



ارزانی امنیت اطلاعات

نگاهی تحلیلی بر معیارهای سنجش امنیت

نویسنده:

ابوذر عرب سرخی

فریبا غفاری

رضا کلانتری



انتشارات آوای قلم

سرشناسه	: عرب سرخی، ابوذر، ۱۳۶۰ -
عنوان و نام پدیدآور	: ارزیابی امنیت اطلاعات، نگاهی تحلیلی بر معیارهای سنجش امنیت/ نویسندگان ابوذر عرب سرخی، فریبا غفاری. رضا کلاتری
مشخصات نشر	: تهران: آوای قلم، ۱۳۹۹.
مشخصات ظاهری	: ۲۸۲ ص.
شابک	: ۹۷۸-۶۲۲-۶۷۱۰-۶۶-۴
وضعیت فهرست نویسی	: فیپا
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: Computer networks -- Security measures
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: Computer security
موضوع	: فناوری اطلاعات -- تدابیر ایمنی
موضوع	: Information technology -- Security measures
شناسه افزوده	: غفاری، فریبا، ۱۳۶۰ -
رده بندی کنگره	: T۱۰۸۱۰۵/۵۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۶۱۲۹۴۸۴

فایده کتاب:

ارزیابی امنیت اطلاعات، نگاهی تحلیلی بر معیارهای سنجش امنیت

نویسندگان:	ابوذر عرب سرخی	تاریخ نشر:	بهار ۱۳۹۹
ناشر:	انتشارات آوای قلم	نوبت چاپ:	اول
حروفچینی و صفحه‌آرایی:	نیره پارسا	شمارگان:	۲۰۰ جلد
طراحی روی جلد:	نیره پارسا	قیمت:	۴۹۰۰۰ تومان
		شابک:	۹۷۸-۶۲۲-۶۷۱۰-۶۶-۴

آدرس: تهران - میدان انقلاب - خیابان کارگر شمالی - ابتدای خیابان نصرت - کوچه باغ نو - کوچه

داوود آبادی شرقی - پلاک ۴ - زنگ دوم

شماره تماس: ۶۶۵۹۱۵۰۴ تلفکس: ۶۶۵۹۱۵۰۵

وب سایت: www.avapublisher.com

حق چاپ برای پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) محفوظ است.

پیشگفتار

اگر به دنیای اطراف خود بنگریم، شاید استفاده از ابزارهای ارتباطات و فناوری اطلاعات امری بسیار پایه‌ای در زندگی امروز به نظر برسد. در این شرایط دیگر نمی‌توانیم تصور کنیم که اگر برنامه‌های کاربردی امروزی و یا بسیاری از ابزارها نبودند، زندگی بشر در عصر ارتباطات چه شکلی به خود می‌گرفت. فناوری اطلاعات و ارتباطات، همان‌طور که بخشی جدایی‌ناپذیر از زندگی افراد است، به‌عنوان شرط بقا سازمان‌ها در عصر حاضر به‌شمار می‌رود. هر ابزار و موجودیتی می‌تواند در کنار مزایایی که برای انسان فراهم کند، خطراتی را نیز برای او داشته باشد. در مورد ارتباطات و ابزارهای فناوری، این مشکلات در غلغله مشکلات اجتماعی - که مورد بحث این کتاب نبوده و از حوصله آن خارج است - مشکلات امنیتی را نیز بر می‌آورد. این مشکلات امنیتی می‌تواند در قالب افشاء داده‌های کاربران، کلاهبرداری‌ها و... نمایان شود. بنابراین سازمان‌ها تلاش می‌کنند تا امنیت خود را بهبود داده و از این طریق برای مشتریان خود تضمین‌ساری نماید. ارزیابی امنیتی معرف روشی است که به سازمان‌ها این امکان را می‌دهد تا از شرایط امنیتی موجود اطمینان حاصل نموده و راه‌کارها و راهبردهای بهبود آن را به‌دست آورند. ارزیابی امنیتی به‌خودی‌خود به‌جودیت خوش‌تعریفی نیست و مشخص است که باید چیزی در سازمان وجود داشته باشد که ارزیابی شود. این موجودیت با عنوان معیار شناخته می‌شود. چنانچه بیشتر به این فرآیند بیاوریم، مشخص می‌شود که هزاران و شاید میلیون‌ها موجودیت برای ارزیابی در سازمان‌ها وجود دارد. اما آیا تمامی آنها پاسخگو به یک ارزیابی است و سازمان را به هدف مشخص خود می‌رساند؟! بدیهی است که این‌طور نیست. از این‌رو در کتاب حاضر برآنیم تا سازمان‌ها را با معیارهایی آشنا کنیم که می‌تواند آنها را در راستای بهبود امنیت اطلاعات هدایت نماید.

در این راستا، دیدگاه‌ها و نگرش‌های مختلفی وجود دارد. مؤلف با بهره‌گیری از مجموعه این موارد در پی آدرس‌دهی به مسائل امنیتی موجود در سازمان‌ها از طریق ارزیابی امنیتی و معیارهای امنیتی است.

فهرست مطالب

عنوان.....	صفحه.....
فصل اول: مقدمه‌ای بر ارزیابی امنیتی.....	۱۹
۱-۱- مقدمه.....	۲۱
۱-۲- نگاهی گذرا بر مفاهیم پایه امنیت اطلاعات.....	۲۱
۱-۳- تعریف امنیت اطلاعات.....	۲۳
۱-۳-۱- تعریف مفاهیم پایه در امنیت اطلاعات.....	۲۴
۱-۳-۲- حریف، ویژگی‌های امنیتی اطلاعات.....	۲۷
۱-۴- مفهوم حساسی ارزیابی امنیتی.....	۳۰
۱-۵- اهمیت جایگاه ارزیابی امنیتی.....	۳۲
۱-۵-۱- پاسخگویی به سوالات مدیریتی.....	۳۲
۱-۵-۲- بهبود امنیت اطلاعات به صورت نظام‌مند.....	۳۵
۱-۵-۳- تأمین اهداف تطبیق و اطمینان.....	۳۶
۱-۵-۴- تأمین اهداف راهبردی، تاکتیکی و عملیاتی.....	۳۷
۱-۵-۵- پرکردن خلاءهای موجود امنیتی بر اثر عدم توانایی ارزیابی امنیتی.....	۳۸
۱-۵-۶- افزایش سودآوری.....	۳۹
۱-۶- نقش معیارهای امنیتی در فرآیند ارزیابی و چگونگی انتخاب آنها.....	۳۹
۱-۶-۱- فرامعیارهای کورس.....	۴۱
۱-۶-۲- فرامعیارهای پرگمتیک.....	۴۲
۱-۶-۲-۱- پیشگویانه بودن.....	۴۲
۱-۶-۲-۲- مربوط بودن.....	۴۴
۱-۶-۲-۳- عملی بودن.....	۴۴
۱-۶-۲-۴- واقعی بودن.....	۴۵
۱-۶-۲-۵- معنی‌دار بودن.....	۴۶
۱-۶-۲-۶- دقیق بودن.....	۴۶
۱-۶-۲-۷- به‌موقع بودن.....	۴۷
۱-۶-۲-۸- مستقل بودن.....	۴۹
۱-۶-۲-۹- هزینه‌بر بودن.....	۴۹
فصل دوم: دیدگاه‌ها و نگرش‌های مختلف نسبت به ارزیابی امنیتی.....	۵۳
۱-۲- مقدمه.....	۵۵

۸	۲-۲- معرفی معیارهای امنیتی براساس نظر متخصصین یا مراجع امنیتی
۹	۳-۲- معیارهای ارزیابی امنیتی براساس سطح تعریف
۱۰	۱-۳-۲- معیارهای راهبردی، مدیریتی و عملیاتی
۱۱	۱-۱-۳-۲- معیارهای راهبردی
۱۲	۲-۱-۳-۲- معیارهای مدیریتی
۱۳	۳-۱-۳-۲- معیارهای عملیاتی
۱۴	۲-۳-۲- معیارهای ورودی-پردازش خروجی
۱۵	۳-۲- معیارهای بلوغ
۱۶	۳-۲-۱- معیارهای آمادگی
۱۷	۴-۲- معیارهای کارکردی و فرآیندی
۱۸	۲-۴-۲- معیارهای فرآیندی
۱۹	۱-۱-۴-۲- معیارهای مدیریت مخاطره
۲۰	۲-۱-۴-۲- معیارهای خزشی-عملی بودن امنیت اطلاعات
۲۱	۳-۱-۴-۲- معیارهای حکمرانی-سیاست و سازماندهی امنیتی
۲۲	۴-۱-۴-۲- معیارهای مدیریت دارایی های اطلاعاتی
۲۳	۵-۱-۴-۲- معیارهای مدیریت تداوم کار
۲۴	۶-۱-۴-۲- معیارهای تطابق و اطمینان
۲۵	۷-۱-۴-۲- معیارهای کارایی و اثربخشی
۲۶	۸-۱-۴-۲- معیارهای صریح و مستقیم
۲۷	۹-۱-۴-۲- معیارهای پایداری
۲۸	۲-۴-۲- معیارهای کارکردی
۲۹	۱-۲-۴-۲- معیارهای امنیتی منابع انسانی
۳۰	۲-۲-۴-۲- معیارهای امنیت فیزیکی
۳۱	۳-۲-۴-۲- معیارهای امنیت فناوری اطلاعات
۳۲	۴-۲-۴-۲- معیارهای کنترل دسترسی
۳۳	۵-۲-۴-۲- معیارهای امنیت نرم افزار
۳۴	۶-۲-۴-۲- معیارهای مدیریت رخداد
۳۵	۵-۲- دسته بندی معیارها براساس قابلیت و نوع سنجش
۳۶	۱-۵-۲- معیارهای کمی
۳۷	۲-۵-۲- معیارهای کیفی
۳۸	۳-۵-۲- معیارهای ترکیبی

عنوان	صفحه
فصل سوم: متخصصین حوزه امنیت و نگاه به معیارهای امنیتی	۸۹
۱-۳-۱- مقدمه	۹۱
۲-۳-۱- معیارهای امنیتی پرگمتیک از منظر پروتبی	۹۱
۱-۳-۲- مدیریت مخاطره امنیت اطلاعات	۹۲
۱-۳-۲-۱- تعداد مخاطره‌های برطرف/ درمان نشده در سطوح مختلف	۹۲
۲-۳-۲-۱- انحراف بودجه امنیت اطلاعات	۹۳
۳-۳-۱- آسیب‌پذیری یا شکنندگی فرآیند یا سیستم	۹۳
۲-۳-۴- تعداد آسیب‌پذیری‌هایی که وصله امنیتی برای آن‌ها نصب نشده	۹۳
۲-۳-۵- درجه مخاطره‌های امنیت اطلاعات	۹۴
۱-۳-۶- میزان هزینه بالقوه برای مخاطره‌های برطرف نشده/ جنبی	۹۵
۲-۳-۷- اخذ کوتاه‌نگ	۹۵
۲-۳-۸- تغییر سطح آ‌وش‌های شبکه	۹۶
۲-۳-۹- همگنی فنی و سازمانی	۹۶
۲-۳-۱۰- درصد کنترل‌هایی که طبق تعریف درست کار می‌کنند	۹۷
۲-۳-۱۱- میزان پوشش بیمه ارمان در تقابلاً بیمه سالانه	۹۷
۲-۳-۱۲- تعداد حمله‌ها	۹۷
۲-۳-۲- معیارهای خط‌مشی امنیتی	۹۷
۲-۳-۱-۲- تعداد خط‌مشی‌ها، استانداردها، رویه‌ها، معیارهای امنیتی دارای مسئول مشخص	۹۸
۲-۳-۲-۲- قابلیت رصد خط‌مشی‌ها، کنترل‌ها، اهداف، استانداردها و رویه‌ها	۹۸
۲-۳-۲-۳- تعداد عملیات مهم که دارای رویه‌های امنیتی مستند و آزموده شده هستند	۹۹
۲-۳-۲-۴- فراگیر بودن پوشش خط‌مشی امنیتی	۹۹
۲-۳-۲-۵- پوشش خط‌مشی توسط چارچوب‌های امنیتی	۹۹
۲-۳-۲-۶- تعداد یا نسبت خط‌مشی‌های امنیتی که مخاطره‌های مانا را آ‌درس‌دهی می‌کند	۱۰۰
۲-۳-۲-۷- کیفیت خط‌مشی‌های امنیتی	۱۰۰
۲-۳-۲-۸- درصد خط‌مشی‌های امنیتی که به‌صورت شفاف به هدف‌های کنترلی نگاشت شده‌اند	۱۰۰
۲-۳-۲-۹- عامل ضربه	۱۰۱
۲-۳-۲-۱۰- تعداد خط‌مشی‌هایی که در زمان مقرر بازبینی نشده‌اند	۱۰۱
۲-۳-۲-۱۱- رتبه خوانایی فیلش-کین‌ساید برای خط‌مشی‌های امنیت	۱۰۲
۲-۳-۲-۱۲- تعداد یا نسبت خط‌مشی‌های امنیتی شفاف	۱۰۲
۲-۳-۲-۱۳- درصد خط‌مشی‌های امنیتی مبتنی بر استانداردهای مستندسازی	۱۰۲

عنوان	صفحه
۳-۲-۲-۱۴- تعداد خط‌مشی‌های ناسازگار با سایر خط‌مشی‌ها	۱۰۳
۳-۲-۳- حکمرانی، مدیریت و سازماندهی امنیت	۱۰۳
۳-۲-۳-۱- کیفیت معیارهای امنیتی مورد استفاده	۱۰۳
۳-۲-۳-۲- درصد کنترل‌های امنیتی که به‌درستی عمل نمی‌کنند	۱۰۴
۳-۲-۳-۳- امنیت اطلاعات در سطوح بالا	۱۰۴
۳-۲-۳-۴- درصد کنترل‌های امنیتی که به‌طور شفاف به هدف‌های امنیتی نگاشت شده‌اند	۱۰۵
۳-۲-۳-۵- تعداد کنترل‌هایی که اهداف تعریف‌شده خود را به‌درستی انجام می‌دهند	۱۰۵
۳-۲-۳-۶- نسبت کنترل‌های حیاتی سازگار با خط‌مشی‌های امنیتی	۱۰۵
۳-۱-۳- وضعیت اقتصادی سازمان	۱۰۶
۳-۲-۳-۸- درصد کنترل‌های افزونه یا اضافی	۱۰۶
۳-۲-۳-۹- هدف‌های کنترلی که با اهداف خاص کسب‌وکار ارتباط تنگاتنگی دارند	۱۰۶
۳-۲-۳-۱۰- زمان به‌روزرسانی آخرین حادثه مهم امنیتی	۱۰۷
۳-۲-۳-۱۱- هزینه سالانه کنترل‌های امنیت اطلاعات	۱۰۷
۳-۲-۳-۱۲- تعداد کنترل‌های امنیتی	۱۰۸
۳-۲-۳-۱۳- گستردگی حسابرسی‌های امنیتی	۱۰۹
۳-۲-۳-۱۴- هزینه امنیت اطلاعات	۱۰۹
۳-۲-۳-۱۵- قانون بنفورد	۱۰۹
۳-۲-۳-۱۶- ارزش خالص فعلی	۱۱۱
۳-۲-۳-۱۷- بازگشت سرمایه	۱۱۲
۳-۲-۳-۱۸- نرخ بازده داخلی	۱۱۲
۳-۲-۳-۱۹- دوره بازگشت سرمایه	۱۱۳
۳-۲-۳-۲۰- نرخ رضایت مشتریان مدیریت امنیت اطلاعات	۱۱۳
۳-۲-۳-۲۱- میزان پوشش کنترل‌های امنیت اطلاعات	۱۱۴
۳-۲-۳-۲۲- سطح وضعیت دفاعی	۱۱۴
۳-۲-۳-۲۳- سازگاری کنترل‌ها	۱۱۵
۳-۲-۳-۲۴- حدود و ثغور کارکردهای امنیت اطلاعات	۱۱۵
۳-۲-۳-۲۵- ارزش در معرض خطر	۱۱۵
۳-۲-۳-۲۶- بازگشت سرمایه‌گذاری امنیت	۱۱۶
۳-۲-۳-۲۷- بودجه امنیت به نسبت بودجه فناوری اطلاعات یا برعکس	۱۱۶
۳-۲-۴- معیارهای مدیریت دارایی اطلاعاتی	۱۱۷
۳-۲-۴-۱- تعداد دارایی‌هایی که صاحب ندارند	۱۱۷

عنوان..... صفحه

- ۱۱۷..... ۳-۴-۲- سهم دارایی‌های اطلاعاتی که طبقه‌بندی نشده‌اند
- ۱۱۸..... ۳-۴-۲- مدت زمانی که دارایی‌های اطلاعاتی بدون متولی بوده‌اند
- ۱۱۸..... ۳-۴-۲- جامعیت فهرست دارایی‌های اطلاعاتی
- ۱۱۸..... ۳-۴-۵- ارزش دارایی‌های اطلاعاتی که صاحب آن‌ها مشخص است
- ۱۱۹..... ۳-۴-۶- درصد دارایی‌های اطلاعاتی که براساس طبقه‌بندی- برچسب زده نشده‌اند
- ۱۱۹..... ۳-۲-۵- معیارهای امنیت منابع انسانی
- ۱۱۹..... ۳-۲-۵-۱- سطح آگاهی امنیتی
- ۱۲۰..... ۳-۲-۱- نرخ استعفاء یا غیبت کارمندان
- ۱۲۱..... ۳-۱-۵- میزان انگیزه و روحیه کارمندان
- ۱۲۲..... ۳-۲-۵-۴- میزان تبعیت مدیران از قوانین
- ۱۲۲..... ۳-۲-۵-۵- فرهنگ امنیت سازمان
- ۱۲۲..... ۳-۲-۵-۶- نسبت سرمایه‌های انسانی به کارمندان
- ۱۲۳..... ۳-۲-۵-۷- مشاهده مستقیم یا غیرمستقیم پرسنل در مورد فرهنگ سازمان
- ۱۲۴..... ۳-۲-۵-۸- میزان ترافیک امنیتی در فضای میز پشتیبان
- ۱۲۵..... ۳-۲-۵-۹- فرهنگ/ جهان بینی سازمان
- ۱۲۵..... ۳-۲-۵-۱۰- تغییر کارمندان در مقابل ریزش حساب‌های کاربری
- ۱۲۶..... ۳-۲-۵-۱۱- اختلال عملکردی سازمانی
- ۱۲۷..... ۳-۲-۵-۱۲- روان‌سنجی
- ۱۲۸..... ۳-۲-۶- معیارهای امنیت فیزیکی
- ۱۲۸..... ۳-۲-۶-۱- مصرف انرژی در واحد رایانه به نسبت ظرفیت تهویه هوا
- ۱۲۹..... ۳-۲-۶-۲- فاصله مابین مکان فیزیکی و مکان دسترسی منطقی
- ۱۲۹..... ۳-۲-۶-۳- تعداد نقاط دسترسی ناامن
- ۱۳۰..... ۳-۲-۶-۴- تعداد مخاطره‌های فیزیکی غیرقابل قبول
- ۱۳۰..... ۳-۲-۶-۵- فاصله مابین پارکینگ کارمندان و میهمانان
- ۱۳۰..... ۳-۲-۶-۶- درصد سازه‌هایی که نور خارجی مناسبی دارند
- ۱۳۱..... ۳-۲-۷- معیارهای امنیت فناوری اطلاعات
- ۱۳۱..... ۳-۲-۷-۱- تعداد سیستم‌های آزمون شده و منطبق بر استانداردهای امنیتی
- ۱۳۲..... ۳-۲-۷-۲- زمان مابین تأیید تغییر تا اعمال تغییر
- ۱۳۳..... ۳-۲-۷-۳- همبستگی بین سیستم/ رخدادنگاری‌های پیکربندی با درخواست تغییر مجاز
- ۱۳۳..... ۳-۲-۷-۴- تعداد سیستم‌های اطلاعاتی با پیکربندی ناامن

۳۳	۵-۷-۲-۳- نرخ درخواست‌های تغییر فوری/ اضطراری
۳۴	۶-۷-۲-۳- تعداد کاربران یا توابعی که حقوق دسترسی بالایی دارند
۳۴	۷-۷-۲-۳- بی‌نظمی محتوای رمز شده
۳۵	۸-۷-۲-۳- درصد تغییرهای ناموفقی که به دلایل امنیتی رخ داده‌اند
۳۵	۹-۷-۲-۳- شاخص آسیب‌پذیری
۳۶	۱۰-۷-۲-۳- تأخیرها و ناسازگاری‌ها در نصب وصله‌های امنیتی
۳۶	۱۱-۷-۲-۳- نرخ شهودی تغییر در فناوری اطلاعات
۳۶	۱۲-۷-۲-۳- پیروی از خط‌مشی‌های نصب وصله امنیتی
۳۶	۱۱-۷-۲-۳- تعداد تغییرها
۳۷	۱۴-۷-۲-۳- تعداد ویروس‌های کشف‌شده در فایل‌های کاربران
۳۷	۵-۷-۲-۳- تعداد بیهرها در قوانین دیواره‌آتش
۳۷	۱۶-۷-۲-۳- رخدادهای مشتریان
۳۸	۸-۲-۳- معیارهای کنترل دسترسی
۳۸	۱-۸-۲-۳- تعداد پیام‌ها دریافتی در سیستم اعلام هشدار/ رخدادنگاری مرکزی
۳۹	۲-۸-۲-۳- مدت‌زمان سپری‌شده از آخرین بازبینی ماتریس کنترل دسترسی سیستم‌ها
۳۹	۳-۸-۲-۳- تعداد حساب‌های کاربری که بر اساس خط‌مشی‌ها غیرفعال شده‌است
۳۹	۴-۸-۲-۳- نرخ تشخیص ناهنجاری‌های دسترسی
۴۰	۵-۸-۲-۳- پوشش و جزئیات ماتریس کنترل دسترسی و طبقی برای برنامه‌های کاربردی
۴۰	۶-۸-۲-۳- وضعیت توسعه ماتریس‌های کنترل دسترسی و سطوحی برای برنامه‌های کاربردی
۴۰	۷-۸-۲-۳- کیفیت کنترل‌های شناسایی و احراز هویت
۴۱	۸-۸-۲-۳- نسبت واحدهای کسب‌وکار که روش‌های شناسایی و احراز هویت خود را آزمایش نموده‌اند
۴۱	۹-۸-۲-۳- تعداد دفعه‌هایی که دارایی‌ها بدون احراز هویت در دسترس افراد/ سیستم‌های غیرمجاز قرار گرفته‌اند
۴۱	۹-۲-۳- معیارهای امنیت نرم افزار
۴۱	۱-۹-۲-۳- درصد کنترل‌هایی که به‌صورت واقعی آزمون شده‌اند
۴۲	۲-۹-۲-۳- سطح تضمین کیفیت نرم‌افزار
۴۳	۳-۹-۲-۳- کیفیت امنیت سیستم که از طریق آزمون مشخص شده‌است
۴۳	۴-۹-۲-۳- سطح امنیت اطلاعات موجود در تضمین کیفیت نرم‌افزار
۴۴	۵-۹-۲-۳- سطح تضمین کیفیت نرم‌افزار موجود در امنیت اطلاعات
۴۴	۶-۹-۲-۳- درصد پیکربندی‌هایی که در راستای خدمات کارایی و امنیت اعمال می‌شوند
۴۴	۷-۹-۲-۳- درصد کنترل‌های فنی که به‌طور امن شکست می‌خورند

عنوان..... صفحه

- ۳-۲-۸- تعداد انحراف‌های شناسایی شده مابین فایل پیکربندی و پیکربندی واقعی دارایی‌ها..... ۱۴۵
- ۳-۲-۱۰- معیارهای مدیریت حوادث..... ۱۴۵
- ۳-۲-۱۰-۱- زمان صرف‌شده برای ترمیم حادثه‌های امنیتی..... ۱۴۶
- ۳-۲-۱۰-۲- فاصله زمانی مابین وقوع و تشخیص حادثه..... ۱۴۶
- ۳-۲-۱۰-۳- درصد حادثه‌هایی که مقصر اصلی آن کشف شده‌است..... ۱۴۶
- ۳-۲-۱۰-۴- هزینه‌های تجمیعی حادثه‌های امنیت اطلاعات..... ۱۴۷
- ۳-۲-۱۰-۵- تعداد کل رویدادها و حادثه‌های امنیت اطلاعات..... ۱۴۸
- ۳-۲-۱۰-۶- تعداد حادثه‌های امنیتی که قابلیت کنترل، پیش‌گیری یا مقابله با آن‌ها وجود دارد..... ۱۴۸
- ۳-۲-۱۰-۷- تأثیرهای غیرمالی حادثه‌های امنیتی..... ۱۴۹
- ۳-۲-۱۱- مدارها، تداوم کسب‌وکار..... ۱۴۹
- ۳-۲-۱۱-۱- میزان پیش‌تحلیل پیامدهای کسب‌وکار..... ۱۴۹
- ۳-۲-۱۱-۲- درصد امنیت‌ای مهم دارای سازمان‌دهی مناسب در حوزه تداوم کسب‌وکار..... ۱۴۹
- ۳-۲-۱۱-۳- درصد رویه‌های کسب‌وکار که هدف‌های زمان‌بازایی و نقطه‌بازایی تعریف‌شده‌ای دارند..... ۱۵۰
- ۳-۲-۱۱-۴- وضعیت نگهداری برنامه‌های تداوم کسب‌وکار..... ۱۵۱
- ۳-۲-۱۱-۵- نتایج آزمون بازایی برنامه..... ۱۵۱
- ۳-۲-۱۱-۶- زمان روشن‌بودن..... ۱۵۲
- ۳-۲-۱۱-۷- ظرفیت و کارایی فناوری اطلاعات..... ۱۵۳
- ۳-۲-۱۱-۸- نگاشت فرآیندهای حیاتی به برنامه‌های بازایی، تداوم کسب‌وکار..... ۱۵۳
- ۳-۲-۱۱-۹- هزینه تداوم کسب‌وکار..... ۱۵۴
- ۳-۲-۱۱-۱۰- تعداد سیستم‌های حساس منطبق بر الزام‌های کنترل امنیت..... ۱۵۴
- ۳-۲-۱۲- معیارهای انطباق و اطمینان امنیت..... ۱۵۵
- ۳-۲-۱۲-۱- تفکیک استثناءها و تبصره‌ها..... ۱۵۵
- ۳-۲-۱۲-۲- تعداد و میزان فاجعه‌بار بودن یافته‌های ممیزی، گزارش‌ها، بازبینی‌ها و ارزیابی‌ها..... ۱۵۵
- ۳-۲-۱۲-۳- وضعیت پیروی از قوانین امنیت اطلاعات که از خارج به سازمان تحمیل شده‌اند..... ۱۵۶
- ۳-۲-۱۲-۴- سوابق جریمه‌های عدم انطباق..... ۱۵۷
- ۳-۲-۱۲-۵- تعداد سیستم‌های اعتبارسنجی‌شده امنیتی..... ۱۵۷
- ۳-۲-۱۲-۶- وضعیت پیروی از الزام‌های اجباری داخلی..... ۱۵۷
- ۳-۲-۱۲-۷- تعداد نرم‌افزارهای بدون مجوز نصب‌شده بر روی دستگاه‌ها..... ۱۵۸
- ۳-۲-۱۲-۸- درصد خطمشی‌های امنیتی پشتیبانی‌شده توسط فعالیت‌های تطابقی مناسب..... ۱۵۸
- ۳-۲-۱۲-۹- الگوی تطابق در مواجهه با شرکاء..... ۱۵۸

۱۵۹	۲-۳-۱۰- تعداد یا نرخ عدم انطباق کشف شده خط مشی ها
۱۵۹	۲-۳-۱۱- عامل شرم
۱۵۹	۲-۳-۱۲- درصد خرید نرم افزارهای غیرمجاز
۱۵۹	۲-۳-۱۳- نسبت هزینه خرج شده برای امنیت بر حاصل ضرب تأثیر بالقوه در احتمال وقوع خطر
۱۶۰	۲-۳-۱۴- تعداد لایسنس های خریداری شده بلااستفاده
	۲-۳-۱۵- درصد دارایی های حیاتی موجود بر روی سیستم هایی که به صورت کامل از الزام های
۱۶۰	تعیین شده پیروی نموده اند
۱۶۰	۳-۳- معیارهای مدیریت امنیت اطلاعات از منظر برونی
۱۶۱	۳-۳- معیارهای کارایی عمومی امنیت
۱۶۱	۳-۳-۱- تعداد بسته هایی که توسط دیواره آتش دور ریخته شده اند
۱۶۱	۳-۳-۱-۱- میزان دفع پردازشگر یا پهنای باند
۱۶۲	۳-۳-۱-۳- ضریب باقی ماندن از انبار
۱۶۲	۳-۳-۱-۴- تغییر در سایر فایل ها
۱۶۲	۳-۳-۵- فایل های اضافی موجود بر روی سرور
۱۶۳	۳-۳-۶- تعداد تلاش های ناموفق برای ورود به سیستم
۱۶۳	۳-۳-۷- دسترسی غیرمجاز به وب سایت
۱۶۳	۳-۳-۸- تخلف سرپرست
۱۶۳	۳-۳-۹- تعداد نفوذهای موفق به سیستم ها
۱۶۴	۳-۳-۲- معیارهای کارایی فنی امنیت
۱۶۴	۳-۳-۱-۲- میزان استفاده از/ بهره وری سیستم
۱۶۴	۳-۳-۲-۲- زمان خاموشی
۱۶۴	۳-۳-۲-۳- میزان پیروی از توافقنامه های سطح سرویس
۱۶۵	۳-۳-۲-۴- میزان کارآمدی پالایش هرزنامه
۱۶۵	۳-۳-۵- تعداد حمله های مقابله شده
۱۶۵	۳-۳-۶- زمان های پاسخ به حادثه
۱۶۵	۳-۳-۷- فاصله های زمانی مابین کشف آسیب پذیری و رفع آن
۱۶۶	۳-۳-۸- نرخ شکست در کنترل
۱۶۶	۳-۳-۹- اثربخشی کنترل ها
۱۶۶	۳-۳-۱۰- هزینه عملیاتی کنترل ها
۱۶۶	۳-۳-۱۱- هزینه نگهداری کنترل ها
۱۶۷	۳-۳-۱۲- تأثیر کنترل ها بر روی کسب و کار

عنوان..... صفحه

۱۶۷	۳-۳-۱۳- شاخص‌های کلیدی عملکرد
۱۶۸	۳-۳-۱۴- شاخص‌های کلیدی هدف
۱۶۹	۳-۳-۳- معیارهای ارزیابی مالی
۱۶۹	۳-۳-۱- برآورد خسارت واحد مورد انتظار
۱۷۰	۳-۳-۲- برآورد خسارت سالانه مورد انتظار
۱۷۰	۳-۳-۳- تحلیل مقرون به صرفه بودن
۱۷۰	۳-۳-۴- تحلیل هزینه-منفعت
۱۷۱	۳-۳-۴- تریه و تحلیل درخت خطا
۱۷۱	۳-۳-۵- چارچوب ارزش رقابتی
۱۷۳	۳-۳-۶- ساختار سلسله‌ای
۱۷۳	۳-۴- معیارهای امنیتی از منظر حاکمیت
۱۷۴	۳-۴-۱- معیارهای امنیتی بحالی
۱۷۶	۳-۴-۲- معیارهای امنیتی تدریس و پیش
۱۸۱	۳-۴-۳- معیارهای دسترسی‌پذیری و اطمینان
۱۸۲	۳-۴-۴- مخاطره‌های برنامه‌کاربرد
۱۸۴	۳-۴-۵- معیارهای کارآمدی فرایندها
۱۹۳	فصل چهارم: معیارهای امنیتی مبتنی بر بهترین تجربیات منتشرشده
۱۹۵	۴-۱- مقدمه
۱۹۵	۴-۲- بهترین تجربه‌ها و جایگاه آن‌ها در تعریف معیارهای امنیتی
۱۹۵	۴-۳- معیارهای امنیتی مبتنی بر چارچوب ساسا
۱۹۷	۴-۳-۱- مشخصه‌های کاربر
۱۹۹	۴-۳-۲- مشخصه‌های مدیریتی
۲۰۱	۴-۳-۳- مشخصه‌های عملیاتی
۲۰۲	۴-۳-۴- مشخصه‌های مدیریت مخاطره‌ها
۲۰۵	۴-۳-۵- مشخصه‌های حکمرانی و تنظیم مقررات
۲۰۶	۴-۳-۶- مشخصه‌های راهبرد فنی
۲۰۸	۴-۳-۷- مشخصه‌های راهبرد کسب‌وکار
۲۱۱	۴-۴- معیارهای امنیتی مبتنی بر دیدگاه مؤسسه ملی استانداردها و فناوری
۲۱۱	۴-۱- بودجه بخش امنیت
۲۱۱	۴-۲- نرخ مدیریت آسیب‌پذیری

عنوان	صفحه
۳-۴-۴- وضعیت کنترل دسترسی	۱۲
۴-۴-۴- وضعیت آموزش و آگاهی بخشی	۱۲
۵-۴-۴- وضعیت ممیزی و حسابرسی	۱۲
۶-۴-۴- وضعیت گواهینامه، اعتبارنامه و ارزیابی امنیتی	۱۳
۷-۴-۴- وضعیت مدیریت پیکربندی	۱۳
۸-۴-۴- وضعیت برنامه ریزی اقتصادی	۱۳
۹-۴-۴- وضعیت شناسایی و احراز هویت	۱۴
۱۰-۴-۴- وضعیت پاسخ به رخداد	۱۵
۱۱-۴-۴- وضعیت نگهداری	۱۵
۱۲-۴-۴- وضعیت محافظت از رسانه	۱۵
۱۳-۴-۴- وضعیت امنیت محیطی و فیزیکی	۱۶
۱۴-۴-۴- وضعیت برنامه بزی	۱۶
۱۵-۴-۴- وضعیت امنیت کد منابع	۱۷
۱۶-۴-۴- وضعیت ارزیابی دوره ها	۱۷
۱۷-۴-۴- وضعیت خرید خدمات سیستم ها	۱۷
۱۸-۴-۴- وضعیت محافظت از سیستم ها	۱۸
فصل پنجم: جمع بندی معیارهای ارزیابی امنیتی	۲۲۱
۱-۵- مقدمه	۲۲۳
۲-۵- نمایه ای انتزاعی از معیارهای امنیتی	۲۲۴
پیوست الف	۲۵۱
مروری اجمالی بر روش های ارزیابی مخاطره	۲۵۱
فهرست واژگان	۲۶۳
مراجع	۲۸۱