استاندارد	موضوع	سال تصویب
INSO-IEC14888-3	فناوری اطلاعات- فنون امنیتی- امضاهای رقمی (دیجیتال) با پیوست قسمت ۳- سازوکارهای بر پایه لگاریتم گسسته	۱۳۹۱
INSO-IEC16206-7	فناوری اطلاعات– فنون امنیتی– مدیریت رخداد امنیت اطلاعات	۱۳۹۲
INSO-IEC-TR 27008	فناوری اطلاعات- فنون امنیتی- راهنماهایی برای ممیزان در کنترل‌های امنیت اطلاعات	۱۳۹۱
INSO-ISO-IEC - 27034-1	فناوری اطلاعات- فنون امنیتی- امنیت برنامه کاربردی- قسمت ۱- مرور کلی و مفاهیم	۱۳۹۴
INSO-ISO-IEC - 27036-3	فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده- قسمت ۳- راهنماهایی برای امنیت زنجیره تأمین فناوری اطلاعات و ارتباطات	۱۳۹۳
INSO-ISO-IEC14888-2	فناوری اطلاعات- فنون امنیتی- امضاهای رقمی (دیجیتالی) با پیوست قسمت ۲- سازوکارهای بر پایه عامل‌بندی صحیح	۱۳۹۰
INSO-ISO-IEC-27002	فناوری اطلاعات- فنون امنیتی- آیین کار برای کنترل‌های امنیت اطلاعات	۱۳۹۴
INSO-ISO-IEC-27033-2	فناوری اطلاعات- فنون امنیتی- امنیت شبکه قسمت ۲- راهنماهایی برای طراحی و پیاده‌سازی امنیت شبکه	۱۳۹۲
INSO-ISO-IEC27035	فناوری اطلاعات– فنون امنیتی– مدیریت رخداد امنیت اطلاعات	۱۳۹۲
INSO-ISO-IEC27036-1	فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط تأمین‌کننده- قسمت ۱- مرور کلی و مفاهیم	۱۳۹۳
INSO-ISO-IEC-29341-13-11	فناوری اطلاعات- معماری افزاره جامع اتصال اجرا UPnP -قسمت۱۳-۱۱ -پروتکل کنترل امنیت افزاره- خدمت کنسول امنیت	۱۳۹۱
INSO-ISO-IEC-TR 27015	فناوری اطلاعات- فنون امنیتی- راهنماهای مدیریت امنیت اطلاعات برای خدمات مالی	۱۳۹۲
INSO-ISO-IEC-TR 27016	فناوری اطلاعات- فنون امنیتی- مدیریت امنیت اطلاعات- اقتصادهای سازمانی	۱۳۹۳
INSO-ISO-IEC-TR-27019	فناوری اطلاعات- فنون امنیتی- راهنماهای مدیریت امنیت اطلاعات برای سامانه‌های کنترل فرایند خاص صنایع انرژی همگانی مبتنی بر استاندارد ISO-IEC 27002	۱۳۹۳
INSO-ISO-IEC-TR-27031	فناوری اطلاعات- فنون امنیتی- راهنماهایی برای آمادگی فناوری اطلاعات و ارتباطات به منظور تداوم کسب‌وکار	۱۳۹۱

جدول (۲): مقررات و قوانین

شماره	عنوان	سال تصویب
۴۸۸۵۰	سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)	۱۳۸۹
۶۶۷۳	قانون اصلاح قانون سازمان اطلاعات و امنیت کشور	۱۳۳۷
۶۸۴۷	قانون مربوط به تشکیل سازمان اطلاعات و امنیت کشور	۱۳۳۵
۳۹۷۶۷	تعیین سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور	۱۳۸۷
۶۳۳۵۱	نامه اصلاحی سند راهبردی برقراری امنیت در فضای تولید و تبادل اطلاعات کشور در محیط‌های رایانه‌ای	۱۳۸۴
۲۵۰۱۴	بخشنامه درخصوص برنامه عملیاتی امنیت فضای تبادل اطلاعات در دستگاه‌ها	۱۳۸۳
۲۴۷۱۵	بخشنامه به کلیه دستگاه‌های اجرایی در خصوص ارائه برنامه عملیاتی امنیت فضای تبادل اطلاعات حوزه‌های مرتبط با خود، هدایت برنامه‌های ایمن‌سازی فضای تبادل اطلاعات شرکت‌ها و مراکز خصوصی و استقرار نسخه اصلی اطلاعات دولتی در محیط و مراکز میزبان‌های داخلی و ...	۱۳۸۳

پیوست شماره ۲

سازمان‌ها و استانداردهای امنیتی بین المللی

معرفی سازمان‌های امنیتی

فناوری اطلاعات دارای یک نقش حیاتی و تعیین‌کننده در اکثر سازمان‌های مدرن اطلاعاتی است. امروزه زیرساخت فناوری اطلاعات سازمان‌ها در محیطی قرار گرفته‌اند که به‌طور فزاینده بر تعداد دشمنان و مهاجمانی که علاقه‌مند به حضور مستمر، مطمئن و سودمند سیستم‌های کامپیوتری نمی‌باشند، افزوده می‌گردد. حملات سیری کاملاً صعودی داشته و متاسفانه اغلب سازمان‌ها قادر به واکنش مناسب در مقابل تهدیدات امنیتی جدید در زمان مطلوب و قبل از سوءاستفاده از سیستم‌های کامپیوتری خود نمی‌باشند.

کاهش مدت زمان لازم به منظور برخورد با تهدیدات امنیتی و افزایش بهره‌وری، از جمله خواسته‌های مشترک سازمان‌ها و کاربران می‌باشد. به منظور برخورد مناسب و ساخت‌یافته با تهدیدات امنیتی، سازمان‌هایی در جهت تدوین استانداردهای امنیتی در حوزه‌های مختلف شکل گرفته‌اند که در ادامه برخی از این سازمان‌ها معرفی شده‌اند. لازم به ذکر است که برخی از سازمان‌ها استانداردهایی را در حوزه‌های مختلف منتشر کرده و برخی به‌طور خاص بر روی یک حوزه امنیتی تمرکز کرده‌اند.

- **بنیاد ملی استانداردها و تکنولوژی[1] (NIST)**

یک آزمایشگاه اندازه‌گیری استانداردها و یک سازمان غیرنظارتی است که زیر نظر وزارت بازرگانی ایالات متحده آمریکا فعالیت می‌کند. این مؤسسه در سال ۱۹۰۱ به عنوان اداره ملی استاندارد تأسیس شد. هدف کلی NIST ارتقاء صنعت در ایالت متحده از طریق ابزارها و اطلاعات مربوط به استانداردها به منظور رقابت مؤثرتر در بازارهای جهانی می‌باشد. استانداردهای NIST طیف گسترده‌ای از فناوری‌ها از جمله شبکه هوشمند برق، علوم نانو و ابزارهای نیمه هادی را استفاده می‌کنند.

- **سازمان بین المللی استاندارد[2] (ISO)**

یک سازمان غیر دولتی و بین‌المللی است که در ۲۴ فوریه سال ۱۹۴۷ تاسیس شده است، دبیرخانه مرکزی این سازمان، در شهر ژنو کشور سوئیس مستقر است. این سازمان متشکل از مؤسسه‌های ملی استانداردسازی

---

[1] National Institute of Standards and Technology
[2] International Organization for Standardization

۱۳۰ کشور بزرگ و کوچک و صنعتی و در حال توسعه از کلیه مناطق دنیا می‌باشد. وظیفه اصلی این سازمان توسعه استاندارد و فعالیت‌های مرتبط در جهان با نگرشی تسهیل‌کننده نسبت به تبادلات بین‌المللی کالاها و خدمات، بهبود همکاری در محدوده علمی، فنی، اطلاعاتی و فعالیت‌های اقتصادی و حمایت از تولیدکننده و مصرف‌کننده می‌باشد. سازمان بین‌المللی استاندارد تدوین استانداردهای فنی و اختیاری را بر عهده دارد. این استانداردها تقریباً تمامی حوزه‌های فناوری را پوشش می‌دهند و به ساخت و عرضه کالاها و خدمات مؤثرتر، ایمن‌تر و بهداشتی‌تر کمک می‌نماید. استانداردهای ISO تجارت و بازرگانی بین کشورها را آسان‌تر و صحیح‌تر می‌کند و به‌طورکلی از مصرف‌کنندگان کالاها و خدمات حمایت می‌کند. به عبارت دیگر اقدامات ISO که منجر به موافقت‌نامه‌های بین‌المللی گشته، نهایتاً به صورت استانداردهای بین‌المللی چاپ می‌شود.

- **اتحادیه بین‌المللی مخابرات[1] (ITU)**

یک سازمان بین‌المللی وابسته به سازمان ملل متحد است که محل اصلی آن در شهر ژنو کشور سوئیس می‌باشد. این سازمان بین‌المللی توصیه‌هایی برای شبکه‌های ارتباطی و مخابراتی و خدمات مبتنی‌بر این شبکه‌ها را در سطح جهانی ارائه می‌دهد و دارای اعضایی از ۱۹۳ کشور و بیش از ۷۰۰ نهاد بخش خصوصی و مؤسسات آموزشی می‌باشد.

نمونه‌هایی از استانداردهای تدوین شده توسط این سازمان عبارتند از:

- سری‌های E: اقدامات شبکه‌ای
- سری‌های H: سامانه‌های صوتی- تصویری و چند رسانه ای شامل H.323 و پروتکل VoIP
- سری‌های I: شبکه دیجیتالی خدمات یکپارچه (ISDN)
- سری‌های Q: استانداردهای سوئیچینگ و سیگنال‌دهی شامل SS7 ، سیگنال‌دهی ISDN PRI، خدمات پیشرفته تماس و غیره

[1] International Telecommunication Union

- سری‌های X: شبکه‌های داده، ارتباطات و امنیت شبکه‌های باز شامل X.25 ، پروتکل بسته‌ای برای شبکه‌های داده و غیره.

- **مؤسسه مهندسان برق و الکترونیک** (IEEE)

این مؤسسه از مؤسسات مهم استانداردسازی در دنیاست. استانداردسازی این مؤسسه طیف وسیعی از موضوعات را در بر می‌گیرد از جمله: مهندسی پزشکی، فناوری اطلاعات، مخابرات، حمل و نقل، فناوری نانو و غیره.

این مؤسسه حدود سی درصد از کل تألیفات جهان را در زمینه برق و کامپیوتر منتشر می‌کند و شمار ژورنال‌های آن به صد می‌رسد. همچنین بیش از ۴۰۰ هزار نفر عضو در ۱۶۰ کشور جهان دارد که ۴۵ درصد این اعضا خارج از ایالات متحده هستند.

- **OWASP** [1]

این مؤسسه، یک انجمن باز است که به‌طور اختصاصی سعی در ایجاد امنیت در تجارت، توسعه، برنامه‌های کاربردی و اهداف سازمان‌ها و ادارات دارد و در جهت برطرف نمودن آسیب‌پذیری‌های امنیتی متداول در تمامی قالب‌های کاری نرم افزار توسعه داده شده است. این انجمن قصد دارد تا با ایجاد امنیت در نرم‌افزارها و تجهیزات مورد استفاده بشر، با نزدیک کردن وسایل هوشمند و تجهیزات قابل برنامه‌ریزی به زندگی حالت مکانیکی بدهد.

- **نیروی کار مهندسی اینترنت** [2] (**IETF**)

گروه مهندسی اینترنت (IETF)، گروهی است که استانداردهای اینترنت را تدوین کرده و بهبود می‌بخشد. این گروه با کنسرسیوم وب جهانی موسوم به W3C [3] و سازمان بین‌المللی استانداردسازی موسوم به ISO/IEC

[1] Open Web Application Security Project
[2] Internet Engineering Task Force
[3] World Wide Web Consortium

همکاری نزدیکی داشته و به‌طور ویژه بر روی مجموعه پروتکل اینترنت کار می‌کند. این گروه یک مؤسسه استاندارد باز بوده که هیچ عضویت رسمی و یا شرایط عضویتی ندارد.

- **کنسرسیوم وب جهانی (W3C)**

سازمان بین‌المللی ایجاد و توسعه استانداردهای وب است که توسط برنرز لی[1] مخترع وب رهبری و در سال ۱۹۹۴ تأسیس شده است. به‌طورکلی هدف آن ایجاد استانداردهایی برای وب سایت‌ها است تا وب سایت‌ها در تمامی مرورگرهای سراسر دنیا سازگار باشند. وی مخترع تعدادی از اصلی‌ترین فناوری‌هایی است که وب به‌دست آن‌ها به شکل امروزی خود در آمده است. از جمله این فناوری‌ها می‌توان به URL[2] یا مشخص‌کننده یکتای منبع، قرارداد انتقال ابرمتن و HTML[3] اشاره کرد.

- **سازمان ترویج استانداردهای اطلاعات ساختاریافته[4] (OASIS)**

سازمان OASIS یک کنسرسیوم غیرانتفایی می‌باشد که توسعه و تصویب استانداردهای باز را برای جامعه اطلاعات جهانی فراهم می‌آورد. OASIS، استانداردهای بین‌المللی را برای امنیت، اینترنت اشیا، محاسبات ابری، داده‌های کلان، انرژی، فناوری‌های محتوا، مدیریت اضطراری و دیگر حوزه‌ها، ارتقا می‌دهد.

- **کمیسیون بین المللی الکتروتکنیک (IEC)[5]**

سازمان بین‌المللی الکتروتکنیک که در سال ۱۹۰۶ با همت دانشمندان، متخصصان و مجامع الکتروتکنیک کشورهای مختلف تاسیس شده است، وظیفه تدوین و انتشار استانداردهای بین‌المللی IEC در حوزه گسترده برق و الکترونیک و زمینه‌های مرتبط را بر عهده دارد. مقر این سازمان تا سال ۱۹۴۸ در شهر لندن بود که از آن سال به بعد به شهر ژنو در کشور سوئیس منتقل شد. با توجه به روند جهانی ایجاد هماهنگی در استانداردهای ملی کشورهای مختلف و پذیرش هرچه بیشتر استانداردهای بین‌المللی از جمله IEC به‌عنوان

[1] Timothy John Berners-Lee
[2] Uniform Resource Locator
[3] HyperText Markup Language
[4] Organization for the Advancement of Structured Information Standards
[5] International Electrotechnical Commission

پایه استانداردهای ملی و مبنای فعالیت‌های ارزیابی انطباق و گواهی محصولات برقی و الکترونیکی به‌منظور تسهیل تجارت بین‌المللی، درشرایط حاضر بیشترین تلاش کشورها، مصروف مشارکت فعال در مراحل تدوین استانداردهای بین المللی می‌شود. بدین لحاظ اکثر استانداردهای ملی کشورهای مختلف به‌طور فزاینده‌ای براساس و معادل با استانداردهای IEC می‌باشند.

- **کمیته‌های فرعی و گروه‌های کاری از مؤسسه استاندارد بین‌المللی آمریکا[1] (ANSI)**

مؤسسه استانداردهای ملی آمریکا اولین سازمان برای حمایت از توسعه استانداردهای فناوری در ایالت متحده می‌باشد. این مؤسسه با گروه‌های صنعتی کار کرده و عضو سازمان بین‌المللی استاندارد ایالت متحده و کمیسیون بین‌المللی الکتروتکنیک می‌باشد.

- **گروه باز[2]**

گروه باز یک کنسرسیوم صنعتی بی‌طرف فناوری و تولیدکننده با بیش از ۵۰۰ سازمان عضو می‌باشد. این سازمان در سال ۱۹۹۶ زمانی‌که X/Open با بنیاد نرم‌افزار باز ادغام شد، شکل گرفت. خدمات ارائه شده این سازمان شامل استراتژی، مدیریت، نوآوری، پژوهش، استانداردها، گواهی‌نامه‌ها و توسعه آزمون می‌باشد.

در ادامه به معرفی سازمان‌هایی که طور خاص برروی یک حوزه امنیتی تمرکز دارند، پرداخته می‌شود.

سازمان‌های ارائه‌دهنده استاندارد برای داده‌های کلان

داده‌های کلان به عنوان زمینه مورد علاقه برای طیف وسیعی از ذی‌نفعان چند جانبه سازمان‌های همکار از جمله کسانی که در روند قانونی استانداردها[3]، کنسروسیوم صنایع و سازمان‌های منبع باز مشغول هستند، ایجاد شده است. این سازمان‌ها متفاوت عمل کرده و بر جنبه‌های مختلفی تمرکز دارند اما تمامی آن‌ها سهمی در پیشبرد حوزه داده‌های کلان دارند. یکپارچه‌سازی طرح‌های اضافی داده‌های کلان همراه با تلاش‌های مشترک در حال انجام، کلید موفقیت این امر است. شناسایی طرح‌های مشترکی که رسیدگی به نیازمندی‌های

[1] American National Standards Institute
[2] Open Group
[3] Jure standards process

معماری را مورد توجه قرار می‌دهد و یا نیازمندی‌هایی که هنوز مورد بررسی قرار نگرفته‌اند، نقطه شروع تلاش‌های مشترک ذی‌نفعان چند جانبه در آینده می‌باشد.

برخی از سازمان‌های توسعه استاندارد پیشرو که بر روی استانداردهای مربوطه به داده‌های کلان کار می‌کنند، شامل موارد زیر می‌باشد:

- **گروه داده کاوی**[1] (DMG)

گروه داده‌کاوی، استانداردهای مربوط به داده‌کاوی را توسعه می‌دهد. این گروه، زبان نشانه‌گذاری مدل پیش‌بینی[2] (PMML)، که یک قالب مبتنی‌بر XML[3] به‌منظور ارائه برنامه کاربردی برای توصیف مدل‌های تولید شده توسط الگوریتم‌های یادگیری ماشین و داده کاوی می‌باشد را توسعه می‌دهد.

- TM Forum

انجمن TM در واقع یک انجمن مدیریت از راه دور[4] می‌باشد که یک انجمن عضو جهانی برای کسب و کار دیجیتالی می‌باشد. این انجمن یک کتاب راهنما برای تجزیه و تحلیل داده کلان که بهترین رویه را بر روی داده کلان توصیف می‌نماید، منتشر نمود.

سازمان‌های ارائه‌دهنده استاندارد برای محاسبات ابری

- **اتحادیه امنیت ابر**[5] **(CSA)**

CSA یک سازمان پیشرو در جهان می‌باشد که به تعریف و بالا بردن سطح آگاهی نسبت به بهترین رویه‌ها و به منظور کمک به حصول اطمینان نسبت به محیط محاسبات ابری امن، اختصاص داده شده است. سازمان CSA، انجمن‌ها، دولت‌ها، صنعتگران، شرکت‌ها و افراد را در زمینه پژوهش، آموزش، صدور گواهی‌نامه، رویدادها و محصولات خاص امنیت ابر، تحت کنترل در می‌آورد. فعالیت‌های سازمان CSA، مزایای عمده‌ای

[1] Data Mining Group
[2] Predictive Model Markup Language
[3] Extensible Markup Language
[4] Tele Management Forum
[5] Cloud Security Alliance

را برای ارائه‌دهندگان و مصرف‌کنندگان خدمات ابر و هم‌چنین برای دولت‌مردان، کارآفرینان[1] و صنعتگران فراهم می‌آورد. این سازمان هم‌چنین یک انجمنی را از طریق احزاب گوناگون فراهم می‌آورد تا بتواند برای ایجاد و حفظ اکوسیستم ابر قابل اعتماد[2]، با یکدیگر فعالیت داشته باشند.

- **SNIA**

مأموریت مؤسسه SNIA، کمک به رشد و مؤفقیت بازار در زمینه ذخیره‌سازی ابری می‌باشد. اهداف این سازمان به شرح زیر است:

- تبدیل شدن به قدرت به‌رسمیت شناخته‌شده در زمینه استانداردهای ذخیره‌سازی ابری
- آموزش جامعه کاربران و تولیدکنندگان به‌منظور ذخیره‌سازی ابری
- توسعه بازار به‌منظور برجسته کردن مزایای ذخیره‌سازی ابری
- همکاری با سایر انجمن‌های صنعتی در زمینه فنی ذخیره‌سازی ابری

- **سازمان DMTF[3]**

سازمان DMTF، استانداردهای قابل مدیریت بازی را در حوزه‌هایی مانند پردازش ابری، مجازی‌سازی، شبکه، سرویس‌دهنده و غیره منتشر می‌کند. شرکت‌های عضو این سازمان و شرکای ائتلاف بین‌المللی، استانداردها را به‌منظور بهبود مدیریت سازگار فناوری اطلاعات، توسعه می‌دهند. در واقع DMTF یک انجمن غیرانتفاعی است که از اعضای صنعتی خصوصی جهت ترویج مدیریت و قابلیت همکاری سامانه‌ها و سازمان‌ها تشکیل شده است و دارای کمیته‌های مختلفی است که هر یک بر روی زمینه خاصی تحقیق می‌کنند.

- کمیته فرعی JTC1، (SG 27)؛ در حال توسعه استانداردهایی برای حفاظت از اطلاعات و فناوری اطلاعات و ارتباطات است که شامل متدهای عمومی، فناوری‌ها و دستورالعمل‌هایی به‌منظور رسیدگی

[1] Entrepreneurs
[2] Trusted cloud ecosystem
[3] Distributed Management Task Force

به امنیت و حریم خصوصی می‌باشد. امنیت و حریم خصوصی یکی از جنبه‌های ICT می‌باشد که می‌تواند در زمینه داده‌های کلان نیز مورد استفاده قرار گیرد.

- در نوامبر سال ۲۰۱۴، کمیته فنی مشترک ISO/IEC (JTC 1)[1]، گروه کاری ۹[2] (WG 9) را در حوزه داده‌های کلان به منظور موارد زیر ایجاد نمود:
  - ارائه خدماتی که محوریت آن بر مبنای استانداردسازی داده‌های کلان می‌باشد.
  - توسعه استانداردهای بنیادی برای داده‌های کلان– از جمله معماری مرجع و استانداردهایی برای واژگان و فرهنگ لغت- به منظور توسعه تلاش های کمیته JTC1 که بر اساس آن، استانداردهای دیگر داده کلان می‌تواند توسعه یابد.
  - شناسایی نهادهای JTC1 و دیگر سازمان‌ها که در حال توسعه استانداردها و مفاهیم مرتبط با داده‌های کلان هستند.
  - تعامل با جامعه خارج از JTC1 به منظور تشویق آن جوامع برای همکاری با JTC1 که در زمینه استانداردگذاری داده‌های کلان تلاش کنند.
- کمیته SC 38، یک کمیته فرعی استانداردسازی می‌باشد که بخشی از کمیته فنی مشترک ISO/IEC JTC 1 از سازمان بین‌المللی ISO و کمیسیون بین‌المللی IEC را تشکیل می‌دهد. کمیته ISO/IEC JTC 1/SC 38 در نشست عمومی ISO/IEC JTC 1 در اکتبر سال ۲۰۰۹، تشکیل شد. دبیرخانه بین‌المللی ISO/IEC JTC 1/SC 38، مؤسسه استاندارد بین‌المللی آمریکا[3] (ANSI) واقع در ایالات متحده می باشد. حوزه فعالیت ISO/IEC JTC 1/SC 38 در زمینه بسترهای توزیع‌شده و محاسبات ابری است.

سازمان‌های ارائه‌دهنده استاندارد برای سامانه‌های کنترل صنعتی

[1] Joint technical committee 1
[2] Working group 9
[3] American National Standards Institute

- **انجمن بین المللی اتوماسیون[1] (ISA)**

انجمن بین‌المللی اتوما سیون (ISA)، که قبلاً به عنوان جامعه ابزار دقیق، سیستم‌ها و اتوما سیون شناخته می‌شد، یک جامعه فنی غیرانتفاعی برای مهندسین، تکنسین‌ها، تجار، اساتید و دانش‌پژوهان است که در حال کار، مطالعه و یا علاقه‌مند به امور و حرفه اتوماسیون صنعتی، مانند ابزار دقیق هستند. ISA رسماً به‌عنوان انجمن ابزار امریکا در تاریخ ۲۸ آوریل سال ۱۹۴۵، در پیتسبورگ، پنسیلوانیا تأسیس شد که معمولاً با نام مخفف آن، ISA شناخته می‌شود و شامل بسیاری از رشته‌های فنی و مهندسی است. ISA یکی از سازمان‌های حرفه‌ای در جهان برای تعیین استانداردها و آموزش متخصصان صنعت در اتوماسیون می‌باشد.

- **شرکت NERC[2]**

NERC یک شرکت غیرانتفاعی مستقر در آتلانتا، جورجیاست که در تاریخ ۲۸ مارس سال ۲۰۰۶، به‌عنوان جانشین شورای قابلیت اطمینان الکتریک آمریکای شمالی شکل گرفت. NERC اصلی در تاریخ یک ژوئن سال ۱۹۶۸ به‌وسیله صنعت تجهیزات الکتریکی برای پیشرفت اعتبار صنعت انتقال قدرت در سیستم‌های برق آمریکای شمالی شکل گرفت. ماموریت NERC حصول اطمینان از قابلیت اطمینان سیستم قدرت آمریکای شمالی می‌باشد.

سازمان های ارائه‌دهنده استاندارد برای حوزه سلامت

- **مؤسسه استاندارد آزمایشگاهی و کلینیکی (CLSI)**

در سال ۱۹۶۸، سی و یک پزشک و دانشمند به نمایندگی از پانزده سازمان برای بهبود وضعیت رسیدگی به بیماران و توسعه یک فرآیند استانداردسازی گرد هم جمع شدند و در سال ۱۹۷۷، CLSI توسط مؤسسه ملی استاندارد آمریکا (ANSI) به رسمیت شناخته شد. CLSI یک مؤسسه است که بدون منفعت و به‌صورت داوطلبانه به ترویج استاندارد مورد استفاده در آزمایشگاه‌ها و راهنماهایی برای

[1] The International Society of Automation
[2] North American Electric Reliability Corporation

سازمان‌های مراقبت پزشکی می‌پردازد. مأموریت این سازمان توسعه شیوه‌های کلینیکی و آزمایشگاهی و ترویج استفاده از آن‌ها در سراسر جهان می‌باشد.

- **انجمن پیشرفت ابزار دقیق پزشکی (AAMI)**

یک سازمان برای توسعه و استفاده ایمن و مؤثر از فناوری‌های پزشکی است که در سال ۱۹۶۵ توسط رابرت دی هال[1] و رابرت جی آلن[2] تاسیس شد. AAMI برای تنظیم مجموعه‌ای از استانداردهای ایمنی برای دستگاه‌های پزشکی در مرحله طراحی و استفاده از آن‌ها فعالیت می‌کند.

سازمان‌های ارائه‌دهنده استاندارد برای اینترنت اشیا

- **OneM2M**

یک سازمان جهانی است که الزامات، معماری، مشخصات API، راه‌حل‌های امنیتی و فناوری‌های اینترنت اشیا و قابلیت همکاری برای نقاط انتهایی را فراهم می‌کند.

این سازمان چارچوبی را برای پشتیبانی طیف گسترده‌ای از برنامه‌های کاربردی و سرویس‌ها از قبیل شهر هوشمند، شبکه هوشمند، امنیت عمومی و سلامت و غیره را فراهم می‌کند.

- **IERC**

سازمان IERC یک مرکز تحقیقات اختصاصی برای اینترنت اشیا است که هدف آن طراحی و اجرای پروژه‌های متعدد در زمینه رفع چالش‌های پیش روی توسعه فناوری اینترنت اشیا در سطح جهان و در نهایت ارائه یک تعریف و دیدگاه ثابت برای این فناوری است که کاملاً مطابق با استانداردهای اروپا باشد. از جمله اهداف اصلی این مرکز می‌توان به موارد ذیل اشاره نمود:

  - ایجاد یک چارچوب همکاری و چشم‌انداز پژوهش برای فعالیت اینترنت اشیا در اروپا و تبدیل شدن به یک دروازه بزرگ ورود اطلاعات و تحقیقات در زمینه این فناوری.

[1] Robert D. Hall
[2] Robert J. Allen

- تعریف یک استراتژی بین‌المللی برای همکاری در حوزه اینترنت اشیا و ایجاد نوآوری در زمینه‌های گوناگون مرتبط با این فناوری و مشاهده و کنترل روی انواع نوآوری‌هایی که در سطح جهانی صورت می‌گیرد.
- هماهنگ نمودن نوآوری‌های انجام شده در حوزه اینترنت اشیا با پروژه‌های متفاوت در فناوری اطلاعات و ارتباطات
- ایجاد و سازماندهی بحث، گفت‌وگو و کارگاه‌های آموزشی که منجر به درک بهتری از فناوری اینترنت اشیا و فناوری‌هایی همچون 5G و فناوری ابر می‌شود.

- **اینترنت اشیای منبع باز OSIOT :**

یک سازمان با هدف توسعه و ترویج استانداردهای منبع باز و آزاد برای ظهور اینترنت اشیا می‌باشد.

استانداردهای امنیتی

در این قسمت لیست کلی استانداردهای امنیتی حوزه‌های مختلف (شبکه، نرم‌افزار، موبایل، اینترنت اشیا و غیره) مشخص شده است. لیست کلی استانداردهای امنیتی در جدول شماره (۱) مشخص شده است:

جدول (۱): لیست استانداردهای امنیتی

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-64	Security Considerations in the System Development Life Cycle, Rev.2 (2008) ملاحظات امنیتی در چرخه حیات توسعه سامانه	NIST	پیاده‌سازی امنیت در چرخه حیات توسعه سامانه‌ها
SP 800-51	Guide to Using Vulnerability Naming Schemes, Rev.1 (2011) راهنمایی برای استفاده از طرح‌های نام‌گذاری آسیب‌پذیری	NIST	ارائه راهنمایی‌هایی در نحوه استفاده از نام‌گذاری آسیب‌پذیری و طرح‌های نام‌گذاری در ارائه محصولات و خدمات
SP 800-61	Computer Security Incident Handling Guide, Rev. 2 (2012) راهنمای رسیدگی به حوادث امنیتی کامپیوتری	NIST	کمک به سازمان‌ها در کاهش خطرات ناشی از حوادث کامپیوتری با ارائه راهنمایی‌هایی در پاسخ به حوادث مؤثر و کارآمد، تشخیص، تحلیل، اولویت‌بندی و کنترل حوادث
SP 800-36	Guide to Selecting Information Technology Security Products (2003) راهنمای انتخاب محصولات امنیتی فناوری اطلاعات	NIST	ارائه لیستی از محصولات امنیتی فناوری اطلاعات و معیارهای انتخاب محصول
SP 800-35	Guide to Information Technology Security Services (2003) راهنمای سرویس‌های امنیتی فناوری اطلاعات	NIST	کمک به سازمان‌ها در انتخاب، اجرا و مدیریت سرویس‌های فناوری اطلاعات در مراحل مختلف چرخه حیات سرویس‌های امنیتی فناوری اطلاعات
SP 800-56a	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, (2013) توصیه‌ای برای طرح‌های تولید جفت کلید با استفاده از رمزنگاری لگاریتم گسسته	NIST	ارائه مشخصاتی جهت ایجاد جفت کلید با استفاده از لگاریتم گسسته

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-57	Recommendation for Key Management Part 1: General, (2016) Part 2: Best Practices for Key Management Organization, (2005) Part 3: Application-Specific Key Management Guidance, (2015) توصیه‌ای برای مدیریت کلید بخش ۱: کلیات بخش ۲: بهترین روش برای سازمان مدیریت کلید بخش ۳: راهنمایی‌هایی جهت مدیریت کلید خاص حوزه نرم‌افزار	NIST	ارائه چارچوب‌هایی برای انتخاب و استفاده از مکانیزم-های رمزنگاری و مسائل مربوط به مدیریت کلید
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems (1996) روش‌ها و اصول پذیرفته‌شده عمومی برای امنیت سامانه‌های فناوری اطلاعات	NIST	ارائه درکی از نیازمندی‌های پایه‌ای امنیتی و اصول پایه امنیت سامانه‌های کامپیوتری
SP 800-70	National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, Rev.3 (2016) برنامه چک لیست ملی برای محصولات فناوری اطلاعات: راهنمایی برای چک لیست کاربران و توسعه‌دهندگان	NIST	ارائه راهنمایی‌هایی جهت انتخاب چک لیست از مخزن چک لیست ملی برای کاربران و تنظیم سیاست‌ها و روش‌ها و نیازمندی‌های عمومی برای شرکت در برنامه چک لیست امنیتی برای توسعه‌دهندگان
SP 800-68	Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist, Rev.1 (2008) راهنمای امنیت سامانه‌های مایکروسافت ویندوز XP برای متخصصان فناوری اطلاعات	NIST	ارائه راهنمایی‌هایی جهت تنظیمات امن برای سامانه-های مایکروسافت ویندوز XP
SP 800-58	Security Considerations for Voice Over IP Systems (2005) ملاحظات امنیتی برای سامانه‌های VOIP	NIST	ارائه راهنمایی‌هایی برای ایجاد شبکه‌های VOIP امن و فناوری VOIP
SP 800-48	Guide to Securing Legacy IEEE 802.11 Wireless Networks, Rev.1 (2008) راهنمایی برای تأمین امنیت شبکه‌های بی‌سیم IEEE 802.11	NIST	ارائه راهنمایی برای سازمان‌ها جهت امنیت شبکه‌های WLAN خود براساس استاندارد IEEE 802.11 به دلیل عدم توانایی استفاده از استاندارد IEEE 802.11i
SP 800-47	Security Guide for Interconnecting Information Technology Systems (2002) راهنمای امنیت برای ارتباطات سیستم‌های فناوری اطلاعات	NIST	ارائه راهنمایی برای توسعه یک برنامه جهت پیاده‌سازی ارتباطات سیستمی و تعریف فرآیند ایجاد ارتباطات

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-46	Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, Rev.2 (2016) راهنمایی برای امنیت دورکاری سازمان‌ها، دسترسی از راه دور و دورکاری دستگاه‌های سرویس‌گیرنده	NIST	کاهش ریسک‌های مرتبط با فناوری‌های سازمانی مورد استفاده در دورکاری مانند دسترسی از راه دور سرویس‌دهنده‌ها، دورکاری دستگاه‌های سرویس‌گیرنده و ارتباطات راه دور
SP 800-45	Guidelines on Electronic Mail Security, V.2 (2007) راهنمایی در مورد امنیت پست الکترونیک	NIST	ارائه توصیه‌هایی برای اقدامات امنیتی در طراحی، پیاده‌سازی سیستم‌های ایمیل در شبکه‌های عمومی و خصوصی
SP 800-44	Guidelines on Securing Public Web Servers, V.2 (2007) راهنمایی در مورد امنیت سرویس‌دهنده‌های وب عمومی	NIST	ارائه توصیه‌هایی در مورد اقدامات امنیتی برای طراحی و پیاده‌سازی سرویس‌دهنده‌های وب در دسترس عموم، از جمله مسائل مربوط به زیرساخت-های شبکه
SP 800-41	Guidelines on Firewalls and Firewall Policy (2009) راهنمایی‌هایی در مورد دیواره آتش و سیاست‌های آن	NIST	کمک به سازمان‌ها در درک قابلیت‌های فناوری‌ها و سیاست‌های دیواره آتش، توسعه سیاست‌های دیواره‌های آتش و نیز انتخاب، پیکربندی، آزمون، استقرار و مدیریت دیواره‌های آتش
SP 800-40	Guide to Enterprise Patch Management Technologies Rev.3 (2013) راهنمایی برای فناوری‌های مدیریت وصله سازمان	NIST	ارائه راهنمایی‌هایی جهت کمک به سازمان در درک اصول اولیه فناوری‌های مدیریت وصله سازمان و بررسی چالش‌های ذاتی در انجام مدیریت وصله
SP 800-33	Underlying Technical Models for Information Technology Security (2001) مدل فنی بنیادی برای امنیت فناوری اطلاعات	NIST	ارائه یک مدل در طراحی و توسعه قابلیت‌های امنیتی فنی
SP 800-31	Intrusion Detection systems سیستم‌های تشخیص نفوذ	NIST	درک اهداف امنیتی روش‌های تشخیص نفوذ جهت انتخاب و پیکربندی سیستم‌های تشخیص نفوذ برای سیستم‌ها و شبکه‌های خاص
SP 800-28	Guidelines on Active Content and Mobile Code, V.2 (2008) راهنما در مورد محتوای فعال و کد موبایل	NIST	ارائه یک دید کلی تکنولوژی‌های محتوای فعال و کد موبایل و درکی برای تصمیم‌گیری‌های امنیت فناوری اطلاعات آگاهانه در برنامه‌های خود
SP 800-55	Performance Measurement Guide for Information Security, Rev.1 (2008) راهنمای سنجش عملکرد برای امنیت اطلاعات	NIST	مشخص نمودن نحوه استفاده از معیارها در سرمایه-گذاری امنیت اطلاعات، شناسایی کنترل‌های امنیتی، سیاست‌ها و رویه‌ها
SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, Rev.1 (2014) راهنمایی برای امنیت گواهی و مجوز رسمی از سیستم اطلاعات فدرال	NIST	

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-53A	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Rev. 4 (2014) راهنمایی برای ارزیابی کنترل‌های امنیتی و حریم خصوصی در سازمان‌ها و سیستم‌های اطلاعات فدرال: ایجاد طرح‌های ارزیابی مؤثر	NIST	ارائه راهنمایی‌هایی برای ایجاد طرح‌های ارزیابی امنیتی مؤثر و مجموعه جامعی از روش‌ها برای اثر بخشی کنترل‌های امنیتی به کار گرفته شده در سیستم‌های اطلاعاتی
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Rev.1 (2012) توصیه‌ای برای الگوریتم رمزگذاری داده سه‌گانه (TDEA) رمز قطعه‌ای	NIST	تعریف مراحل رمزنگاری موردنیاز به منظور حفاظت از اطلاعات با استفاده از الگوریتم رمزگذاری داده سه‌گانه
SP 800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques (2001) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: روش‌ها و تکنیک‌ها	NIST	ارائه راهنمایی مرتبط با مد عملیاتی با استفاده از الگوریتم رمزنگاری قطعه‌ای کلید متقارن
SP 800-38B	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication (2016) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: مد CMAC برای احرازهویت	NIST	ارائه الگوریتم کد تصدیق پیام (MAC) مبتنی بر رمزنگاری قطعه‌ای کلید متقارن
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality (2007) توصیه‌ای برای مدهای عملیاتی رمز قطعه‌ای: مد CCM برای احرازهویت و محرمانگی	NIST	ارائه مد عملیاتی CCM برای الگوریتم رمزنگاری قطعه‌ای کلید متقارن و اطمینان از محرمانگی و صحت داده‌های کامپیوتر
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Rev 1a (2010) یک مجموعه آزمون آماری برای مولد اعداد تصادفی و شبه تصادفی برای برنامه‌های کاربردی رمزنگاری	NIST	ارائه معیارهایی جهت انتخاب و آزمون مولد عدد تصادفی و شبه تصادفی
SP 800-21	Guideline for Implementing Cryptography in the Federal Government راهنمایی برای پیاده‌سازی رمزنگاری در دولت فدرال	NIST	ارائه راهنمایی‌هایی به سازمان جهت انتخاب کنترل‌های رمزنگاری را برای محافظت از داده‌های حساس طبقه بندی نشده
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures (2012) سیستم اعتبارسنجی مد عملیاتی برای الگوریتم رمزنگاری داده سه‌گانه (TMOVS): الزامات و روش‌ها	NIST	طراحی اولیه و پیکربندی TMOVS و بررسی الگوریتم رمزنگاری داده سه گانه

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-12	An Introduction to Computer Security, Rev.1 (2017) مقدمه‌ای بر امنیت کامپیوتر	NIST	ارائه راهنمایی‌هایی در رابطه با امنیت کامپیوتر از جمله امنیت سخت‌افزار، نرم‌افزار و منابع اطلاعاتی، مفاهیم مرتبط با امنیت کامپیوتر، ملاحظات هزینه و روابط بین کنترل‌های امنیتی
SP 800-34	Contingency Planning Guide for Federal Information Systems, Rev.1 (2010) راهنمای برنامه‌ریزی وقوع حادثه احتمالی سیستم‌های اطلاعاتی فدرال	NIST	ارائه اطلاعاتی در روابط متقابل بین برنامه‌ریزی وقوع حادثه احتمالی سیستم اطلاعات و انواع دیگر از امنیت و مدیریت اضطراری مربوط به برنامه‌های وقوع حادثه احتمالی، انعطاف‌پذیری سازمانی، و چرخه حیات توسعه سیستم
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, Rev. A (2004) اصول مهندسی برای امنیت فناوری اطلاعات	NIST	ارائه لیستی از اصول امنیتی در سطح سیستم در طراحی، توسعه و بهره‌برداری از یک سیستم اطلاعاتی
SP 800-65	Integrating IT Security into the Capital Planning and Investment Control Process, 2005 یکپارچه‌سازی امنیت فناوری اطلاعات در فرایند برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری	NIST	کمک به سازمان فدرال جهت یکپارچه‌سازی امنیت فرایندهای برنامه‌ریزی سرمایه و کنترل سرمایه‌گذاری جهت کمک به مدیریت و سنجش سرمایه‌گذاری‌های امنیتی
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories, 2008 راهنمایی برای نگاشت انواع اطلاعات و سیستم‌های اطلاعاتی به دسته‌های امنیت	NIST	کمک به سازمان‌ها به منظور نگاشت سطوح تأثیر امنیت به انواع اطلاعات و سیستم‌های اطلاعاتی
SP 800-59	Guideline for Identifying an Information System as a National Security System, 2003 راهنمایی برای شناسایی یک سیستم اطلاعاتی به عنوان یک سیستم امنیت ملی	NIST	ارائه راهنمایی‌های توسعه یافته در رابطه با وزارت دفاع، از جمله سازمان امنیت ملی، برای شناسایی یک سیستم اطلاعاتی به عنوان سیستم امنیت ملی
SP 800-23	Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000 راهنمایی‌هایی برای سازمان‌های فدرال جهت تضمین امنیت و کسب یا استفاده از محصولات بررسی یا ارزیابی شده	NIST	ارائه دستورالعمل‌هایی برای سازمان‌های فدرال جهت دستیابی و استفاده از محصولات امنیتی فناوری اطلاعات
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 2008 معرفی منابع مقدماتی جهت پیاده‌سازی قوانین امنیتی قانون پاسخگویی و انتقال بیمه بهداشت و درمان	NIST	ارائه یک دید کلی از استانداردهای امنیتی موجود در قانون امنیتی HIPAA

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-30	Risk Management Guide for Information Technology Systems راهنمای مدیریت ریسک برای سیستم‌های فناوری اطلاعات	NIST	کمک به سازمان‌ها برای مدیریت بهتر ریسک مربوط به فناوری اطلاعات و همچنین توانایی یکپارچه‌سازی چرخه حیات توسعه سیستم
SP 800-53	Recommended Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4 (2013) کنترل‌های امنیتی و حریم خصوصی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال	NIST	ارائه کاتالوگی از کنترل‌های امنیتی و حفظ حریم خصوصی برای سیستم‌های اطلاعات فدرال و سازمان‌ها
SP 800-18	Guide for Developing Security Plans for Federal Information Systems, 2006 راهنمایی برای توسعه برنامه‌های امنیتی برای سیستم‌های اطلاعاتی فدرال	NIST	هدف از طرح‌ریزی امنیت اطلاعات، بهبود حفاظت از منابع سیستم اطلاعات است.
SP 800-50	Building an Information Technology Security Awareness and Training Program, 2003 ایجاد یک برنامه آموزشی و آگاهی از امنیت فناوری اطلاعات	NIST	ایجاد یک برنامه آموزشی و آگاهی از امنیت فناوری اطلاعات
SP 800-16	A Role-Based Model for Federal Information Technology/Cybersecurity Training, Rev. 1, 2014 یک مدل مبتنی بر نقش برای آموزش امنیت سایبری/ فناوری اطلاعات فدرال	NIST	ارائه چارچوب جدیدی جهت آموزش امنیت فناوری اطلاعات
SP 800-100	Information Security Handbook: A Guide for Managers کتاب امنیت اطلاعات: راهنمایی برای مدیران	NIST	آشنایی مدیران با طیف گسترده‌ای از عناصر برنامه‌ی امنیت از جمله:مدیریت ریسک، برنامه‌ریزی امنیتی، طرح‌های احتمالی فناوری اطلاعات و غیره
SP 800-81	Secure Domain Name System (DNS) Deployment Guide, Rev 2, (2013) راهنمای استقرار امن سیستم نام دامنه	NIST	ارائه راهنمایی برای سازمان‌ها در درک توسعه امن سرویس‌های DNS
SP 800-92	Guide to Computer Security Log Management, (2006) راهنمایی برای مدیریت وقایع امنیتی کامپیوتر	NIST	ارائه یک راهنمای کاربردی برای توسعه، پیاده‌سازی و حفاظت مؤثر از روش‌های مدیریت وقایع در سراسر یک سازمان

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 800-94	Guide to Intrusion Detection and Prevention Systems (IDPS), Rev 1, (2012) راهنمایی برای سیستم‌های تشخیص و پیشگیری از نفوذ	NIST	کمک به سازمان‌ها در فهم فناوری‌های سیستم پیشگیری از نفوذ[1] و سیستم تشخیص نفوذ[2] و همچنین طراحی، پیاده‌سازی، پیکربندی، امن‌سازی، پایش و حفاظت این سیستم‌ها
SP 800-95	Guide to Secure Web Services, (2007) راهنمایی برای امنیت سرویس‌های وب	NIST	کمک به سازمان‌ها در درک چالش‌های یکپارچه‌سازی روش‌های امنیت اطلاعات در طراحی معماری سرویس‌گرا و توسعه براساس سرویس‌های وب
SP 800-97	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, (2007) ایجاد شبکه‌های امنیتی مستحکم بی‌سیم: راهنمایی برای IEEE 802.11i	NIST	ارائه راهنمایی درباره ویژگی‌های امنیتی و قابلیت های مرتبط با IEEE 802.11i از طریق چارچوب آن برای توسعه شبکه‌های امن مستحکم
SP 800-113	Guide to SSL VPNs, (2008) راهنمایی برای شبکه خصوصی مجازی مبتنی بر لایه سوکت امن	NIST	کمک به سازمان‌ها در فهم فناوری‌های SSL VPN و طراحی، پیاده‌سازی، پیکربندی، امن‌سازی، پایش و نگهداری راه‌حل‌های این فناوری‌ها
SP 800-119	Guidelines for the Secure Deployment of IPv6, (2010) راهنمایی برای توسعه امن IPv6	NIST	راهنمایی برای پروتکل IPv6، مشخصات و بیان ملاحظات امنیتی مرتبط با آن
SP 800-120	Recommendation for EAP Methods Used in Wireless Network Access Authentication, (2009) توصیه‌هایی برای روش‌های پروتکل احراز هویت توسعه‌پذیر به‌کار رفته در احرازهویت دسترسی به شبکه بی‌سیم	NIST	ارائه نیازمندی‌های امنیتی اصلی برای متدهای پروتکل احراز هویت توسعه‌پذیر[3] برای احراز هویت دسترسی بی‌سیم و ایجاد کلید
SP 800-123	Guide to General Server Security, (2008) راهنمایی برای امنیت سرویس‌دهنده عمومی	NIST	بررسی ضرورت نیاز به امن‌سازی سرویس‌دهنده‌ها و ارائه توصیه‌هایی برای انتخاب، پیاده‌سازی و حفظ کنترل‌های امنیتی لازم
SP 800-125B	Secure Virtual Network Configuration for Virtual Machine (VM) Protection, (2016)	NIST	تحلیل مزایا و معایب چهار حوزه پیکربندی شبکه مجازی از جمله بخش‌بندی شبکه، افزونگی مسیر

[1] intrusion prevention system
[2] intrusion detection system
[3] Extensible Authentication Protocol

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
	پیکربندی امن شبکه مجازی جهت حفاظت ماشین مجازی		شبکه[1]، کنترل ترافیک با استفاده از دیواره آتش و پایش ترافیک ماشین مجازی از نقطه نظر امنیتی و ارائه توصیه‌هایی برای سازمان‌ها جهت استفاده از تنظیمات پیکربندی
SP 800-127	Guide to Securing WiMAX Wireless Communications, (2010) راهنمایی برای امن‌سازی ارتباطات بی‌سیم WiMAX	NIST	فراهم نمودن اطلاعاتی برای سازمان‌ها در خصوص قابلیت‌های امنیتی ارتباطات بی‌سیم با استفاده از شبکه‌های وایمکس و فراهم نمودن توصیه‌هایی برای استفاده از این قابلیت‌ها
SP 800-128	Guide for Security-Focused Configuration Management of Information Systems, (2011) راهنمایی برای مدیریت پیکربندی متمرکز بر امنیت سیستم‌های اطلاعاتی	NIST	ارائه راهنمایی برای پیاده‌سازی خانواده مدیریت پیکربندی کنترل‌های امنیتی تعریف شده در استاندارد NIST SP 800-53
SP 800-150	Guide to Cyber Threat Information Sharing, (2016) راهنمایی برای به اشتراک‌گذاری اطلاعات تهدید سایبری	NIST	راهنمایی برای به اشتراک‌گذاری اطلاعات تهدید سایبری داخل یک سازمان، استفاده از اطلاعات تهدید سایبری دریافت شده از منابع خارجی و تولید اطلاعات تهدید سایبری که می‌تواند با سایر سازمان‌ها به اشتراک گذاشته شود
SP 800-153	Guidelines for Securing Wireless Local Area Networks (WLANs), 2012)(راهنمایی برای امن‌سازی شبکه‌های محلی بی‌سیم	NIST	ارائه توصیه‌هایی برای بهبود پیکربندی امنیتی و پایش شبکه‌های محلی بی‌سیم و تجهیزات متصل به این شبکه‌ها
SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Rev 1, (2016) حفاظت از اطلاعات غیرمحرمانه کنترل شده در سازمان‌ها و سیستم‌های غیر فدرال	NIST	ارائه موسسات فدرال با نیازمندی‌های توصیه شده برای حفاظت از محرمانگی اطلاعات طبقه‌بندی نشده کنترل شده
SP 800-175A	Guideline for Using Cryptographic Standards in the Federal Government: Directives, Mandates and Policies, (2016)	NIST	ارائه راهنمایی‌هایی جهت استفاده از رمزنگاری و استانداردهای رمزنگاری NIST توسط دولت فدرال برای حفاظت از اطلاعات حساس دیجیتالی و

[1] Network Path Redundancy

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
	راهنمایی برای استفاده از استانداردهای رمزنگاری در دولت فدرال: دستورالعمل‌ها، تعهدات و سیاست‌ها		طبقه‌بندی نشده در هنگام انتقال و در حین ذخیره‌سازی، شناسایی الزامات مورد نیاز برای رمزنگاری و خلاصه‌ای از قوانین و مقررات مربوط به حفاظت از اطلاعات حساس دولت فدرال
SP 800-175B	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, (2016) راهنمایی برای استفاده از استانداردهای رمزنگاری در دولت فدرال: مکانیسم‌های رمزنگاری	NIST	ارائه راهنمایی درباره متدها و سرویس‌های موجود رمزنگاری برای حفاظت از اطلاعات حساس دولت فدرال و مروری از استانداردهای رمزنگاری NIST
SP 800-184	Guide for Cybersecurity Event Recovery, (2016) راهنمایی برای بازیابی رویداد امنیت سایبری	NIST	کمک به سازمان‌ها به شیوه‌ای مستقل از تکنولوژی در بهبود برنامه بازیابی وقایع سایبری، فرآیندها و رویه‌های آن‌ها با هدف بازگشت سریع‌تر عملیات نرمال خود
SP 800-82	Guide to Industrial Control Systems (ICS) Security, Rev 2 (2015) راهنمایی برای امنیت سیستم‌های کنترل صنعتی	NIST	ارائه روش‌ها و کنترل‌های امنیتی برای امنیت تمام سیستم کنترل صنعتی
SP 500-291	NIST Cloud Computing Standards Roadmap, (2013) نقشه راه استانداردهای محاسبات ابری مؤسسه NIST	NIST	ارائه استانداردهای موجود در زمینه محاسبات ابری
SP 500-292	NIST Cloud Computing Reference Architecture, (2011) معماری مرجع محاسبات ابری NIST	NIST	فراهم آوردن معماری مرجع محاسبات ابری به‌منظور ارائه خدمات و فناوری محاسبات ابری
SP 500-293	US Government Cloud Computing Technology Roadmap ,(2014) نقشه راه فناوری محاسبات ابری دولت ایالات متحده	NIST	ارائه نقشه راه فناوری محاسبات ابری دولت ایالات متحده با هدف کاهش عدم اطمینان و نیز تسهیل توسعه بیشتر مدل محاسبات ابری

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
SP 500-299	NIST Cloud Computing Security Reference Architecture,(2013) معماری مرجع امنیت محاسبات ابری مؤسسه NIST	NIST	ارائه درک درستی از وابستگی‌های متقابل در بین خدمات ابر، عامل‌ها و نیازمندی‌های مورد نیاز دولت آمریکا در بدست آوردن خدمات ابر با سطوح امنیتی مختلف
SP 800-144	Guidelines on Security and Privacy in Public Cloud Computing,(2011) راهنمای امنیت و حریم خصوصی در محاسبات ابر عمومی	NIST	ارائه یک دید کلی از محاسبات ابری عمومی و چالش‌های حریم خصوصی و نیز امنیت مورد نیاز
SP 800-145	The NIST Definition of Cloud Computing, (2012) تعاریف NIST از محاسبات ابری	NIST	ارائه جنبه‌های مهمی از محاسبات ابری به منظور فراهم‌آوری بهترین استفاده از محاسبات ابری
SP 800-146	Cloud Computing Synopsis and Recommendations, (2012) توصیه‌ها و مرور اجمالی بر محاسبات ابری	NIST	توصیف حوزه فناوری‌های محاسبات ابری و همچنین ارائه توصیه‌نامه‌هایی برای تصمیم‌گیرندگان فناوری اطلاعات
SP 800-125	Guide to Security for Full Virtualization Technologies, (2011) راهنمای امنیت برای فناوری‌های مجازی‌سازی کامل	NIST	رسیدگی به نگرانی‌های موجود در زمینه فناوری‌های مجازی‌سازی کامل برای سرویس‌گیرنده و نیز مجازی‌سازی دسکتاپ
Interagency Report 7904	Trusted Geolocation in the Cloud: Proof of Concept Implementation, (2015) منطقه جغرافیایی قابل اعتماد در ابر: اثبات اجرای مفاهیم	NIST	ارائه اثبات اجرای مفاهیم به‌منظور رسیدگی به چالش‌های مناطق جغرافیایی و فناوری‌های زیرساخت به‌عنوان یک خدمت محاسبات ابری
	Cybersecurity Framework Manufacturing Profile (Draft), (2016) مشخصات تولیدی چارچوب امنیت سایبری	NIST	ارائه جزئیات پیاده‌سازی چارچوب امنیت سایبری توسعه یافته برای محیط تولیدی
IR 8089	An Industrial Control System Cybersecurity Performance Testbed (2015) بستر آزمایشی عملکرد امنیت سایبری یک سیستم کنترل صنعتی	NIST	ارائه بستر آزمایشی برای بررسی عملکرد امنیتی سیستم‌های کنترل صنعتی بر اساس الزامات و کنترل‌های امنیتی
	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (draft) (2017) چارچوبی برای بهبود امنیت سایبری زیرساخت‌های حیاتی	NIST	ارائه یک رویکرد مبتنی بر ریسک برای مدیریت ریسک امنیت سایبری
IR 7628	Guidelines for Smart Grid Cyber Security (2014) راهنمایی برای امنیت سایبری شبکه هوشمند برق	NIST	این گزارش سه جلدی، راهنمایی برای امنیت سایبری شبکه‌های هوشمند برق است: جلد ۱ - استراتژی، معماری و الزامات سطح بالای امنیت سایبری شبکه هوشمند جلد ۲ - حفظ حریم خصوصی و شبکه هوشمند جلد ۳ - تجزیه و تحلیل‌ها و منابع حمایت

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
IR 7761	NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications, Rev. 1 طرح اولویت اقدامات پنل تعاملی شبکه‌های هوشمند: دستورالعمل‌هایی برای ارزیابی استانداردهای بی سیم برای کاربردی‌های شبکه هوشمند	NIST	ارائه ابزار کلیدی و روش‌هایی برای کمک به طراحان سیستم شبکه هوشمند در تصمیم‌گیری آگاهانه در مورد فناوری‌های بی‌سیم موجود و در حال ظهور
SP 1058	Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts استفاده از نرم‌افزار آنتی‌ویروس مبتنی بر میزبان بر روی سیستم‌های کنترل صنعتی: دستورالعمل‌ها و روش آزمونی برای ارزیابی اثرات عملکرد	NIST	ارائه دستورالعمل‌های نصب، پیکربندی، اجرا و نگهداری نرم افزار آنتی‌ویروس بر روی یک سیستم کنترل صنعتی
SP 1108R3	NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0 (2014) چارچوب و نقشه راه NIST برای استانداردهای قابلیت همکاری شبکه‌های هوشمند	NIST	مجموعه‌ای از دستورالعمل‌ها برای به روز کردن شبکه‌های هوشمند برق و ایجاد امنیت سایبری در آن‌ها
FIPS 140-2	Security Requirements for Cryptographic Modules, 2001 نیازمندی‌های امنیتی برای ماژول‌های رمزنگاری	NIST	ارائه نیازمندی‌های امنیتی در رابطه با طراحی اجرای ماژول رمزنگاری
FIPS 196	Entity Authentication Using Public Key Cryptography احرازهویت موجودیت با استفاده از رمزنگاری کلید عمومی	NIST	ارائه پروتکل‌هایی برای احرازهویت موجودیت با استفاده از رمزنگاری کلید عمومی
FIPS 180-4	Secure Hash Standard (SHS) (2015) استاندارد درهم‌سازی امن	NIST	ارائه الگوریتم‌های درهم‌سازی امن جهت خلاصه‌سازی پیام‌ها
FIPS 186	Digital Signature Standard (DSS), (2013) استاندارد امضای دیجیتال	NIST	ارائه مجموعه‌ای از الگوریتم‌ها برای امضای دیجیتال
FIPS 197	Advanced Encryption Standard (AES), (2001) استاندارد رمزگذاری پیشرفته	NIST	جهت اطمینان از محرمانه بودن اطلاعات الکترونیکی تصویب شده است

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC), (2008) کد اصالت‌سنجی پیام برپایه درهم‌سازی	NIST	ارائه یک مکانیسم برای تایید پیام با استفاده از توابع هش رمزنگاری
FIPS 191	Guideline for The Analysis Local Area Network Security راهنمایی جهت تحلیل امنیت شبکه‌های محلی	NIST	درک نیاز به امنیت شبکه، و ارائه راهنمایی در تعیین کنترل‌های امنیتی شبکه
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems, 2004 استانداردهایی برای دسته‌بندی امنیت سیستم‌های اطلاعاتی و اطلاعات فدرال	NIST	ارائه استانداردهایی برای طبقه‌بندی امنیت اطلاعات و سیستم‌های اطلاعاتی
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems, 2006 حداقل الزامات امنیتی برای سیستم‌های اطلاعاتی و اطلاعات فدرال	NIST	ارائه حداقل نیازمندی‌های امنیتی برای اطلاعات و سیستم‌های اطلاعاتی و پشتیبانی از یک فرآیند مبتنی بر ریسک برای انتخاب کنترل‌های امنیتی مورد نیاز جهت برقراری حداقل نیازمندی‌های امنیتی
IEEE Std 1686	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (2013) استاندارد IEEE برای قابلیت‌های امنیت سایبری دستگاه‌های الکترونیکی هوشمند در ایستگاه فرعی	IEEE	تعریف توابع و ویژگی‌هایی در دستگاه‌های الکترونیکی هوشمند ایستگاه‌های فرعی برای جای دادن برنامه‌های حفاظت از زیرساخت‌های حیاتی
IEEE P1711	Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links (2010) استانداردی برای یک پروتکل رمزنگاری برای امنیت سایبری پیوندهای سریال ایستگاه‌های فرعی	IEEE	ارائه استانداردی برای یک پروتکل رمزنگاری برای امنیت سایبری پیوندهای سریال ایستگاه‌های فرعی
IEEE P1711.3	Standard for Secure SCADA Communications Protocol (SSCP) (2013) استانداردی برای پروتکل ارتباطات امن اسکادا	IEEE	تعریف پروتکل ارتباطات امن اسکادا (SSCP)، یک پروتکل رمزنگاری برای ارائه یکپارچگی و محرمانگی اختیاری برای امنیت سایبری ارتباطات پیوندهای سریال ایستگاه‌های فرعی بدون حمایت از پیام همه پخشی و بدون هیچ گونه نیازمندی‌های زمانی
IEEE Std 1815	IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3) استاندارد IEEE برای پروتکل شبکه توزیع‌شده ارتباطات سیستم‌های برق	IEEE	ارائه استانداردی برای پروتکل شبکه توزیع شده[1] ارتباطات سیستم‌های برق الکتریکی

[1] Distributed Network Protocol (DNP3)

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
P2301	Guide for Cloud Portability and Interoperability Profiles, (2014) دستورالعمل‌هایی برای مشخصات قابلیت حمل و قابلیت همکاری ابر (CPIP)	IEEE	کمک به تولیدکنندگان و کاربران در توسعه، ساخت، استفاده از محصولات و خدمات محاسبات ابری با هدف افزایش قابلیت حمل، قابلیت به اشتراک‌گذاری[1] و قابلیت همکاری سیستم‌های محاسبات ابری
P2302	Standard for Inter cloud Interoperability and Federation, (2011) استانداردی برای یکپارچه‌سازی و قابلیت همکاری بین ابری (SIIF)	IEEE	ارائه حوزه فنی توسعه استانداردهای خاص در زمینه مربوط به ابر به‌منظور یکپارچه‌سازی و قابلیت همکاری بین ابری
RFC 6272	Internet Protocols for the Smart Grid پروتکل‌های اینترنت برای شبکه هوشمند برق	IETF	شناسایی پروتکل‌های زیرساخت کلید از سلسله پروتکل‌های اینترنت برای استفاده در شبکه هوشمند برق
RFC 4130	MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2), 2005 مبادله امن داده‌های کسب و کار نظیر به نظیر مبتنی‌بر MIME، با استفاده از HTTP، بیانیه کاربردی	IETF	ارائه یک بیانیه کاربردی برای نحوه مبادله داده‌های کسب و کار ساخت یافته به صورت امن با استفاده از پروتکل انتقال HTTP به جای پروتکل SMTP، راهنمایی برای MIME EDI و ارائه مشخصات آن، تضمین قابلیت همکاری میان عامل‌های کاربر B2B EC

[1] Commonality

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
RFC 4033	DNS Security Introduction and Requirements, (2005) نیازمندی‌ها و معرفی امنیت DNS	IETF	معرفی سرویس‌هایی برای امنیت سیستم نام‌دامنه، قابلیت‌ها و محدودیت‌ها
RFC 4034	Resource Records for the DNS Security Extensions, (2005) رکوردهای منبع برای توسعه امنیت DNS	IETF	تعریف کلید عمومی، هیئت امضاءکننده، امضای دیجیتال رکورد منبع و انکار وجود رکوردهای منبع تصدیق شده و تشریح جزئیات هدف و قالب هر رکورد و بیان یک نمونه از هر رکورد منبع
RFC 4035	Protocol Modifications for the DNS Security Extensions, (2005) اصلاحات پروتکل برای توسعه امنیت DNS	IETF	توصیف اصلاحات پروتکل DNSSEC و مفهوم یک منطقه امضاء شده همراه با الزاماتی برای خدمت و برطرف‌سازی مسائل با استفاده از DNSSEC
RFC 4398	Storing Certificates in the Domain Name System (DNS), (2006) ذخیره‌سازی گواهینامه‌ها در سیستم نام دامنه (DNS)	IETF	بررسی ذخیره‌سازی رکوردهای گواهی‌نامه‌های رمزنگاری ذخیره شده در DNS
RFC 4255	Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints, (2006) استفاده از DNS برای انتشار اثر انگشت‌های کلید SSH به صورت امن	IETF	شرح یک روش تایید کلیدهای میزبان SSH با استفاده از DNSSEC و تعریف یک رکورد منبع DNS جدید، حاوی اثرانگشت کلید SSH
RFC 6698	The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, (2012) پروتکل احراز هویت موجودیت‌های نام (DANE) امنیت لایه انتقال: TLSA	IETF	ارائه روشی به منظور احراز هویت موجودیت‌های سرویس‌گیرنده و سرویس‌دهنده TLS بدون یک مرکز اعطای گواهینامه (CA)
RFC 7671	The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance, (2015) پروتکل احراز هویت مبتنی بر DNS موجودیت‌های نام‌گذاری شده (DANE): راهنمایی عملی و بروزرسانی‌ها	IETF	توصیه به مجموعه کوچکتری از ترکیب بهترین اقدامات به منظور ایجاد سادگی در طراحی، پیاده سازی و استقرار
RFC 7513	Source Address Validation Improvement (SAVI) Solution for DHCP, (2015) راه حل بهبود اعتبارسنجی آدرس مبداء[1] برای DHCP	IETF	ارائه روش‌هایی برای ایجاد اتصالاتی میان آدرس‌های IP تخصیص داده شده به DHCPv4/DHCPv6 و لنگر متصل کننده روی یک دستگاه بهبود اعتبارسنجی آدرس مبدا

[1] Source Address Validation Improvement

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
RFC 7610	DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers, (2015) پوشش محافظ DHCPv6؛ حفاظت در برابر سرویس‌دهنده‌های متقلب DHCPv6	IETF	معرفی مکانیزمی برای محافظت میزبان‌های متصل به شبکه‌های سوئیچی در برابر سرویس‌دهنده‌های DHCPv6 متقلب و همچنین ارائه بهترین اقدامات برای پیاده‌سازی پوشش محافظ DHCPv6
RFC 6353	Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), (2011) مدل انتقال TLS برای پروتکل SNMP	IETF	تعریف دو پروتکل انتقال SSH و TLS/DTLS و استفاده از مشخصات مدل امنیت انتقال
RFC 7454	BGP Operations and Security, (2015) امنیت و اقدامات BGP	IETF	ارائه اقداماتی به منظور حفاظت از نشست‌های BGP، کنترل بهتر جریان اطلاعات مسیریابی
RFC 5077	Transport Layer Security (TLS) Session Resumption without Server-Side State, (2008) نشست مجدد TLS بدون در نظرگیری وضعیت سمت سرویس‌دهنده	IETF	ارائه یک روش به منظور شروع مجدد یک نشست بدون نیاز به وضعیت یک نشست خاص در TLS سرویس‌دهنده
RFC 7301	Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension, (2014) ضمیمه مذاکره پروتکل TLS مبتنی بر لایه کاربرد	IETF	توصیف ضمیمه پروتکل TLS برای مذاکره پروتکل لایه کاربرد در دست تکانی TLS و ایجاد امکان مذاکره پروتکل بکار رفته در داخل اتصال TLS برای لایه کاربرد
RFC 6242	Using the NETCONF Protocol over Secure Shell (SSH), (2011) استفاده از پروتکل NETCONF بر روی پوسته امن (SSH)	IETF	چگونگی کاربرد NETCONF در داخل نشست SSH و استفاده از پروتکل اتصال SSH (RFC 4254) روی پروتکل انتقال (RFC 4253)

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
ISO/IEC 17788	Information technology -- Cloud computing -- Overview and vocabulary,(2014) فناوری اطلاعات- محاسبات ابری- مرور کلی و واژگان	ISO/IEC	ارائه اصطلاحات محاسبات ابری و واژگان این محاسبات
ISO/IEC 17789	Information technology -- Cloud computing -- Reference architecture, (2014) فناوری اطلاعات- محاسبات ابری- معماری مرجع	ISO/IEC	ارائه معماری مرجع شامل نقش‌ها، فعالیت‌ها، اجزای عملکردی و روابط بین محاسبات ابری
ISO/IEC 27017	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services,(2015) فناوری اطلاعات- فنون امنیتی- کد عمل برای کنترل‌های امنیت اطلاعات بر مبنای استاندارد ISO/IEC 27002 برای خدمات ابر	ISO/IEC	ارائه دستورالعمل‌هایی به‌منظور استفاده از خدمات ابر با توجه به کنترل‌های امنیت اطلاعات قابل اجرا
ISO/IEC 27018	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, (2014) فناوری اطلاعات- فنون امنیتی- کد عمل جهت حفاظت از اطلاعات شناسایی شخصی (PII) در ابرهای عمومی که به عنوان پردازنده‌های PII عمل می‌کنند.	ISO/IEC	ارائه کنترل‌ها و دستورالعمل‌های قابل اجرا در چارچوب تهدیدات علیه امنیت اطلاعات ارائه‌دهندگان خدمات محیط ابر عمومی مبتنی بر استانداردهای ISO/IEC 29100 و ISO/IEC 27002.
ISO/IEC 17826	Information technology -- Cloud Data Management Interface (CDMI),(2016) فناوری اطلاعات- رابط مدیریت داده‌های ابر	ISO/IEC	مشخص نمودن واسطهایی به‌منظور دسترسی به فضای ذخیره‌سازی ابر و همچنین داده‌های ذخیره‌شده در آن
ISO/IEC 27036-2	Information technology-- Security techniques-- Information security for supplier relationships-- Part 2: Requirements, (2014) فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط عرضه‌کنندگان- بخش دوم: نیازمندی‌ها	ISO/IEC	ارائه امنیت اطلاعات بنیادی برای تعریف، پیاده‌سازی، اجرا، نظارت، بازنگری، نگه‌داری و بهبود روابط عرضه‌کننده کالا و خریدار از جمله خدمات محاسبات ابری
ISO/IEC 27036-4	Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services,(2016) فناوری اطلاعات- فنون امنیتی- امنیت اطلاعات برای روابط عرضه‌کنندگان- بخش چهارم: راهنمایی برای امنیت خدمات ابر	ISO/IEC	ارائه دستورالعمل‌ها و کنترل‌هایی درباره تهدیدات امنیت اطلاعات و نیز نحوه پاسخ‌گویی به این تهدیدات در رابطه با مشتریان و عرضه‌کنندگان خدمات ابر
ISO/IEC 27040	Information technology -- Security techniques -- Storage security, (2015) فناوری اطلاعات- فنون امنیتی- امنیت ذخیره‌سازی	ISO/IEC	ارائه راهنمای فنی دقیق در مورد کاهش ریسک با به‌کارگیری رویکرد اثبات شده در زمینه برنامه‌ریزی، طراحی، مستندسازی و پیاده‌سازی امنیت ذخیره‌سازی داده

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
ISO TR 17791	Health informatics -- Guidance on standards for enabling safety in health software (2013) اطلاعات سلامت- راهنمای استانداردهایی برای قابلیت ایمنی در نرم‌افزار سلامت	ISO	ارائه راهنمایی برای شناسایی یک مجموعه منسجم از استانداردهای بین‌المللی مربوط به توسعه، اجرا و استفاده امن نرم‌افزار سلامت
ISO 14971	Medical devices -- Application of risk management to medical devices (2007) دستگاه‌های پزشکی- کاربرد مدیریت ریسک در دستگاه‌های پزشکی	ISO	ارائه فرایندی برای شناسایی خطرات مرتبط با دستگاه‌های پزشکی
ISO/IEC 20547-4	Information technology -- Big data reference architecture -- Part 4: Security and privacy fabric, (2019) فناوری اطلاعات- معماری مرجع داده‌های کلان- بخش چهارم: امنیت و حریم خصوصی	ISO/IEC	توصیف روش‌های تأمین حریم خصوصی و امنیت پایه اعمال شده در تمامی جنبه‌های مدل مرجع از جمله نقش‌های داده کلان، فعالیت‌ها و اجزای عملکردی
ISO/IEC 27000	Information technology – Security techniques – Information security manage systems – Overview and vocabulary,(2016) های مدیریت های امنیتی- سیستم‌فناوری اطلاعات- روش امنیت اطلاعات- مرور کلی و واژگان	ISO/IEC	بررسی کلی سیستم‌های مدیریت امنیت اطلاعات، واژگان و تعاریف مشترک مورد استفاده در مجموعه استانداردهای ISMS[1]
ISO/IEC 29100	Information technology – Security techniques – Privacy framework,(2011) فناوری اطلاعات- روش‌های امنیتی- چارچوب حریم خصوصی	ISO/IEC	ارائه یک چارچوب حریم خصوصی برای اشخاص حقیقی و سازمان‌های درگیر در طراحی، توسعه، آزمون، نگه‌داری و اجرای سیستم‌ها و خدمات فناوری اطلاعات و ارتباطات.
	The Big Data Analytics Guidebook, (2015) کتاب راهنمای تجزیه و تحلیل داده کلان	TMF	تعریف دستورالعمل‌هایی به‌منظور ارائه یک مدل مرجع، موارد کاربرد، بخش‌های سازنده و تجزیه و تحلیل مخزن داده‌های کلان جهت تحلیل‌های داده‌های کلان

[1] Information Security Manage Systems

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
Y.3600	Big data standardization roadmap,(2016) نقشه راه استانداردسازی داده‌های کلان	ITU-T	توصیف ویژگی‌ها و مفاهیم کلی از اکوسیستم داده‌های کلان
Y.BigDataEX-reqts	Big data exchange framework and requirements, (2017) چارچوب و الزامات تبادل داده‌های کلان	ITU-T	مشخص نمودن چارچوب تبادلات داده‌های کلان و الزامات آن‌ها بر اساس موارد استفاده و سناریوها، تجزیه و تحلیل شکاف‌های موجود و شناسایی الزامات عملکردی در میان اکوسیستم ارتباطات راه دور
Y.BdaaS-arch	Functional architecture of Big data as a Service, (2016) معماری عملکردی داده‌های کلان به‌عنوان یک خدمت	ITU-T	توصیف اجزای عملیاتی، معماری عملیاتی و نیز نقاط مرجع از داده‌های کلان به‌عنوان یک خدمت
Y.bDDN-req	Requirement of big data-driven networking (bDDN), (2018) نیازمندی‌های شبکه‌های مبتنی‌بر داده‌های کلان	ITU-T	مشخص نمودن نیازمندی‌های شبکه‌های مبتنی‌بر داده‌های کلان با هدف استفاده مؤثر از اطلاعات با ارزش شبکه توسط شبکه
Y.bDDN-fr	Framework of big data driven networking based on DPI,(2018) چارچوبی برای شبکه‌های مبتنی‌بر داده‌های کلان بر اساس DPI	ITU-T	ارائه چارچوبی برای شبکه‌های داده‌های کلان مبتنی‌بر DPI
Y.dsf-reqts	Requirements and capabilities for data storage federation,(2018) الزامات و قابلیت‌هایی به‌منظور یکپارچه‌سازی ذخیره‌سازی داده‌ها	ITU-T	توصیف و بررسی کلی، الزامات و قابلیت‌های یکپارچه‌سازی ذخیره‌سازی داده
Y.bDPI-Mec	Mechanism of deep packet inspection applied in network big data context,(2018) مکانیسم بازرسی عمیق و دقیق بسته‌های مورد استفاده در زمینه داده‌های کلان شبکه	ITU-T	پرداختن به بازرسی عمیق بسته‌ها در داده‌های کلان به دلیل نامناسب بودن این مکانیسم‌ها در روش‌های سنتی برای این داده‌ها
Y.SDN-ARCH	Functional architecture of software-defined networking, (2017) معماری عملکردی شبکه‌های مبتنی‌بر نرم‌افزار	ITU-T	توصیف چارچوب شبکه‌های مبتنی‌بر نرم‌افزار شامل تعاریف، اهداف، قابلیت‌های سطح بالا، نیازمندی‌ها و نیز معماری سطح بالا SDN
Y.bdp-reqts	Big data – Requirements for data provenance, (2018) داده‌های کلان– الزامات مورد نیاز منابع داده	ITU-T	بررسی کلی و بیان الزامات مورد نیاز منابع داده‌های کلان شامل ویژگی‌ها، منطق برنامه کاربردی و چارچوب عملکردی
TU-T Y.3300	Framework of software-defined networking, (2016) چارچوب شبکه‌های مبتنی‌بر نرم‌افزار	ITU-T	توصیف چارچوب شبکه مبتنی‌بر نرم‌افزار شامل تعاریف، اهداف، قابلیت‌های سطح بالا، نیازمندی‌ها و معماری سطح بالا SDN
Y.IoT-BigData-reqts	Specific requirements and capabilities of the Internet of Things for Big data,(2016) الزامات و قابلیت‌های خاص اینترنت اشیا برای داده‌های کلان	ITU-T	تعیین نیازمندی‌ها و قابلیت‌های اینترنت اشیا برای داده‌های کلان و نیز ارائه یک چارچوب کاربردی از IoT از منظر نیازمندی‌ها و قابلیت‌های خاص IoT جهت رسیدگی به چالش‌ها در زمینه داده‌های کلان

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
Y.cceco	Cloud Computing Ecosystem, use cases and general requirements,(2012) اکوسیستم محاسبات ابری، موارد کاربرد و نیازمندی‌های کلی و عمومی	ITU-T	ارائه نیازمندی‌های عمومی در زمینه اکوسیستم ابر متمرکز بر یکپارچه‌سازی و نیز حمایت از مدل محاسبات ابری و فناوری‌ها در محیط‌های مخابراتی و فناوری اطلاعات و ارتباطات، با توجه به موارد امنیتی مرتبط با ابر
Y.ccic	Framework of inter-cloud computing for network and infrastructure, (2015) چارچوب محاسبات بین ابری برای شبکه و زیرساخت	ITU-T	تمرکز بر روی استفاده از منابع شبکه و زیرساخت‌ها و همچنین تصریح چارچوب بین ابری به‌منظور متصل نمودن تعداد زیادی از اپراتورهای کسب‌وکار IaaS و Naas
Y.ccra	Cloud Computing Reference Architecture, (2012) معماری مرجع محاسبات ابری	ITU-T	توسعه معماری مرجع محاسبات ابری بر اساس اسناد Y.CCEco و ISO/IEC WD 17789
X.ccsec (ITU-T X.1601)	Security framework for cloud computing, (2015) چارچوب امنیتی برای محاسبات ابری	ITU-T	ارائه یک چارچوب امنیتی سطح بالا برای محاسبات ابری مبتنی‌بر تهدیدات امنیتی، نیازمندی‌های امنیتی و مناطق امنیتی ابر
X.goscc (ITU-T X.1642)	Guidelines for the operational security of cloud computing, (2015) راهنمایی برای امنیت عملیاتی محاسبات ابری	ITU-T	فراهم کردن دستورالعمل‌هایی برای امنیت عملیاتی محاسبات ابری از جمله راهنمای توافق‌نامه سطح خدمات[1] (SLA) و همچنین حفظ امنیت در محاسبات ابری
X.sfcse (ITU-T X.1602)	Security functional requirements for software as a service application environments,(2015) نیازمندی‌های عملکردی امنیت برای محیط کاربردی نرم‌افزار به‌عنوان خدمت[3] (SaaS)	ITU-T	ارائه یک توصیف عملکردی عمومی برای محیط کاربردی نرم‌افزار به‌عنوان یک خدمت سرویس‌گرای امن[2] مستقل از انواع شبکه، سیستم‌عامل، میان‌افزار، محصولات و یا راه‌حل‌های خاص
X.idmcc	Requirement of IdM in Cloud Computing, (2014) نیازمندی‌های مدیریت هویت در محاسبات ابری	ITU-T	تمرکز بر روی هماهنگ‌سازی[4] خدمات مخابراتی و اینترنت برمبنای زیرساخت‌های مدیریت هویت مشترک در محیط محاسبات ابری
QCTIC	Trusted inter-cloud computing framework and requirements, (2015) نیازمندی‌ها و چارچوب‌های محاسبات بین ابری قابل اعتماد	ITU-T	ارائه چارچوب محاسبات بین ابری قابل اعتماد و موارد کاربردی مبتنی‌بر چارچوب مشخص شده در Rec. Y.3511 با توجه به برقراری الزامات امنیتی قابل اعتماد
M.mivrcc	Requirements and analysis for management interface of virtualized resources in cloud computing, (2017) نیازمندی‌ها و تحلیل‌های لازم برای رابط مدیریت منابع مجازی در محاسبات ابری	ITU-T	تعیین نیازمندی‌ها و تحلیل‌ها برای رابط مدیریت بین سیستم پشتیبانی عملیات ابر[5] (COSS) و عامل مدیریت منابع مجازی[6] (VRM) شامل مدیریت تنظیمات، مدیریت خطا و مدیریت عملکرد

[1] service level agreement
[2] secure service oriented Software as a Service
[3] Software as a Service
[4] Harmonization
[5] Cloud Operational Support System
[6] Virtualized Resource Management

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
X.CSCdataSec (ITU-T X.1641)	Guidelines for cloud service customer data security, (2016) دستورالعمل‌هایی برای امنیت داده‌های مشتری خدمات ابر	ITU-T	ارائه راهنمایی‌هایی جهت حصول اطمینان نسبت به استفاده از مکانیسم‌های امنیتی مناسب جهت امنیت داده‌های مشتری خدمات ابر توسط CSP[1]
X.dsms	Data security requirements for the monitoring service of cloud computing, (2017) نیازمندی‌های امنیت داده‌ها به‌منظور نظارت بر خدمات محاسبات ابری	ITU-T	تجزیه و تحلیل نیازمندی‌های امنیتی داده به‌منظور نظارت بر خدمات محاسبات ابری، شامل نظارت بر حوزه‌های داده، نظارت بر چرخه عمر داده، نظارت بر اکتساب داده‌ها و ارائه نیازمندی‌های امنیتی در مورد نحوه ذخیره‌سازی داده‌ها
X.SRIaaS	Security requirements of public infrastructure as a service (IaaS) in cloud computing,(2018) نیازمندی‌های امنیتی زیرساخت‌های عمومی به‌عنوان یک خدمت در محاسبات ابری	ITU-T	مستندسازی نیازمندی‌های امنیتی IaaS عمومی به‌منظور بهبود سطح امنیت کلی در سراسر مراحل برنامه‌ریزی، ساخت و نیز مراحل عملیاتی بسترها و خدمات IaaS
Y.e2ecslm-Req	End-to-end cloud service lifecycle management requirements, (2016) نیازمندی‌های مدیریت چرخه حیات خدمات ابر انتها به انتها	ITU-T	تعیین الزامات عملکردی چرخه حیات از جنبه‌های مدیریت خدمات ابر شامل مدیریت وقایع[2]، مدیریت سیاست[3]، مدیریت اطلاعات مربوط به نقش، مدیریت منابع، مدیریت بستر و مدیریت محتوا
Q18 Y.CCNaaS-arch	Cloud computing - Functional Architecture of Network as a Service, (2016) محاسبات ابری- معماری عملکردی شبکه به‌عنوان یک خدمت	ITU-T	تعیین معماری کاربردی NaaS شامل قابلیت‌ها، اجزای عملکردی و هم‌چنین رویه‌ها و نقاط مرجع مبتنی‌بر نیازمندی‌های عملکردی مشخص‌شده در سند Y.3512
Y.e2eccrmr	Cloud computing framework for end-to-end resource management, (2015) چارچوب محاسبات ابری برای مدیریت منابع انتها به انتها	ITU-T	فراهم آوردن مدیریت یکپارچه خدمات و منابع در شیوه‌ای انتها به انتها و با توجه به خدمات پیکربندی‌شده بر روی یک یا تعدادی از سیستم‌های ابری و نیز با هدف ارائه برنامه‌های کاربردی در لایه‌های بالایی
ISA / IEC-62443ANSI / ISA-99	Security for Industrial Automation and Control Systems امنیت برای سیستم‌های کنترل و اتوماسیون صنعتی	ISA	تعریف یک سری از استانداردها، گزارش‌های فنی و اطلاعات مرتبط جهت ارائه روشی برای پیاده‌سازی الکترونیکی امن سیستم‌های کنترل و اتوماسیون صنعتی (IACS)
ANSI/ISA-95	Enterprise-Control System Integration یکپارچه‌سازی سیستم کنترل و شرکت	ISA	ارائه یک استاندارد بین‌المللی از جامعه بین‌المللی اتوماسیون جهت توسعه‌ی یک رابط خودکار بین شرکت و سیستم‌های کنترل صنعتی
ISA100.11A	Wireless Systems for Automation: Process control and related applications سیستم‌های بی‌سیم برای خودکارسازی: کنترل فرآیند و برنامه‌های کاربردی مربوطه	ISA	ایجاد روش‌های توصیه شده، گزارش‌های فنی و اطلاعات مربوطه برای پیاده‌سازی سیستم‌های بی‌سیم در اتوماسیون و محیط‌های کنترلی

[1] Cloud Service Provider
[2] Events management
[3] policy management

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
	21 Steps to Improve Cyber Security of SCADA Networks ۲۱ گام برای بهبود امنیت سایبری شبکه‌های اسکادا	DHS-NCCIC, ICS-CERT	۲۱ گام شامل اقدامات ضروری جهت بهبود حفاظت از شبکه‌های اسکادا
	Recommended Practice: Creating Cyber Forensics Plans for Control Systems (2008) رویه‌های توصیه شده: ارائه طرح‌های جرم‌یابی سایبری برای سیستم‌های کنترل	DHS-NCCIC, ICS-CERT	ارائه راهنمایی‌های همراه با پیچیدگی‌های خاص جرم‌یابی سایبری برای سیستم‌های کنترل صنعتی
	Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability (2009) رویه توصیه شده: توسعه یک قابلیت پاسخ به رویداد امنیت سایبری برای سیستم‌های کنترل صنعتی	DHS-NCCIC, ICS-CERT	ارائه توصیه‌هایی برای کمک به تاسیسات صنعتی برای واکنش بهتر به حوادث سایبری
	Recommended Practice Case Study: Cross-Site Scripting (2007) رویه‌های توصیه شده- مطالعه موردی: حمله Cross-Site Scripting	DHS-NCCIC, ICS-CERT	تشریح جرئیات حمله Cross-Site Scripting علیه سیستم‌های کنترل صنعتی
	Recommended Practice for Patch Management of Control Systems (2008) رویه‌های توصیه شده برای مدیریت وصله سیستم‌های کنترلی	DHS-NCCIC, ICS-CERT	تشریح مدیریت وصله نرم‌افزار سیستم‌های کنترل صنعتی
	Recommended Practice for Securing Control System Modems (2008) رویه‌های توصیه شده برای تأمین امنیت مودم‌های سیستم کنترلی	DHS-NCCIC, ICS-CERT	ارائه راهنمایی‌هایی برای تجزیه و تحلیل متدولوژی‌های ارزیابی خطرات امنیتی درمورد مودم‌ها و استفاده از آن‌ها در یک سازمان
	Recommended Practice: Configuring and Managing Remote Access for Industrial Control Systems (2010) رویه‌های توصیه شده: پیکربندی و مدیریت دسترسی راه دور برای سیستم‌های کنترل صنعتی	DHS-NCCIC, ICS-CERT	ارائه پشتیبانی برای راه‌حل‌های دسترسی از راه دور برای سیستم‌های کنترل صنعتی
	Catalog of Control Systems Security: Recommendations for Standards Developers (2011) کاتالوگ امنیت سیستم‌های کنترل: توصیه‌هایی برای توسعه‌دهندگان استانداردها	NCCIC, ICS-CERT	ارائه تلفیقی از شیوه‌های توصیه‌شده توسط صنعت‌های مختلف برای افزایش امنیت سیستم‌های کنترلی خود در برابر حملات فیزیکی و شبکه
	Control Systems Cyber Security: Defense in Depth Strategies (2016) امنیت سایبری سیستم‌های کنترل: استراتژی‌های دفاع در عمق	NCCIC, ICS-CERT	ارائه راهنمایی‌هایی برای توسعه استراتژی‌های بهبوددهنده تهدیدات سایبری ویژه و همچنین توصیه‌های برای ایجاد یک برنامه امنیتی دفاع در عمق برای محیط‌های سیستم کنترلی

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
	Cyber Security Assessments of Industrial Control Systems (2010) ارزیابی امنیت سایبری سیستم‌های کنترل صنعتی	NCCIC, ICS-CERT	ارائه یک نمای کلی از فرآیند ارزیابی برای درک کاربران از چگونگی ارزیابی امنیت سایبری ICS
	FIREWALL DEPLOYMENT FOR SCADA AND PROCESS CONTROL NETWORKS (2005) استقرار دیواره‌آتش برای اسکادا و شبکه‌های کنترل فرآیند	CPNI	توضیح درمورد دیواره‌های آتش، مدیریت و پیکربندی و به کارگیری آن‌ها در معماری شبکه کنترلی
	NESCOR[1] Guide to Penetration Testing for Electric Utilities (2014) راهنمای NESCOR برای آزمون نفوذپذیری تجهیزات الکتریکی	EPRI	ارائه نحوه انجام آزمون نفوذپذیری در شبکه‌های برق
	Object Linking and Embedding (OLE) for Process Control (OPC) standards OLE برای استانداردهای کنترل فرآیند	OPC foundation	یک سری از استانداردهای تعامل متقابل برای تبادل امن و قابل اعتماد اطلاعات در فضای اتوماسیون صنعتی و در صنایع دیگر
AGA Standard 12	Cryptographic Protection of SCADA Communications محافظت به وسیله رمزنگاری از ارتباطات اسکادا	AGA[2]	ارائه شیوه‌های توصیه شده‌ای برای محافظت از ارتباطات اسکادا در برابر حوادث سایبری با تمرکز روی حصول اطمینان از محرمانه بودن ارتباطات اسکادا
MTR070050	MITRE TECHNICAL REPORT: Addressing Industrial Control Systems in NIST Special Publication 800-53 پرداختن به سیستم‌های کنترل صنعتی در NIST SP 800-53	MITRE Department	تحلیل چگونگی پرداختن SP 800-53 به امنیت سایبری در سیستم‌های کنترل صنعتی (ICS)، با تمرکز خاص بر روی سیستم‌های انرژی الکتریکی
	NERC CIP (critical infrastructure protection) حفاظت از زیرساخت‌های حیاتی	CIP	طرح NERC CIP شامل ۹ استاندارد و ۴۵ نیازمندی جهت پوشش امنیت محیطی الکترونیکی و حفاظت از دارایی‌های حیاتی سایبری و همچنین تعریف روش‌های آموزش پرسنل، مدیریت امنیت و برنامه‌ریزی بازیابی فاجعه
	Power systems management and associated information exchange مدیریت سیستم‌های برق و تبادل اطلاعات مربوطه	IEC	توسعه استانداردهایی به منظور تبادل اطلاعات برای سیستم‌های قدرت و دیگر سیستم‌های مرتبط از جمله سیستم‌های مدیریت انرژی، اسکادا، اتوماسیون توزیع‌شده و محافظت از راه دور

[1] National Electric Sector Cybersecurity Organization Resource
[2] American Gas Association

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
API 1164	Pipeline SCADA Security, Second Edition (2009) امنیت اسکادای خط لوله	American Petroleum Institute (API)	راهنمایی برای اپراتورهای سیستم‌های خط لوله نفت و گاز طبیعی به منظور مدیریت صحت و امنیت سیستم اسکادا
AUTO11-A2	IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard- second edition (2014) امنیت IT ابزار تشخیصی آزمایشگاهی و سیستم‌های نرم‌افزار	CLSI[1]	ارائه یک چارچوب برای مسائل امنیت ارتباطات IT بین فروشندگان سیستم‌های تشخیص پزشکی و سازمان‌های بهداشت و درمان
IEC 80001	Application of risk management for IT-networks incorporating medical devices (2010) کاربرد مدیریت ریسک برای دستگاه‌های پزشکی ادغام‌شده با شبکه‌های IT	IEC	استانداردی برای پشتیبانی از مدیریت تجهیزات پزشکی ادغام‌شده با شبکه‌های فناوری اطلاعات
AAMI TIR57	Principles for medical device security—Risk management (2016) اصولی برای مدیریت ریسک امنیتی دستگاه‌های پزشکی	AAMI[2]	ارائه راهنمایی برای انجام مدیریت ریسک امنیت اطلاعات برای یک دستگاه پزشکی در زمینه فرآیند "مدیریت ریسک ایمنی"[3] مورد نیاز ISO 14971
	The Privacy and Security Gaps in Health Information Exchanges (2011) شکاف‌های حریم خصوصی و امنیت در مبادلات اطلاعات سلامت	AHIMA[4] and HIMSS[5]	بیان مسائل مربوط به مدیریت امنیت، امنیت فنی و فیزیکی، مدیریت دسترسی، سلامت عمومی و حریم خصوصی در انتقال اطلاعات پزشکی
DSP0243	Open Virtualization Format Specification, (2015) مشخصات قالب مجازی‌سازی باز (OVF)	DMTF	ارائه قالب باز، قابل حمل، امن، کارآمد و توسعه‌پذیر به‌منظور بسته‌بندی و توزیع نرم‌افزار برای اجرا در ماشین‌های مجازی
DSP0263	Cloud Infrastructure Management Interface (CIMI) Model and REST Interface over HTTP, (2016) مدل رابط مدیریت زیرساخت ابر (CIMI) و رابط REST برروی پروتکل HTTP	DMTF	توصیف یک مدل و پروتکل به‌منظور تعامل مدیریت در بین یک ارائه‌دهنده زیرساخت ابر به‌عنوان یک خدمت و مصرف‌کنندگان خدمات IaaS

[1] Clinical and Laboratory Standards Institute
[2] The Association for the Advancement of Medical Instrumentation
[3] Safety Risk Management
[4] American Health Information Management Association
[5] Healthcare Information and Management Systems Society

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
DSP0264	Cloud Infrastructure Management Interface - Common Information Model (CIMI-CIM), (2013) رابط مدیریت زیرساخت ابر- مدل اطلاعات مشترک	DMTF	امکان‌پذیر ساختن استفاده از فرا مدل مشترک با استفاده از مدل اطلاعات مشترک (CIM) و به‌منظور توصیف مدل منطقی CIMI
DSP2028	Cloud Auditing Data Federation (CADF) Use Case, (2012) موارد کاربرد یکپارچه‌سازی ممیزی داده ابر	DMTF	ارائه مجموعه‌ای از مواردکاربرد در دنیای واقعی جهت فراهم کردن ملاحظات ممیزی خاص منابع مبتنی‌بر ابر، شامل نوع داده، منبع و تعاملات مورد انتظار توسط نهادهای مسئول
	Open certification Framework, (2013) چارچوب صدور گواهی‌نامه باز	CSA	ارائه یک طرح صنعتی به‌منظور تولید گواهی‌نامه‌های قابل اعتماد، معتبر و جهانی و با توجه به اهداف کنترلی و راهنماهای امنیتی توسط ارائه‌دهندگان خدمات ابر
	Trusted Cloud Initiative (TCI) Reference Architecture Model,(2011) مدل معماری مرجع طرح ابر قابل اعتماد	CSA	ارائه ترکیب بهترین الگوهای معماری به‌منظور ایجاد یک رویکرد جامع برای امنیت ابر
	Cloud Controls Matrix (CCM),(2017) ماتریس کنترل‌های ابر	CSA	ارائه یک چارچوب کنترل‌های امنیتی برای ارائه‌دهنده خدمات ابر و مصرف‌کننده آن خدمات
	Top Threats to cloud computing,(2017) تهدیدات مهم در محاسبات ابری	CSA	ارائه زمینه‌های مورد نیاز برای کمک به سازمان‌ها به‌منظور تصمیم‌گیری درست در زمینه مدیریت ریسک با توجه به استراتژی‌های به‌تصویب رسیده در ابر
	Security as a Service (SecaaS) Implementation Guidance, (2016) راهنمای اجرای امنیت به‌عنوان یک خدمت	CSA	ارائه راهنمایی‌هایی به‌منظور اجرای امنیت در حوزه‌های طراحی، پیاده‌سازی، خدمات مدیریت دسترسی و به‌طور خاص موارد اعمال شده در محاسبات ابری
	Security Guidance for Critical Areas of Focus in Cloud Computing, (2015) راهنمای امنیتی برای حوزه‌های بحرانی متمرکز در محاسبات ابری	CSA	شامل ۱۴ حوزه کاری که این حوزه‌های کاری با استانداردهای صنعتی و بهترین رویه‌ها، برابری می‌کنند. هم‌چنین این راهنما به‌عنوان یک عامل مهم در مدیریت استراتژیک خدمات ابر عمل می‌کند.
	Cloud Application Management for Platforms (CAMP), (2014) مدیریت برنامه‌های کاربردی ابر برای پلتفرم‌ها	OASIS	تعریف مصنوعات و رابط برنامه‌های کاربردی که بایستی توسط پلتفرم به‌عنوان یک خدمت ابر جهت مدیریت ایجاد، اجرا، نظارت و وصله برنامه‌های کاربردی در ابر ارائه شود.
	Identity in the Cloud (IDCloud),(2012) هویت در ابر	OASIS	هماهنگی تعاریف، اصطلاحات و واژگان هویت در زمینه محاسبات ابری و توسعه مشخصات استانداردهای باز به منظور استقرار، تأمین و مدیریت هویت
	Topology and Orchestration Specification for Cloud Applications (TOSCA),(2016) مشخصات توپولوژی و تنظیمات مربوط به برنامه‌های کاربردی ابر	OASIS	ارائه یک استاندارد ابر باز جدید به‌منظور ایجاد اکوسیستم منحصربه‌فرد با هدف بهبود قابلیت حمل برنامه‌های کاربردی و خدمات ابر در سراسر چرخه حیات آن‌ها
	Symptoms Automation Framework (SAF), (2014) چارچوب اتوماسیون علائم	OASIS	ارائه تعاریفی از یک معماری مرجع برای چارچوب اتوماسیون علائم، یک ابزار در تشخیص خودکار، بهینه‌سازی، اصلاح و بازسازی جنبه‌های عملیاتی از یک سیستم پیچیده به ویژه مراکز داده

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
	Cloud Authorization (CloudAuthZ),(2016) مجوزدهی ابر	OASIS	توسعه بهبود مدل‌ها به‌منظور مدیریت مجوزها و حقوق دسترسی در زمینه‌های SaaS، PaaS، IaaS
	Public Administration Cloud Requirements (PACR), (2013) الزامات ابر جهت مدیریت ملی	OASIS	توسعه الزامات عملیاتی محاسبات ابری برای ادارات دولتی به‌منظور ارائه تضمین قابلیت ممیزی[1]، آزمون انطباق‌پذیری[2] و معیارهای اکتساب[3]
	Security Services (SAML) TC, (2012) سرویس‌های امنیتی (زبان نشانه گذاری تاکید امنیتی)	OASIS	چارچوب مبتنی بر XML برای مرتبط کردن اطلاعات ویژگی‌ها و حقوق و احرازهویت کاربر
	eXtensible Access Control Markup Language (XACML) TC, (2013) زبان نشانه‌گذاری قابل گسترش کنترل دسترسی	OASIS	طرح XML پایه برای نشان دادن سیاست مجوز دهی و حقوق
	Trusted Multi-Tenant Infrastructure (TMI) architecture, (2014) معماری زیرساخت چند کاربره مورد اعتماد	TCG	ارائه مدل‌های مرجع انتها به انتها[4] به‌منظور استقرار عملی زیرساخت‌های ابر قابل اعتماد
	Trusted Multi-Tenant Infrastructure (TMI) Use Cases, (2011) موارد استفاده زیرساخت چندکاربره مورد اعتماد	TCG	نگاشت فناوری‌های TCG و استانداردهای صنعتی مناسب به‌منظور توصیف روابط بنیادی در بین اجزای متفاوت یک سازمان در یک حوزه محاسباتی قابل اعتماد
	Cloud Data Management Interface (CDMI) specification,(2015) مشخصات رابط مدیریت داده‌های ابر	SNIA	ارائه یک پروتکل با ویژگی‌های خود تأمینی[5]، مدیریتی و با دسترسی به فضای ذخیره‌سازی ابر
	Information technology -- Cloud Data Management Interface (CDMI),(2016) فناوری اطلاعات– رابط مدیریت داده‌های ابر	ISO/IEC & SNIA	ارائه رابطی به منظور دسترسی به فضای ذخیره‌سازی ابر و مدیریت اطلاعات ذخیره‌شده در آن
	Service-oriented Cloud Computing Infrastructure (SOCCI) Framework,(2011) چارچوب زیرساخت محاسبات ابری خدمت‌گرا	Open Group	ارائه چارچوب زیرساخت محاسبات ابری خدمت‌گرا به‌منظور کمک به کسب‌وکار و فناوری اطلاعات حرفه‌ای

[1] Auditable assurance
[2] Conformance testing
[3] Acquisition criteria
[4] End-to-End reference models
[5] Self-provisioning

شماره استاندارد	نام استاندارد	سازمان منتشر کننده	هدف
	Cloud Computing Reference Architecture (CCRA), (2013) معماری مرجع محاسبات ابری	Open Group	ارائه مجموعه‌ای از الگوهای مهاجرت به ابر، شامل چارچوب مشترک به‌منظور هماهنگی در بین رویکردهای مهاجرتی مختلف در حمایت از به‌کارگیری ابر به عنوان یک الگوی قابل تحویل
ETSI TS 133 220	Digital Cellular Telecommunications System (Phase 2+) (GSM)/ Universal Mobile Telecommunications System (UMTS)/ LTE/ Generic Authentication Architecture (GAA)/ Generic Bootstrapping Architecture (GBA), (2016) سیستم‌های مخابرات دیجیتال تلفن همراه (GSM)- سیستم جهانی ارتباطات راه دور موبایل- فناوری تکامل بلند مدت (LTE)- سرویس‌های همه پخشی/چندپخشی چندرسانه‌ای	3GPP	شرح ویژگی‌ها و مکانیزم‌های امنیتی جهت راه‌اندازی[1] مکانیزم احرازهویت و توافق کلید برای امنیت نرم‌افزار
ETSI TS 118 508	Analysis of Security Solutions for the oneM2M System, (2014) تجزیه و تحلیل راه‌حل‌های امنیتی برای سیستم oneM2M	oneM2M	بررسی سرویس‌های امنیتی، تجزیه و تحلیل تهدید و نیازمندی‌های امنیتی در سیستم‌های oneM2M
ETSI TS 118 103	Security solutions, (2016) راحل‌های امنیتی	oneM2M	راه حل امنیتی قابل اجرا در سیستم M2M
ETSI EN 300 175-7	Digital Enhanced Cordless Telecommunications (DECT)/Common Interface (CI)/ Part 7: Security features, (2015) ارتباطات بی‌سیم پیشرفته دیجیتالی/رابط مشترک /بخش۷: ویژگی‌های امنیتی	ETSI DECT	الزامات مورد نیاز برای یکپارچه‌سازی ویژگی‌های امنیتی ارائه شده با معماری DECT CL
	XML Key Management Specification, (2005) مشخصات مدیریت کلید XML	W3C	مشخصه پروتکل‌ها و سرویس‌های XKMS وخصوصیات امنیتی برای مدیریت کلید XML

[1] bootstrap

پیوست شماره ۳

لغت‌نامه

فارسی	لاتین
انتزاعی	Abstraction
دقت	Accuracy
بازیگران	Actors
تجمیع	aggregation
هشدار	alert
برنامه‌های کاربردی	Application
بایگانی	Archive
مصنوعات	Artifact
دارایی	Asset
اطمینان	Assurance
بدون استفاده	At rest
ممیزی	Audit
احرازهویت	Authentication
مجوزدهی	Authorization
دسترس‌پذیری	Avalability
پشتیبان‌گیری	Backup
نشان	Badge
نقض	Breaks
بخش‌های سازنده	Building Block
کسب و کار	Business
زنجیره نگهداری	Chain of custody
نقطه بررسی	Checkpoint
اصلاح	Cleansed
محیط بسترهای محاسبات همراه و تحویل ابری	Cloud delivery and mobile computing platforms
جوامع درگیر	Communities Involved
جامعیت	Completeness
تطابق پذیری	Compliance
مؤلفه	Component
سازمان اصلی	Core Enterprise
سیاست‌های امنیت فرهنگی	Cultural Security Policies
داشبورد	Dashboard
تضمین داده	Data Assurance

فارسی	لاتین
پالایه داده	Data Redaction
مدل‌سازی امنیت داده	Data Security Modeling
بازرسی عمیق	Deep Inspection
دفاع در عمق	Defense in-Depth
طراحی پاسخگویی	Design for Accountability
طراحی مقررات	Design for Regulations
جرم یابی دیجیتالی	Digital Forensics
بازیابی فاجعه	Disaster Recovery
محرک	Driver
فراسازمانی	Enterprise
هک اخلاقی	Ethical Hacking
مدیریت استثنا	Exception management
سوءاستفاده	Exploit
سازمان گسترده	Extended Enterprise
قابلیت توسعه	Extensibility
مثبت کاذب	False Positive
دیوار آتش	Firewall
تشخیص تقلب	Fraud Detection
توزیع کد	Handing over Code
تله عسل	honeypot
سرویس‌های هویت و ویژگی	Identity and Attribute Services (IdAS)
صدور هویت	Identity Issuing
گواهی مجدد هویت	Identity Recertification
سرویس‌های تلفیق هویت	Identity Resolution Services
لغو هویت	Identity Revocation
مدیریت هویت، دسترسی و حق	Identity, Access, and Entitlement Management
قابل استفاده	In motion
مدیریت حادثه	Incident Management
زیرساخت	infrastructure
اعتبارسنجی ورودی و رمزنگاری خروجی	Input Validation and Output Encoding
قابلیت همکاری	Interoperability
وقفه	Intrupt

فارسی	لاتین
تشخیص نفوذ	Intrusion Detection
چارچوب معماری سازمانی ایران	Iran Enterprise Architecture Framework (IEAF)
ثبت وقایع	Logging
مدل داده منطقی	Logical data model
دست دادن	Loss
بدافزارها	Malware
فراداده	Metadata
میان‌افزار	Middleware
بحرانی از لحاظ مأموریت	Mission-critical
پیمانه‌ای	Modularity
غیرحیاتی	Non-critical
جریان های ناهنجاری	Non-normative flow
جریان هنجار	Normative flow
باز بودن	Openness
یتیم	Orphan
بسته	Package
وصله	Patch
محتوا	Payload
افراد	People
اطلاعات شناسایی شخصی	Personally identifiable information
مدل داده فیزیکی	Physical data model
پذیرش سیاست	Policy Adoption
تألیف سیاست	Policy Authoring
درک سیاست	Policy Awareness
توسعه سیاست	Policy Deployment
عمومی کردن سیاست	Policy Socialization
حریم خصوصی	Privacy
تخصیص	Provisioning
ارائه‌دهنده‌ی ابر عمومی	Public cloud provider
سامانه بازشناسی با امواج رادیویی	Radio-frequency identification (RFID)
بی‌درنگ	Real-time
سابقه	Record

فارسی	لاتین
تخصیص انتشار	Release Provisioning
اصلاح	Remediation
خطر، مخاطره	Risk
بحرانی از لحاظ ایمنی	Safety-critical
شِما	Schema
امنیت به طور پیش‌فرض	Security by Default
همبستگی رویدادهای امنیتی	Security Event Correlation
بررسی سلامت امنیت	Security Healthchecking
درک و بینش امنیتی	Security Intelligence
مدل مرجع امنیت	Security Reference Model
میزخدمت	Service Desk
مدیریت نشست	Session Management
ورود یکپارچه	Single Sign-on
سازمان نرم	Soft Enterprise
پشته	Stack
سامانه سرپرستی و گردآوری داده	Supervisory Control and Data Acquisition (SCADA)
مراقبت و نظارت فیزیکی	Surveillance and Physical Monitoring
تهدید	Threat
کاهش تهدید	Threat Mitigation
توکن- نشانه	Token
فعال‌سازی	Trigger
اعتبارسنجی	Verification
مجازی‌سازی	Virtualization
فناوری‌های مجازی‌سازی	Virtualization Technology
آسیب‌پذیری	Vulnerability
جریان کاری	Workflow