ISMS

By:

Information

Security

Management

System

ISMS

By:

آرامش در زندگي بدون امنيت امكانپذير نيست .

همیشه باید نگران باشید

ISMS

By:

ITیک سکه دوروست: هم فرصت است و هم تهدید ! اگر به همان نسبتی که به توسعه و همه گیری اش توجه و تکیه میکنیم به "امنیت" آن توجه نکنیم میتواند به سادگی و در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود.

نیاز روزافزون به استفاده از فناوريهاي نوين در عرصه اطلاعات و ارتباطات، ضرورت استقرار يك نظام مديريت امنيت اطلاعات را بيش از پيش آشكار مي‌نمايد .

ISMS

By:

به طور کلی می توان فرایند امن سازی را در 4 شاخه ی اصلی طبقه بندی کرد :

1- امنیت دررایانه ها

2- امنیت در شبکه ها

3- امنیت در سازمان ها

4-امنیت کاربران

ISMS

By:

ISMS چیست ؟

برگرفته از کلمات زیر و به معناي “سیستم مدیریت امنیت اطلاعات” است .

Information Security Management System

ISMSبه مدیران این امکان را می دهد تا بتوانند امنیت سیستم های خود را با به حداقل رساندن ریسک های تجاری کنترل کنند.

ISMS

By:

سيستم مديريت امنيت اطلاعات (ISMS) راهكار حل مشكلات امنيتی در سيستم‌هاي اطلاعاتي است، يک سيستم جامع امنيتي بر سه پايه بنا مي‌شود:

- بررسی و تحليل سيستم اطلاعاتی
- سياستها و دستورالعملهاي امنيتي
- تكنولوژي و محصولات امنيت
- عوامل اجرايي

ISMS

By:

حفاظت سه بعدی از اطلاعات سازمان

- حفظ محرمانه بودن اطلاعات از طریق اطمینان از دسترسی اطلاعات تنها توسط افراد مجاز.

- حفظ یکپارچگی اطلاعات از لحاظ دقت و کامل بودن و روشهای پردازش
- قابلیت دسترسی اطلاعات و دارایی های مرتبط توسط افراد مجاز در زمان نیاز.

By:

علل بروز مشکلات امنیتی

علل بروز مشکلات امنیتی

By:

- ضعف فناوری
- ضعف پیکربندی
- ضعف سیاست ها

ضعف فناوری

By:

- ضعف پروتکل TCP/IP
- ضعف سیستم عامل
- ضعف تجهیزات شبکه ای

ضعف پیکربندی

By:

- استفاده غیرایمن از account کاربران
- استفاده از system accountکه رمز عبور آنها به سادگی قابل تشخیص است.
- عدم پیکربندی صحیح سرویس های اینترنت
- غیرایمن بودن تنظیمات پیش فرض در برخی محصولات
- عدم پیکربندی صحیح تجهیزات شبکه ای

ضعف سیاست ها

By:

- عدم وجود يك سياست امنيتی مكتوب
- سیاست های سازمانی
- رها کردن مدیریت امنیت شبکه به حال خود
- نصب و انجام تغییرات مغایر با سیاست های تعریف شده
- عدم وجود برنامه ای مدون جهت برخورد با حوادث غیرمترقبه

By:

استانداردهاي ISMS

استانداردهاي ISMS

By:

با ارائه اولين استاندارد مديريت امنيت اطلاعات در سال 1995، نگرش سيستماتيک به مقوله ايمن‌سازي فضاي تبادل اطلاعات شکل گرفت. بر اساس اين نگرش، تامين امنيت فضاي تبادل اطلاعات سازمانها، دفعتا مقدور نمي‌باشد و لازم است اين امر بصورت مداوم در يک چرخه ايمن‌سازي شامل مراحل طراحي، پياده‌سازي، ارزيابي و اصلاح، انجام گيرد.

استانداردهاي ISMS

By:

در تمام استانداردها، نكات زير مورد توجه قرار گرفته شده است:

- ✓تعيين مراحل ايمن‌سازي و نحوه شكل‌گيري چرخه امنيت اطلاعات و ارتباطات سازمان
- ✓جزئيات مراحل ايمن‌سازي و تكنيكهاي فني مورد استفاده در هر مرحله
- ✓ليست و محتواي طرح‌ها و برنامه‌هاي امنيتي موردنياز سازمان
- ✓ضرورت و جزئيات ايجاد تشكيلات سياستگذاري، اجرائي و فني تامين امنيت اطلاعات و ارتباطات سازمان
- ✓كنترل‌هاي امنيتي موردنياز براي هر يک از سيستم‌هاي اطلاعاتي و ارتباطي سازمان

By:

استانداردهاي ISMS

- استاندارد مدیریتی BS7799 موسسه استاندارد انگلیس
- استاندارد مدیریتی ISO/IEC 17799 موسسه بین‌المللی استاندارد
- استانداردهای مدیریتی سری 27000 موسسه بین المللی استاندارد
- گزارش فنی ISO/IEC TR 13335 موسسه بین‌المللی استاندارد
- استاندارد ITBPM
- استانداردامنیتی ACSI33
- استاندارد AS/NZS

استاندارد BS7799 موسسه استاندارد انگلیس

By:

نسخه اول:	BS7799:1	1995
نسخه دوم:	BS7799:2	1999
نسخه آخر:	BS7799:2002	2002

استاندارد BS7799 موسسه استاندارد انگليس-بخش اول

By:

- تدوين سياست امنيتي سازمان
- ايجاد تشكيلات تامين امنيت سازمان
- دسته‌بندي سرمايه‌ها و تعيين كنترل‌هاي لازم
- امنيت پرسنلي
- امنيت فيزيكي و پيرامون

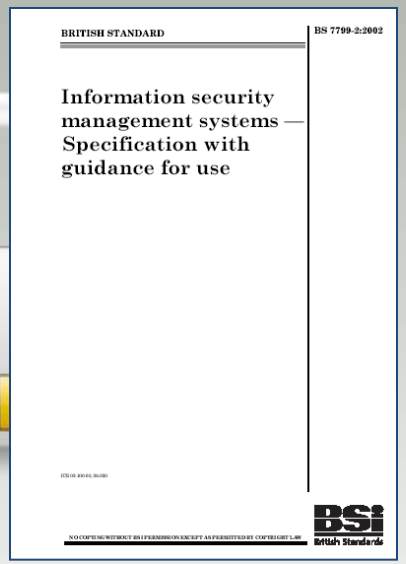
استاندارد BS7799 موسسه استاندارد انگلیس-بخش اول

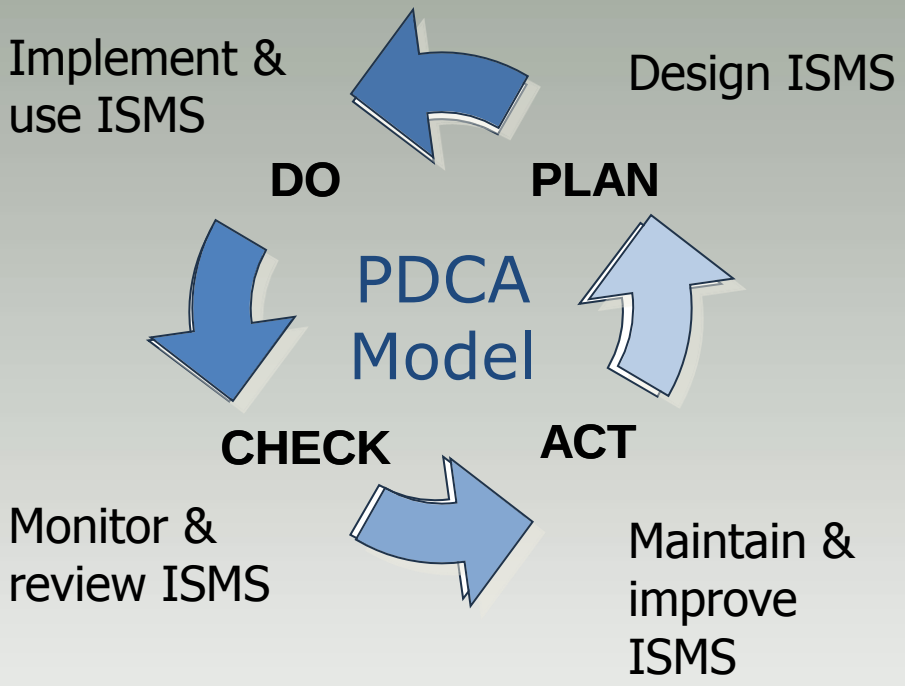
By:

- مديريت ارتباطات
- كنترل دسترسي
- نگهداري و توسعه سيستم‌ها
- مديريت تداوم فعاليت سازمان
- پاسخگوئي به نيازهاي امنيتي

استاندارد BS7799 موسسه استاندارد انگلیس-بخش دوم

By:





Risk based continual improvement framework for information security management

Plan

By:

ISMS را برنامه ریزی کن

این فاز در واقع مرحله مشخص شدن تعاريف اوليه پاده سازي ISMS ميباشد.تهيه سياست هاي امنيتي ،مقاصد،تعريف پردازش هاي مختلف درون سازماني و روتين هاي عملياتي و..در اين مرحله تعريف و پياده سازي ميشوند.

Do

By:

انجام بده (ISMS را پیاده نموده و از آن بهره برداری کن)

پیاده سازي و اجراي سیاست هاي امنیتي،کنترل ها پردازش ها در این مرحله انجام میشود.

در واقع این مرحله اجراي کلیه مراحل فاز اول را طلب میکند.

Check

By:

كنترل كن (ISMS را پايش كرده و مورد بازنگری قرار بده)

در اين مرحله ارزيابي موفقيت پياده سازي سياست هاي مختلف امنيتي،همچنين تجربه هاي عملي و گزارش هاي مديريتي گرد آوري خواهند شد.

Act

By:

رفتار کن (**ISMS** رانگهداری نموده و آنرا بهبود ببخش)

اجراي موارد ترميمي و باز نگري در نحوه مديريت طلاعات،همچنين تصحيح موارد مختلف در اين فاز انجام ميشود.

استاندارد ISO/IEC 17799 موسسه بين‌المللي استاندارد

By:

در سال 2000 ، بخش اول استاندارد BS7799:2 بدون هيچگونه تغييري توسط موسسة بين المللي استاندارد بعنوان استاندارد ISO/IEC 17799 منتشر شد.

استاندارد ISO/IEC 17799 موسسه بين‌المللي استاندارد

By:

- طرح تداوم خدمات تجاري
- كنترل بر نحوه دستيابي به سيستم
- توسعه و پشتيباني سيستم
- ايجاد امنيت فيزيكي و محيطي
- انطباق امنيت

موسسه بين‌المللي استاندارد ISO/IEC 17799 استاندارد

By:

- امنيت كاركنان
- ايجاد امنيت سازماني
- مديريت رايانه و عمليات
- كنترل و طبقه بندي دارايي ها
- امنيت اطلاعاتي

موسسه بين‌المللي استاندارد ISO/IEC TR13335 راهنماي فني

By:

اين گزارش فني در قالب 5 بخش مستقل در فواصل سالهاي 1996 تا 2001 توسط موسسة بين المللي استاندارد منتشر شده است.

در واقع مكمل استانداردهاي مديريتي BS7799 و ISO/IEC 17799 مي باشد .

ISO/IEC TR13335 -بخش اول

By:

در اين بخش كه در سال 1996 منتشر شد، مفاهيم كلي امنيت طلاعات از قبيل سرمايه، تهديد، آسيب پذيري، ريسک، ضربه و ... ، روابط بين اين مفاهيم و مدل مديريت مخاطرات امنيتي، ارائه شده است .

ISO/IEC TR13335 -بخش دوم

By:

این بخش که در سال1997 منتشر شد ، مراحل ايمن سازي و ساختارتشكيلات تامين امنيت اطلاعات سازمان ارائه شده است .

بخش دوم- ISO/IEC TR13335

By:

تعيين اهداف، راهبردها و سياست‌هاي امنيتي فضاي تبادل اطلاعات سازمان

تحليل مخاطرات امنيتي فضاي تبادل اطلاعات سازمان

انتخاب حفاظ ها و ارائه طرح امنيت

پيادەسازي طرح امنيت

پشتيباني امنيت فضاي تبادل اطلاعات سازمان

بخش سوم- ISO/IEC TR13335

در اين بخش كه در سال 1998 منتشر شد، تكنيكهاي طراحي، پياده سازي و پشتيباني امنيت اطلاعات از جمله محورها و جزئيات سياستهاي امنيتي سازمان، تكنيكهاي تحليل مخاطرات امنيتي، محتواي طرح امنيتي، جزئيات پياده سازي طرح امنيتي و پشتيباني امنيت اطلاعات، ارائه شده است.

بخش چهارم- ISO/IEC TR13335

By:

در این بخش که در سال 2000 منتشر شد، ضمن تشریح حفاظهاي فیزیکي، سازماني و حفاظهاي خاص سیستمهاي اطلاعاتي، نحوة انتخاب حفاظهاي مورد نیاز براي تامین هریک از مولفههاي امنیت اطلاعات، ارائه شده است.

بخش پنجم- ISO/IEC TR13335

در اين بخش كه در سال 2001 منتشر شد، ضمن افزودن مقولة ارتباطات و مروري بر بخشهاي دوم تا چهارم اين گزارش فني، تكنيكهاي تامين امنيت ارتباطات از قبيل شبكه‌هاي خصوصي مجازي، امنيت در گذرگاه‌ها، تشخيص تهاجم و كدهاي مخرب، ارائه شده است.

By:

مهندسي امنيت

تعريف مهندسي امنيت

By:

مهندسي امنيت مجموعه فعاليت‌هايي است كه براي حصول و نگهداري سطوح مناسبي از :

-محرمانگي (Confidentiality)

-صحت (Integrity)

-قابليت دسترسي (Availability)

-حساب پذيري (Accountability)

- اصالت (Authenticity)و

- قابليت اطمينان (Reliability)

به صورت قاعده مند در يك سازمان انجام مي‌شود.

تعريف مهندسي امنيت

By:

- محرمانگي: اطلاعات براي افراد، موجوديت‌ها يا فرآيندهاي غيرمجاز در دسترس قرار نگيرد يا افشا نشود.

- صحت : صحت سيستم و صحت داده

صحت داده : داده ها به صورت غير مجاز تغيير پيدا نكنند يا از بين نروند.

صحت سيستم : فعاليت‌هاي مورد انتظار از سيستم بدون عيب و خالي از دستكاري هاي غير مجاز (تعمدي يا تصادفي) در سيستم انجام شود.

- اصالت: هويت واقعي يك موجوديت با هويت مورد ادعا يكسان باشد.

تعريف مهندسي امنيت

By:

- قابليت دسترسي: منابع براي يك موجوديت مجاز در هنگام نياز در دسترس و قابل استفاده باشد.
- حساب پذيري: فعاليت‌هاي موجوديت‌ها در سيستم اطلاعاتي به صورت جداگانه قابل رديابي و بررسي باشد.
- قابليت اعتماد: سازگار بودن رفتارها و نتايج مورد انتظار

اصول مهندسي امنيت

By:

- امنيت فضاي تبادل اطلاعات مفهومي كلان و مبتني بر حوزه هاي مختلف دانش است.

- امنيت هر سيستم تعريف مخصوص به خود دارد .
- امنيت ابزاري براي رسيدن به هدف سيستم است.
- امنيت نسبي است.

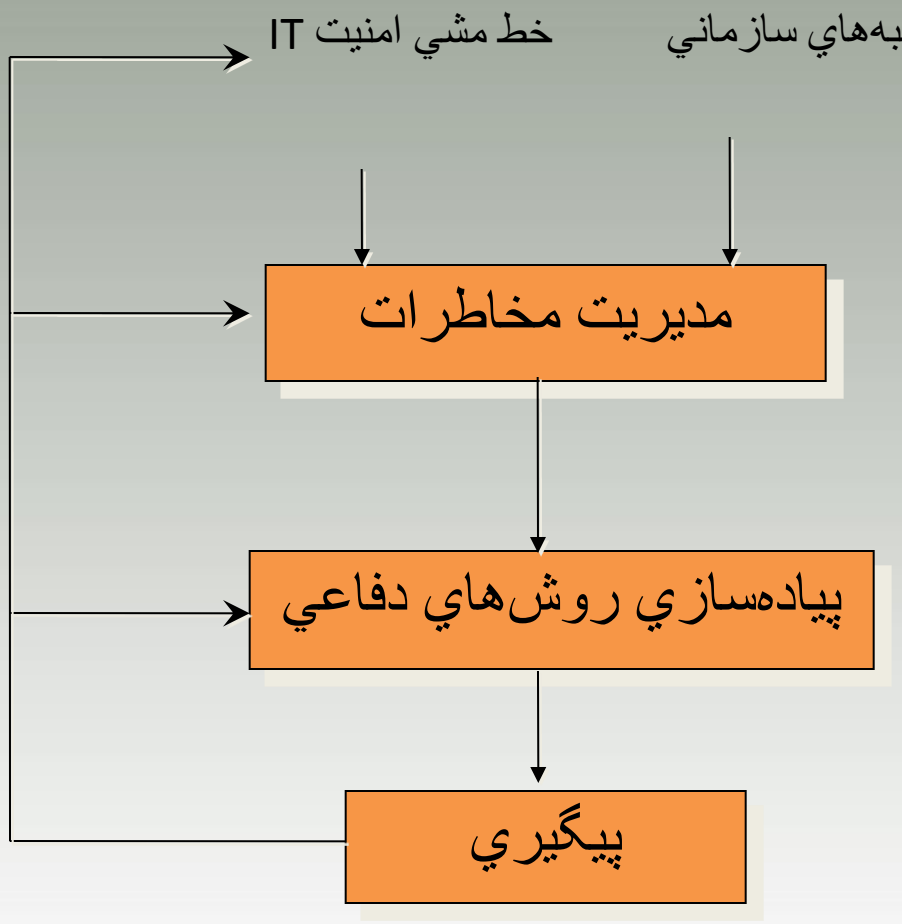
اصول مهندسي امنيت

By:

- امنيت سيستم يك طرح يكپارچه و جامع مي‌طلبد.
- حيطة مسئوليتها و مقررات امنيتي بايد كاملاً شفاف و غيرمبهم باشد.
- طرح امنيتي بايد مقرون به صرفه باشد.
- امنيت هر سيستم توسط عوامل اجتماعي محدود مي‌شود.
- امنيت هر سيستم بايد بطور متناوب مورد ارزيابي مجدد قرار گيرد.

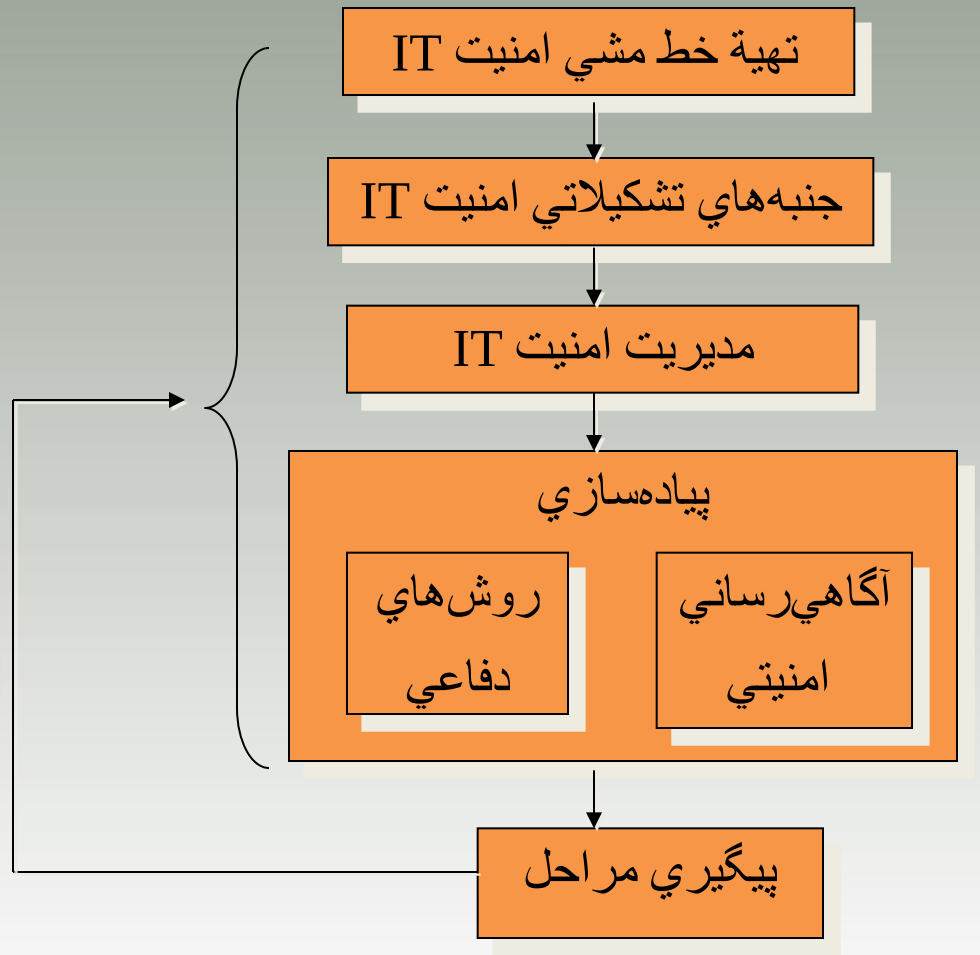
چرخه ی حیات مهندسی امینت

By:



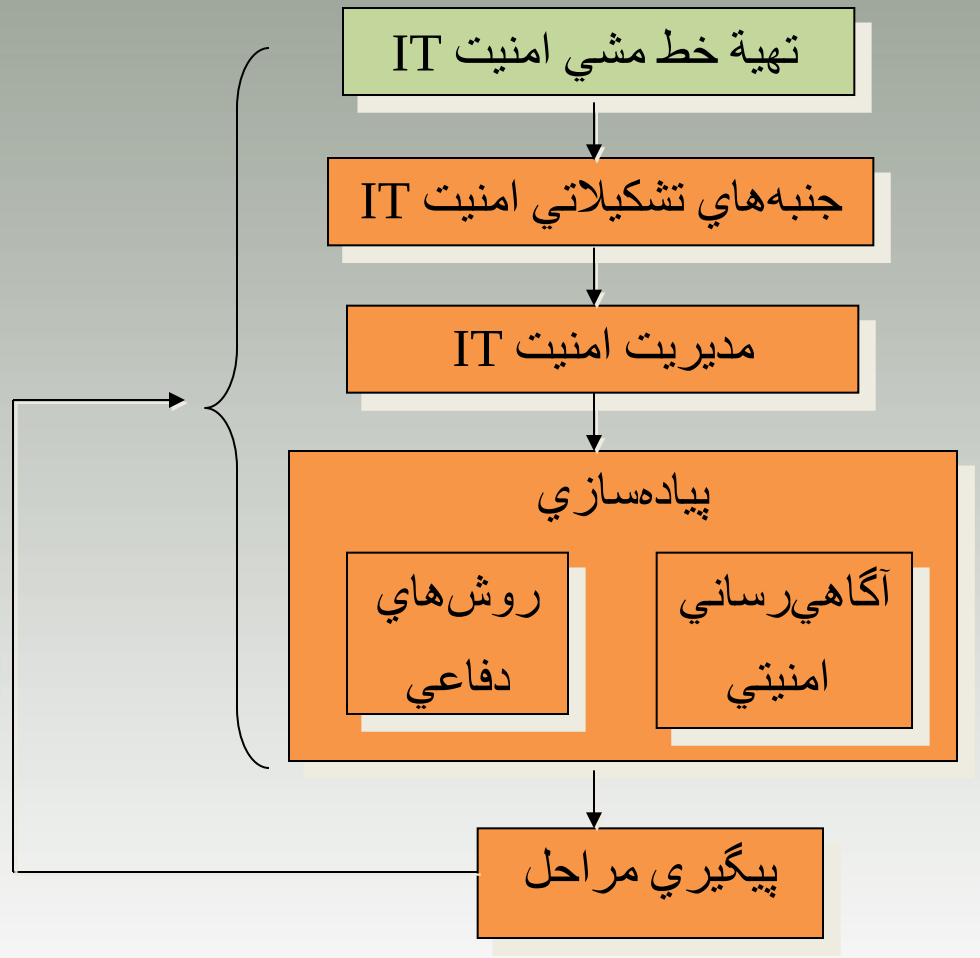
چرخه ی حیات مهندسی امینت

By:



تهية خط مشي امنيت IT

By:



تهية خط مشي امنيت IT

By:

براي ايجاد امنيت در يك سازمان، اولين قدم تدوين اهداف، استراتژي و خط مشي امنيتي سازمان است.

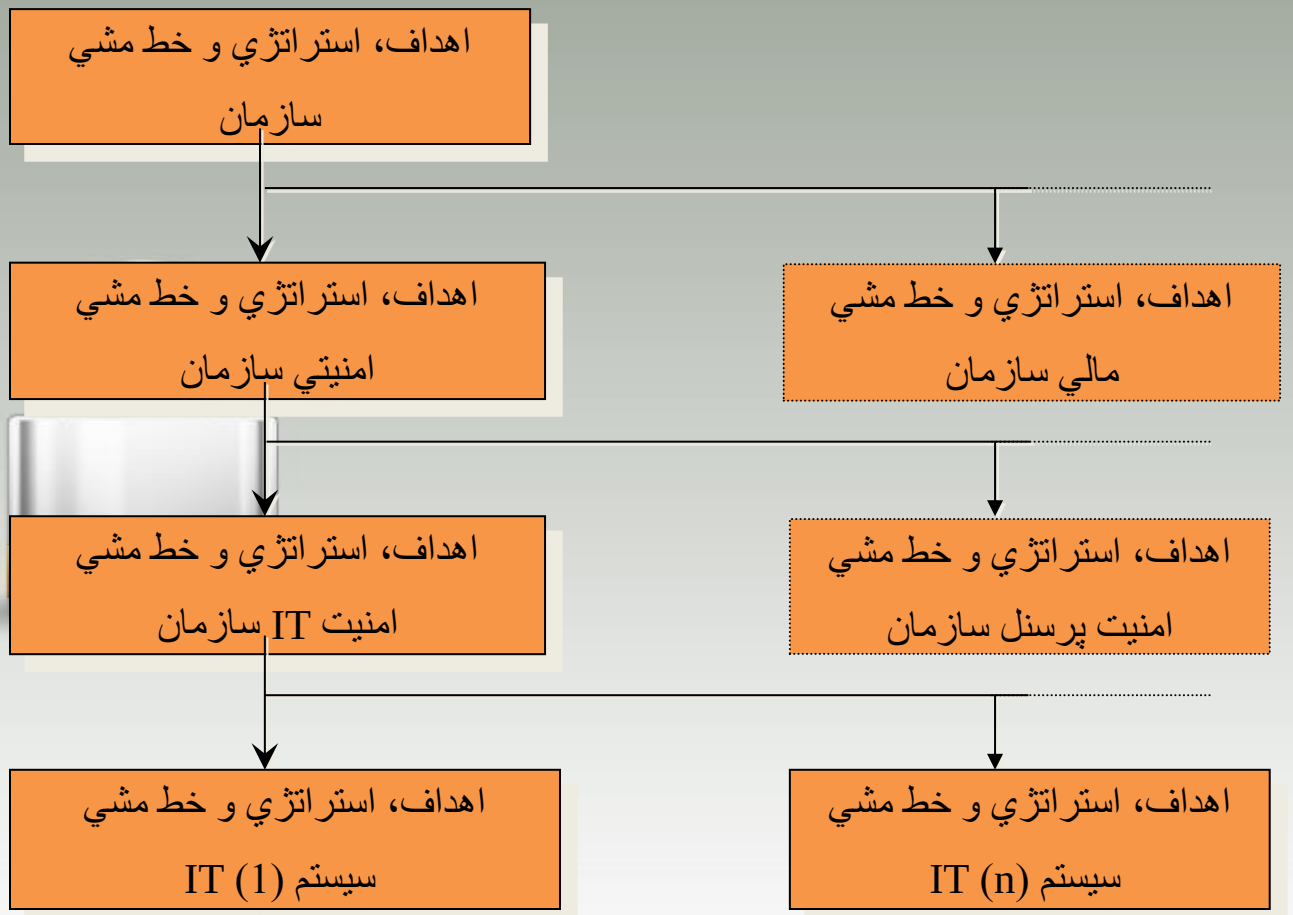
اهداف (Objectives)

استراتژي (Strategy)

خط مشي (Policy)

سلسله مراتب اهداف، استراتژي و خط مشي

By:



جنبه‌هاي تشكيلاتي امنيت IT

By:

- تهية خط مشي امنيت IT
- جنبه‌هاي تشكيلاتي امنيت IT
- مديريت امنيت IT
- پياده‌سازي
  - روش‌هاي دفاعي
  - آگاهي‌رساني امنيتي
- پيگيري مراحل

جنبه‌هاي تشكيلاتي امنيت IT

By:

مديريت سازمان

متصدي امنيت سازمان

دستورالعمل‌ها و
خط مشي امنيتي
سازمانIT

متصدي امنيت IT

متصدي امنيت زير بخش

دستورالعمل‌ها و
خط مشي زيربخش
IT

متصدي امنيت سيستم

دستورالعمل‌ها و
خط مشي امنيتی
سيستم 1 IT

مديريت امنيت IT

By:

تهية خط مشي امنيت IT

جنبه‌هاي تشكيلاتي امنيت IT

مديريت امنيت IT

پياده‌سازي

روش‌هاي دفاعي

آگاهي‌رساني امنيتي

پيگيري مراحل

مديريت امنيت IT

By:

مديريت امنيت اطلاعات بخشي از مديريت اطلاعات است كه وظيفه تعيين اهداف امنيت و بررسي موانع سر راه رسيدن به اين اهداف و ارائه راهكارهاي لازم را بر عهده دارد. همچنين مديريت امنيت وظيفه پياده سازي و كنترل عملكرد سيستم امنيت سازمان را بر عهده داشته و در نهايت بايد تلاش كند تا سيستم را هميشه روزآمد نگه دارد.

مدیریت امنیت IT

By:

مدیریت امنیت IT شامل موارد زیر است:

- مدیریت پیکربندی
- مدیریت تغییرات
- مدیریت مخاطرات

مديريت پيكربندي

By:

فرآيندي است براي حصول اطمينان از اينكه تغييرات در سيستم تأثير كنترل‌هاي امنيتي و به تبع امنيت كل سيستم را كاهش ندهد.

مديريت تغييرات

By:

فرآيندي است كه براي شناسايي نيازمندي‌هاي جديد امنيتي در هنگام بروز تغيير در سيستم IT انجام مي‌شود.

- انواع تغييرات در سيستم IT :

- روال‌هاي جديد
- تجديد سخت‌افزارها
- اتصالات جديد شبكه
- بروز رساني نرم‌افزارها
- كاربران جديد
- ...

مدیریت مخاطرات

By:

یکی از مهمترین قابلیتهای ISMS که در هر سازمانی به فراخور نیاز باید انجام می‌شود، مدیریت مخاطرات یا Risk Management است. ریسک یا مخاطره عبارت است از احتمال ضرر و زیانی که متوجه یک دارایی سازمان (در اینجا اطلاعات) می‌باشد. عدم قطعیت (در نتیجه مقیاس ناپذیری) یکی از مهمترین ویژگیهای مفهوم ریسک است. طبعا این عدم قطعیت به معنای غیر قابل محاسبه و مقایسه بودن ریسکها نیست.

مديريت مخاطرات

By:

- مديريت مخاطرات فرآيندي است براي شناسايي و ارزيابي:

- دارايي‌هاي كه بايستي حفاظت شوند (Assets)
- تهديدات (Threats)
- رخنه‌ها (Vulnerabilities)
- آسيبها (Impacts)
- مخاطرات (Risks)
- روش‌هاي مقابله (Safeguards)
- ريسك باقي مانده (Residual Risks)

مدیریت مخاطرات

By:

By:

تهية خط مشي امنيت IT

جنبه‌هاي تشكيلاتي امنيت IT

مديريت امنيت IT

پياده‌سازي

روش‌هاي دفاعي

آگاهي‌رساني امنيتي

پيگيري مراحل

پيادەسازي

By:

- آگاهي‌رساني امنيتي
- روش‌هاي دفاعي

By:

تهية خط مشي امنيت IT

جنبه‌هاي تشكيلاتي امنيت IT

مديريت امنيت IT

پياده‌سازي

روش‌هاي دفاعي

آگاهي‌رساني امنيتي

پيگيري مراحل

كنترل‌هاي امنيتي

By:

تجربيات, روال‌ها يا مكانيزم‌هاي محافظت در مقابل تهديدات

- كنترل‌هاي امنيتي در حوزه‌هاي زير قابل اعمال هستند :

سخت‌افزار (پشتيباني, كليدها و ...)
نرم‌افزار (امضاء رقمي, ثبت وقايع (Log) , ابزارهاي ضد ويروس)
ارتباطات (فايروال, رمزنگاري)
محيط فيزيكي (نرده و حفاظ و ...)
پرسنل (آگاهي رساني و آموزش, روال‌هاي استخدام, عزل و استعفا و ...)
كنترل استفاده از سيستم‌ها (احراز اصالت, كنترل دسترسي و ...)

كنترل‌هاي امنيتي از يكديگر مستقل نيستند و بايستي آنها را به صورت تركيبي استفاده نمود.

انواع کنترل های امنیتی

By:

- کنترلهاي مديريتي
- کنترلهاي عملياتي
- کنترلهاي فني

کنترل های فنی

By:

سیستم های اطلاعاتی

By:

سیستم عامل : با این که هر سیستم عاملی دارای ضعف های امنیتی مختص به خود است ، ولی عمومیت و رواج يك سیستم عامل می تواند زمینه شناسائی و سوء استفاده از ضعف های امنیتی آن را تسریع نماید . شاید به همین دلیل باشد که ضعف های ویندوز شرکت مایکروسافت سریع تر از سایر سیستم های عامل بر همگان آشکار می شود چراکه اکثر کاربران بر روی کامپیوتر خود از یکی از نسخه های ویندوز این شرکت استفاده می نمایند . شاید بتوان گفت که لینوکس و یا یونیکس نسبت به ویندوز دارای ضعف های امنیتی کمتری می باشند ولی سیستم های عامل فوق نیز دارای ضعف امنیتی مختص به خود می باشند که به دلیل عدم استفاده عام از آنها تاکنون کمتر شناسائی شده اند .

سیستم های اطلاعاتی

By:

پایگاه داده: امنیت پایگاه داده فرآیند حفاظت از داده های سازمان در برابر دسترسی و استفاده غیر مجاز، افشاگری، تخریب و یا تغییر می باشد.

شبكة ارتباطي : تمامی تجهیزات شبکه ای نظیر سرویس دهندگان ، روترها ، سوئیچ ها و نظایر آن دارای برخی ضعف های امنیتی ذاتی می باشند . با تبعیت از يك سیاست تعریف شده مناسب برای پیکربندی و نصب تجهیزات شبکه ای می توان بطرز کاملا" محسوسی آثار و تبعات این نوع ضعف های امنیتی را کاهش داد . نصب و پیکربندی هر گونه تجهیزات شبکه ای می بایست مبتنی بر اصول و سیاست های امنیتی تعریف شده باشد .

By:

تهية خط مشي امنيت IT

جنبه‌هاي تشكيلاتي امنيت IT

مديريت امنيت IT

پياده‌سازي

روش‌هاي دفاعي

آگاهي‌رساني امنيتي

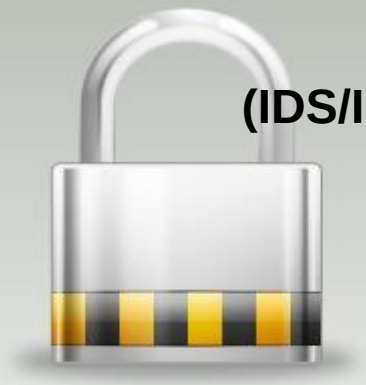
پيگيري مراحل

سرويسهاي اساسي

By:

حفاظت از شبكة خودي

ديواره آتش(Firewall)



سيستم هاي تشخيص و مقابله با نفوذ (IDS/IPS)

ضد ويروس

مانيتورهای Log

سيستمهای فريب

...

سرويسهاي اساسي

By:

ارتباط امن بين‌شبكه‌اي

روش هاي رمزنگاري

شبكه اختصاصي مجازي (VPN)

زير ساخت كليد عمومي (PKI)

امضاء ديجيتالي

...

روش هاي رمزنگاري

By:

رمزنگاري عبارتست از تبديل داده ها به ظاهري كه نهايتا بدون داشتن يک كليد مخصوص قرائت آن غير ممكن باشد.هدف آن حفظ حريم خصوصي است با پنهان نگاه داشتن اطلاعات از افرادي كه نبايد به آنها دسترسي داشته باشند.

شبکه اختصاصي مجازي (VPN)

By:

یک VPN ، شبکه ای اختصاصی بوده که از اینترنت برای ارتباط با سایت های از راه دور و ارتباط کاربران با یکدیگر استفاده می نماید. این نوع شبکه ها بجای استفاده از خطوط واقعی نظیر خطوط Leased ، از یک ارتباط مجازی به کمک اینترنت برای ایجاد شبکه اختصاصی استفاده می کنند .

زير ساخت كليد عمومي (PKI)

By:

PKI (Public Key Infrastructure) به عنوان استانداردي كه عملا براي يكي كردن امنيت محتواي ديجيتالي و فرايند هاي تجارت الكترونيک و همچنين پرونده ها و اسناد الكترونيكي مورد استفاده قرار مي گرفت ظهور كرد.اين سيستم به بازرگانان اجازه مي دهد از سرعت اينترنت استفاده كرده تا اطلاعات مهم تجاري آنان از رهگيري ، دخالت و دسترسي غير مجاز در امان بماند.يک PKI كاربران را قادر مي سازد از يک شبكه عمومي ناامن مانند اينترنت به صورتي امن و خصوصي براي تبادلات اطلاعات استفاده كنند.اين كار از طريق يک جفت كليد رمز عمومي و اختصاصي كه از يک منبع مسؤل و مورد اعتماد صادر شده و به اشتراک گذارده مي شود انجام گيرد .

By:

امضاء ديجيتالي

امضاء هاي ديجيتالي ، فن آوري ديگري است كه توسط رمزنگاري كليد عمومي فعال گرديد و اين امكان را به مردم مي دهد كه اسناد و معاملات را طوري امضا كنند كه گيرنده بتواند هويت فرستنده را تأييد كند.امضاء ديجيتالي شامل يک اثر انگشت رياضي منحصر به فرد از پيام فعلي است كه به آن One-Way-Hash نيز گفته مي شود.

سرويسهاي اساسي

By:

مديريت امنيت

استانداردهاي مديريت امنيت (ISO-17799، ...)

By:

تهية خط مشي امنيت IT

جنبه‌هاي تشكيلاتي امنيت IT

مديريت امنيت IT

پياده‌سازي

روش‌هاي دفاعي

آگاهي‌رساني امنيتي

پيگيري مراحل

بیومتریک

By:

فناوری بیومتریک اگرچه از تخصصهایی سود می جوید که هر یک از آنها سابقه ی دیرینه در علم و صنعت دارند ولی دارای تعاریف، مفاهیم و کاربست های نو و جدیدی است. این فناوری که در واقع روشهای تعیین یا تایید هویت افراد به صورت خودکار، طبق شناسه های فیزیولوژیکی یا رفتاری است در سالهای گذشته، بیشتر در فیلم های سینمایی به عنوان یک فناوری پیشرفته علمی- تخیلی نمود داشته است و در عین حال در تعدادی از مراکز حساس که نیازمند به ضریب امنیتی بالایی بوده اند نیز بکار گرفته شده است. پیچیدگی سخت افزاری و نرم افزاری سامانه ها و قلت کاربرد آنها، هزینه¬های ساخت و راه¬اندازی گزافی را به مجریان چنین طرحهایی تحمیل می کرده است .

بیومتریک

By:

انواع بیومتریکها

بیومتریکهای فیزیولوژیکی

بیومتریکهای رفتاري

بیومتریک فیزیولوژیکی

By:

بیومتریکهای فیزیولوژیکی عبارتند از:

عنبیه نگاری

شبکیه نگاری

ا نگشت نگاری

چهره نگاری

دست نگاری

صوت نگاری

بیومتریک رفتاری

By:

بیومتریکهای رفتاري عبارتند از:

امضا نگاری

نحوه ی تایپ کردن

سایر بیومتریک

By:

پارامترهاي ديگري هم اخيراً مورد استفاده قرار گرفته است كه به علل مختلف هنوز كاربرد وسيعي ندارند. از جمله مي توان به بيومتريكهاي زير اشاره كرد

- DNA
- نحوه راه رفتن
- الگوي رگهاي پشت دست
- خطوط كف دست
- شكل گوش
- بوي بدن
- و الگوي بافتهاي زير پوستي دست

By:

آموزش

آموزش های عمومی

آموزش های اختصاصی

ISMS درایران

By:

برخی دلایل عدم توجه به ISMS در ایران :

الف: عدم تخصیص جایگاه مناسب به مسائل امنیتی

ب: کمبود های تئوریک و عملی کارشناسان

ج: عدم آموزش و اطلاع رسانی

By:

File-folder.ir