

18V7077

السلامة

مدیریت امنیت اطلاعات

تالیف و تدوین

دکتر ناصر مدیری

مہندس مریم جدی



Publication

Mehregane Ghalam

سرشناسه	: مدیری، ناصر، ۱۳۴۱
عنوان و نام پدیدآور	: مدیریت امنیت اطلاعات/ تالیف و تدوین ناصر مدیری، مریم جدی.
مشخصات نشر	: تهران: مهرگان قلم، ۱۳۹۵.
مشخصات ظاهری	: ۳۱۰ص: مصور.
شابک	: ۹۷۸-۶۰۰-۶۲۳۶-۹۳-۳
وضعیت فهرست نویسی	: فیپا
یادداشت	: واژه نامه.
یادداشت	: نمایه.
موضوع	: کامپیوترها -- کنترل دستیابی
موضوع	: تکنولوژی اطلاعات -- مدیریت
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: شبکه های کامپیوتری -- تدابیر ایمنی
شناسه افزوده	: جدی، مریم، ۱۳۴۲
رده بندی کنگره	: ۱۳۹۵ م۴م/۹/۷۶۷۴ Q
رده دی یویی	: ۰۰۵/۸
شماره شابشناسی ملی	: ۴۵۸۷۱۳۹

نام کتاب : مدیریت امنیت اطلاعات

مولف : ناصر مدیری-مریم جدی

ناشر: مهرگان قلم

نوبت چاپ اول: زمستان ۹۵

شابک: ۹۷۸-۶۰۰-۶۲۳۶-۹۳-۳

تیراژ: ۵۰۰

قیمت: ۳۲۰۰۰ تومان

تکثیر تمام یا قسمتی از اثر بدون مجوز کتبی ناشر ممنوع است و متخلفان به موجب قانون حمایت حقوق مولفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار خواهند گرفت.



Publication Mehregane Ghalam



مرکز بخش

انتشارات مهرگان قلم:

تهران - میدان انقلاب - خیابان کارگر جنوبی - بعد از خیابان وحید نظری - کوچه گشتاب-پلاک ۷ واحد ۲

تلفن تماس: ۰۹۱۲۳۱۴۶۰۵۸ - ۶۶۴۷۷۲۲۴-۵

سه دشواری در کار تالیف وجود دارد:

نوشتن چیزی که قابل نشر باشد،

یافتن مرد شریفی که آنرا نشر دهد،

پیدا کردن مردان و زنان حساس و نکته سنجی که آنرا بخوانند!!

((کولتون))

به نام هستی بخش دانا

تاکنون کتب متعددی در زمینه امنیت اطلاعات در کشور تالیف و ترجمه شده است ولی امروز کتابی که کلیه مباحث پیشرفته در سیستم مدیریت امنیت اطلاعات را به طور جامعی پوشش دهد و مطابق با علم روز دنیا نیز باشد در دسترس نبوده است. پس از سالها تدریس و فعالیت در زمینه امنیت اطلاعات، با توجه به نیاز مبرم جامعه علمی و مسئولین، مصمم شدیم کتابی را در زمینه تالیف و گردآوری، چنین منبع اطلاعاتی، به انجام رسانیم. پرداختن به مطالب و به روز در زمینه سیستم مدیریت امنیت اطلاعات به نحوی که خواننده را به طریقی آگاه روان و تخصصی تا انتها همراه کند از اهم دغدغه های مولفین این کتاب بوده است. فصول کتاب "مهندسی سیستم مدیریت امنیت اطلاعات" در راستای نیل به اهداف ذکرشده نحوی کاملاً مستقل و در عین حال انشعاری به هم پیوسته مطرح شده است.

با توجه به گستردگی این مباحث، در پایان هر فصل، منابعی جهت مطالعه ی بیشتر آورده است. خصوصیت بارز این کتاب، سادگی بیان به همراه استفاده از شکل ها و مثالهای ملموس جهت بهتر مفاهیم در هر مبحث است.

مطالب مطرح شده در هر فصل:

- ♦ فصل اول، امنیت اطلاعات
- ♦ فصل دوم، سیاست های امنیتی
- ♦ فصل سوم، حاکمیت فن آوری
- ♦ فصل چهارم، حاکمیت امنیت فن آوری
- ♦ فصل پنجم، برنامه جامع مدیریت فن آوری
- ♦ فصل ششم، استانداردهای سری IEC/ISO27000

- ♦ فصل هفتم، استاندارد 27001 IEC/ISO
- ♦ فصل هشتم، استاندارد 27002 IEC/ISO
- ♦ فصل نهم، پروسه سیستم مدیریت امنیت اطلاعات

امید است این کتاب بتواند در خدمت دانشجویان رشته‌های مختلف علوم کامپیوتر قرار گیرد.
در خاتمه بر خود لازم می‌دانیم از تمامی عزیزی که به نوعی در گردآوری مطالب این کتاب ما را یاری رساندند کمال تشکر و قدردانی را بعمل آوریم.
بی‌صبرانه منتظر نظرات، انتقادات و پیشنهادات شما هستیم.

پست الکترونیکی اندیس نظرات:

info@27000.ir
www.27000.ir

ناصر مدیری - مریم جدی

فهرست مطالب

14	1. امنیت اطلاعات
14	1.1. خلاصه فصل
14	1.2. مفاهیم بنیادی در امنیت اطلاعات
15	1.3. امنیت اطلاعات
17	1.4. پروسه امنیت اطلاعات
17	1.5. مهندسی امنیت
19	1.6. اصول مهندسی امنیت
20	1.7. چرخه حیات مهندسی امنیت
20	1.7.1. سلسله مراتب اهداف، استراتژی و خط مشی
21	1.7.2. جنبه‌های عملیاتی امنیت سازمان
22	1.8. مدیریت امنیت اطلاعات
22	1.9. ارزیابی کیفیت مهندسی امنیت
24	1.10. متدولوژی
26	1.11. فرآیندهای سیستم مهندسی امنیت
27	1.12. سؤالات متداول
27	1.13. منابعی برای مطالعه بیشتر
30	2. سیاست‌های امنیتی
30	2.1. خلاصه فصل
30	2.2. خط مشی امنیتی چیست؟
31	2.3. سیاست امنیتی چیست؟
33	2.4. اجزاء خط مشی امنیتی
35	2.5. سؤالات متداول
35	2.6. منابعی برای مطالعه بیشتر
38	3. حاکمیت فن آوری
38	3.1. خلاصه فصل
39	3.2. خصیصه‌های حاکمیت مطلوب
40	3.3. مفهوم حاکمیت فناوری اطلاعات

42	3. اهمیت حاکمیت فناوری اطلاعات
43	3. تعاریف مختلف از حاکمیت فناوری اطلاعات
44	3. ضرورت حاکمیت فناوری اطلاعات
45	3. اهمیت متریک‌های کارایی برای حاکمیت فناوری
46	3. محدودیت حاکمیت فناوری اطلاعات
46	3. نواحی تمرکز حاکمیت فناوری اطلاعات
47	3.1 معماری‌های حاکمیت فناوری اطلاعات
48	3.10.1 3. معرفی معماری COBIT
50	3.10.2 3. معرفی معماری ITIL
53	3.1.1 منشأ ITIL چیست؟
53	3.1.1 نسخه‌های مختلف ITIL
55	3.1.1 مشخصه‌های کلیدی ITIL
56	3.1.1 موجودیتهای ITIL
56	3.1.1 مزایای کاربرد ITIL در سازمان
56	3.1.1 مایل استونهای مهم پنج گانه در تحقق موفق ITIL
56	3.1.1 سؤالات متداول
58	3.1.1 منابعی برای مطالعه بیشتر
60	4. حاکمیت امنیت فن آوری
60	4. خلاصه فصل
61	4. تعریف برنامه ریزی استراتژیک فناوری اطلاعات
62	4. ضرورت تدوین برنامه استراتژیک فناوری اطلاعات
62	4. مزایای تدوین برنامه استراتژیک
63	4. فرآیند برنامه ریزی استراتژیک فناوری اطلاعات
66	4. مشکلات برنامه ریزی استراتژیک فناوری اطلاعات
66	4. سؤالات متداول
66	4. منابعی برای مطالعه بیشتر
68	5. برنامه جامع مدیریت فن آوری
68	5. خلاصه فصل
69	5. طرح جامع فناوری اطلاعات و ارتباطات
74	5. اهداف طرح جامع فناوری اطلاعات و ارتباطات

75	5.4. اصول حاکم بر طرح
76	5.5. متدولوژی طرح جامع
77	5.6. تدوین طرح جامع فناوری اطلاعات
78	5.7. فرآیند تدوین طرح جامع
78	5.8. سیاست‌های اصلی طرح جامع فناوری اطلاعات
78	5.9. مراحل تدوین طرح جامع
80	5.10. نکات قابل تأمل
82	5.11. سوابق متداول
82	5.12. منابع برای مطالعه بیشتر
84	6. استانداردهای سری ISO/IEC 27000
84	6.1. خلاصه فصل
84	6.2. مروری بر استانداردهای BS 7900
84	6.3. تاریخچه استانداردهای BS 7900
85	6.4. نحوه عملکرد استانداردهای سری ISO/IEC 27000
85	6.5. ISO/IEC 27000
87	6.6. ارتباط بین خانواده استانداردهای سری ISO/IEC 27000
87	6.7. اهم مسائل در استانداردهای سری IEC/ISO 27000
88	6.8. ارتباط مهندسی امنیت و استاندارد 27000
89	6.9. 27001: نیازمندی‌های ISMS
89	6.10. 27002: موارد کاربردی ISMS
89	6.11. 27003: راهنمای پیاده‌سازی ISMS
90	6.12. 27004: اندازه‌گیری و تعیین سطح ISMS
90	6.13. 27005: اندازه‌گیری و تعیین سطح ISMS
90	6.14. 27006: نیازمندیهای بازرسی و تصدیق ISMS
90	6.15. 27007: راهنمای میزان ISMS
90	6.16. 27008: راهنمای میزان کنترل‌های ISMS
91	6.17. 27010: راهنماهای ISMS برای ارتباطات بین بخش
91	6.18. 27011: راهنمای برای تأمین ارتباطات راه دور سازمانها
91	6.19. 27013: راهنماهایی برای پیاده‌سازی یکپارچه 27001 و 20000-1
91	6.20. 27014: چارچوب حاکمیت امنیت اطلاعات

91	27015.6: راهنمای ISMS برای خدمات مالی و بیمه‌ای
92	27034.6: راهنمای امنیت برنامه کاربردی
92	27033.6: استاندارد چندبخشی
94	27036.6: راهبردهای امنیتی برای ارتباطات خارج از سازمان
96	6: سوالات متداول
96	6: منابعی برای مطالعه بیشتر
98	استاندارد ISO/IEC 27001
98	خلاصه فصل
98	آشنایی با استاندارد ISO/IEC 27001
99	فواید استاندارد ISO/IEC 27001
100	مزایای استاندارد ISO/IEC 27001
101	BS7799 / ISO 27001
101	معرفی سه مؤلفه اصلی حفاظت اطلاعات (CIA)
102	استاندارد ISO/IEC 27001، پردازش مدیریت داده‌ها
102	همسویی با سایر استانداردهای سیستم مدیریت
102	ISO 27001 و مدیریت آن
104	7: متدولوژی ISO/IEC 27001
104	7: گامهای الزامی در پیاده‌سازی ISO/IEC 27001
105	7: ساختار ISO/IEC 27001
106	7: پروسه اجرای ISO/IEC 27001
106	7: بکارگیری ISO 9001 برای پیاده‌سازی ISO 27001
108	7: FAQهایی برای ISO/IEC 27001
108	7: حوزه‌های مدیریت اطلاعات
108	7: حوزه اول - خط مشی امنیتی
109	7: اجزاء خط مشی امنیتی
110	7: حوزه دوم - سازماندهی امنیت اطلاعات
110	7: حوزه سوم - مدیریت دارائی‌ها
111	7: حوزه چهارم - امنیت منابع انسانی
112	7: حوزه پنجم - امنیت محیطی و فیزیکی
113	7: حوزه ششم - مدیریت اطلاعات و ارتباطات

115	7.24. حوزه هفتم - کنترل دسترسی
116	7.25. حوزه هشتم - تهیه، نگهداری و توسعه سیستم
117	7.26. حوزه نهم - مدیریت حوادث امنیت اطلاعات
118	7.27. حوزه دهم - طرح تداوم کسب و کار
118	7.28. حوزه یازدهم - مطابقت با قوانین
119	7.29. گامهای مهم در پیاده سازی و اخذ گواهینامه 27001
119	7.30. فرآیند دریافت گواهی ISO/IEC 27001
120	7.31. سمالات متداول
120	7.32. منابع برای مطالعه بیشتر
22	8. استاندارد ISO/IEC 27002
122	8.1. خلاصه فصل
122	8.2. استاندارد ISO/IEC 27002
123	8.3. حوزه استاندارد
123	8.4. حوزه های مدیریت اطلاعات ISO/IEC 27002
123	8.5. هدف و دیدگاه استاندارد
125	8.6. سازگاری با سایر استانداردهای سری
125	8.7. کاربرد
125	8.8. واژگان و تعاریف
127	8.9. استاندارد ملی
129	8.10. سرفصلها
129	8.11. معرفی استاندارد ISO/IEC 27005
130	8.12. پروسه مدیریت ریسک و استاندارد ISO 27005
131	8.13. فلوچارت مدیریت ریسک توسط ISO/IEC 27005
131	8.14. سوالات متداول
132	8.15. منابعی برای مطالعه بیشتر
34	9. پروسه سیستم مدیریت امنیت اطلاعات
134	9.1. خلاصه فصل
135	9.2. سیستم مدیریت امنیت اطلاعات
136	9.3. سیستم مدیریت امنیت اطلاعات
137	9.4. اهداف کلان سیستم مدیریت امنیت اطلاعات

138	9. دامنه و راهبردهای سیستم مدیریت امنیت اطلاعات
139	9. هدف سیستم مدیریت امنیت اطلاعات
139	9. استانداردهای مدیریت امنیت اطلاعات
139	9.7.1. رهیافت استفاده از استانداردهای مدیریتی
140	9.7.2. مروری بر استانداردهای مدیریت امنیت اطلاعات
143	9. کیفیت سیستم مدیریت امنیت اطلاعات
143	9. اندازه گیری سیستم مدیریت امنیت اطلاعات
144	9.1. تشکیلات تأمین امنیت فضای تبادل اطلاعات
146	9.10.1. شرح وظایف تشکیلات امنیتی
148	9.1. ایجاد سیستم مدیریت امنیت اطلاعات
151	9.1. پیاده سازی و اجرای ISMS
152	9.1. پایش و بازنگری SMS
153	9.1. چرخه استمرار سیستم مدیریت امنیت اطلاعات
163	9.1. مستندات ISMS
163	9.15.1. اهداف، راهبردها و سیاست‌های امنیتی
165	9.15.2. طرح تحلیل مخاطرات امنیتی
166	9.15.3. مستندات مفید
166	9.1. فاکتورهای مهم در موفقیت ISMS
168	9.1. نیازهای ISMS
169	9.1. نگهداری و بهبود ISMS
169	9.1. مشکلات پیاده سازی ISMS
170	9.2. ساختار ISMS
171	9.2. مزایای ISMS
172	9.2. مسئولیتها و تعهدات
173	9.2. مسیر دستیابی به گواهینامه - الزامات گواهینامه
173	9.2. پروسه اخذ گواهینامه ISMS (فازها و وظایف)
176	9.2. FAQ هایی برای ISMS
177	9.2. سؤالات متداول
178	9.2. منابعی برای مطالعه بیشتر

80	1. ضمیمه اول.....
80	فرآیندهای فناوری اطلاعات برای هریک از حوزه های اصلی COBIT.....
82	2. ضمیمه دوم.....
82	استانداردهای سری 27000.....
85	3. ضمیمه سوم.....
85	پیوست اف- اهداف کنترلی و کنترل ها (الزامی).....
09	4. ضمیمه چهارم: 11 حوزه قابل پیاده سازی برای ISMS.....
16	5. ضمیمه پنجم: حوزه دارائی های اطلاعاتی.....
33	6. ضمیمه ششم: مدیریت منابع انسانی.....
47	7. ضمیمه هفتم: مدیریت امنیت فیزیکی و محیطی.....
78	8. ضمیمه هشتم: مدیریت مراد اطلاعات امنیتی.....
98	9. ضمیمه نهم.....
98	واژگان و عبارات (انگلیسی به فارسی).....
303	10. ضمیمه دهم.....
303	فهرست علائم اختصاری.....