

آکادمی امنیت سایبری فن آوری اطلاعات رجاء



۰۲۱-۶۶۴۰۹۲۸۸

It@raja.ac.ir



تمام حقوق این اثر محفوظ است و هرگونه تکثیر یا تولید مجدد آن به کلی یا جزئی و در هر قالبی (چاپی، فتوکپی، فایل الکترونیکی، صدا و تصویر) بدون اجازه کتبی از شرکت فناوری اطلاعات رجاء شرعاً حرام و ممنوع است.

تلفن تماس: ۰۲۱-۶۶۴۰۹۲۸۸



فهرست مطالب

۴.....	۱. مقدمه.....
۵.....	۲. دوره های آموزشی امنیت اطلاعات.....
۵.....	۲,۱ امنیت اطلاعات.....
۶.....	۲,۲ امنیت سایبری سیستم های کنترل صنعتی.....
۸.....	۲,۳ ممیز امنیت سایبری.....
۹.....	۲,۴ ارزیابی و مدیریت مخاطرات سایبری.....
۱۰.....	۲,۵ مدیریت حوادث سایبری.....
۱۳.....	۲,۶ طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS).....
۱۴.....	۲,۷ سرممیزی سیستم مدیریت امنیت اطلاعات.....
۱۵.....	۲,۸ مدیریت راهبردی امنیت اطلاعات.....
۱۸.....	۲,۹ دفاع فعال سایبری.....
۲۰.....	۲,۱۰ راهبردهای امن سازی زیرساخت های حیاتی.....
۲۵.....	۲,۱۱ مدل بلوغ امنیت اطلاعات.....
۲۵.....	۲,۱۲ امنیت کاربر رایانه (CSCU).....
۲۶.....	۲,۱۳ تهدیدها و آسیب های فضای مجازی.....
۲۷.....	۲,۱۴ مدیریت امنیت اطلاعات در گزینش و استخدام کارکنان.....
۲۸.....	۳. اطلاعات تماس.....



۱. مقدمه

امروزه امنیت اطلاعات یکی از چالشهای اصلی در عصر فناوری اطلاعات محسوب میشود و حفاظت از اطلاعات در مقابل دسترسی غیرمجاز، تغییرات، خرابکاری و افشا امری ضروری و اجتناب ناپذیر به شمار میآید. فراهم آوری صحت و تمامیت اطلاعات به گونهای که در زمان مناسب، اطلاعات در دسترس افراد مجازی قرار گیرد که نیازمند آن هستند، عاملی است که منجر به اثربخشی کسب و کارها میشود. در سالهای اخیر، با افزایش تهدیدات و حملات سایبری به سازمانها و روند رو به گسترش آن، امنیت داراییهای اطلاعاتی برای تمام سازمانها امری حیاتی بوده و مستلزم یک مدیریت اثربخش برای آموزش همه کارکنان جهت حفاظت از اطلاعات سازمانی میباشد. از اینرو، برگزاری دورههای آموزشی امنیت اطلاعات در دو سطح مدیریت و کارکنان، در سازمانها یک ضرورت به شمار میرود. در این سند، به معرفی خدمات آموزشی اینجانب در حوزه امنیت اطلاعات پرداخته میشود. لازم به ذکر است دو دوره از مجموعه دورهه <<مدیریت اطلاعات>> و <<شبکه و امنیت اطلاعات در سازمانها>> آموزشی کارکنان دولت که توسط، سازمان مدیریت و برنامه ریزی کشور مصوب شده است نیز توسط اینجانب تدریس میشود.

خدایا چنان کن سرانجام کار، تو خشنود باشی و ما رستگار

فناوری اطلاعات رجا

بهار ۱۳۹۶



۲. دوره های آموزشی امنیت اطلاعات

۲,۱ امنیت اطلاعات

امروزه با گسترش روز افزون فناوری اطلاعات در سازمانها و بهره گیری از ابعاد گسترده آن در امر خدمات رسانی و حتی تولید محصولات، عنصر ارزشمندی به نام اطلاعات در پیکره سازمان ها پدید آمده که مهمترین دارایی آن سازمان نیز به شمار میرود. استفاده از فناوری اطلاعات و بهره‌مندی از سیستم های ذخیره و پردازش اطلاعات، به عنوان ابزاری قدرتمند، باعث متمایز شدن سازمان ها از یکدیگر شده و آنهایی که از این فرصت های بی بدیل فناورانه توانسته اند در زمان مناسب خویش، به بهترین نحو ممکن بهره برداری کنند گوی سبقت را از سایر رقبا ر بوده و موجب سودآوری کسب و کار خود شده اند. بنابراین در دنیای رقابتی امروز، اطلاعات به عنوان عنصری حیاتی که بقای سازمان ها به شدت به آن وابسته است نیازمند راهکارهای حفاظتی مناسب جهت جلوگیری از تخریب، دستکاری، حذف و یا ایجاد وقفه در خدمات میباشد.

در دوره آموزشی امنیت اطلاعات، با نگاهی ویژه به امنیت اطلاعات و تمرکز بر حفظ و نگهداشت اطلاعات، مخاطبان آموزش های لازم را در این خصوص فرا گرفته و میتوانند از دارایی های سازمانی به نحو شایسته ای حفاظت کنند.

سرفصل ها و محتوای این دوره عبارت است از:

- تعاریف و اصطلاح های امنیت اطلاعات
- آشنایی با تروجانها، درهای پشتی، روتکیت ها، ویروس ها و کرم ها و همچنین نحوه پاکسازی و مقابله با آنها
- بررسی تکنیکهای شکستن پسوردها و روشهای جلوگیری از آنها
- معرفی ابزارهای آزمون نفوذپذیری و ارزیابی آسیب پذیری نرم افزارها و برنامه های مبتنی بر وب سازمان
- بررسی حملات مهندسی اجتماعی و روشهای نوین تخلیه اطلاعاتی
- امنیت در حملات تزریق کد و چگونگی مقابله با آنها (SQL Injection & XSS)
- آشنایی با حملات سازمانی و روش های مقابله با آنها
- امنیت شبکه های بیسیم
- ایمن سازی سیستم عاملهای ویندوز و لینوکس
- آشنایی با تنظیمات امنیتی اکتیو دایرکتوری و کارگزار کنترل کننده دامنه (DC)
- تحلیل حملات انکار سرویس (DoS) و نحوه مقابله با آنها
- امنیت فیزیکی و محیط پیرامونی
- نحوه تنظیم خط مشی ها، روش های اجرایی و کنترل های امنیتی مناسب، مطابق با الزامات خاص کسب و کار
- معرفی هانی پات ها، بررسی نحوه عملکرد آنها و چگونگی پیکربندی آنها در معماری شبکه سازمان
- امنیت فیزیکی و منطقی مرکز داده سازمان
- آشنایی با دیوارهای آتش و پیکربندی امنیتی آنها
- آشنایی با نحوه تنظیم گزارش های وقایع، خطاها و مستندات امنیتی در سازمان
- امنیت شبکه و پایش امنیتی آن
- آشنایی با سیستم مدیریت امنیت اطلاعات (ISMS) و الزامات امنیتی آن



- مدیریت کلمه عبور حساب های کاربری و الزام های کنترل دسترسی
- مدیریت آسیب پذیری ها و مخاطرات امنیتی در سازمان
- مدیریت امنیت اطلاعات کارکنان
- آشنایی با نحوه کرک کردن پسورد انواع سیستم عامل های ویندوز و بررسی روش های جلوگیری از آنها
- آشنایی با نحوه کرک کردن رمز عبور بایوس سیستم و چگونگی جلوگیری از آنها
- امنیت مبتنی بر مرورگر و وبگردی امن
- امنیت تجهیزات داخلی و بیرونی سازمان و نگهداری ایمن تجهیزات
- امنیت کابل کشی و خطوط ارتباطی شبکه سازمان
- آشنایی با روش های امن امحای اطلاعات
- آشنایی با نحوه جلوگیری از نشت اطلاعات سازمانی.

۲,۲ امنیت سایبری سیستم های کنترل صنعتی

سیستم های کنترل صنعتی، سیستم هایی مبتنی بر رایانه هستند که برای کنترل فرایندهای صنعتی و عملکردهای فیزیکی استفاده میشوند. استفاده گسترده از این سیستم ها در زیرساخت ها و سامانه های حیاتی کشور، موجب شکل گیری نوع جدیدی از حملات سایبری به شبکه های بزرگ صنعتی کشورمان شده است که از نمونه های مشهور و شناخته شده آن در سال های اخیر میتوان به استاکس نت اشاره کرد.

در این دوره آموزشی، ضمن بررسی چالش ها و مشکلات امنیتی سیستم های کنترل صنعتی، ارایه راهکارهای اجرایی برای کاهش مخاطرات امنیتی این سیستم ها، روش های امن سازی آنها بر اساس استانداردهای بین المللی، آشنایی با بهترین تجربه های جهانی در حوزه حفاظت از سیستمهای کنترل صنعتی و همچنین بررسی الزامات ملی ایران در این خصوص، از دیگر موارد مطرح در این دوره است.

سرفصل ها و محتوای این دوره عبارت است از:

- آشنایی با سامانه های حیاتی و غیرحیاتی
- مشکلات و چالش های امنیتی سیستم های کنترل صنعتی
 - مفاهیم امنیتی سیستم های کنترل صنعتی
 - ضرورت توجه به امنیت سیستم های کنترل صنعتی
 - رخدادهای امنیتی سیستم های کنترل صنعتی
 - انواع بدافزارهای سیستم های کنترل صنعتی
 - آشنایی با آسیب پذیری های موجود در سیستم های کنترل صنعتی
 - آشنایی با آسیب پذیری های حیاتی در طراحی محصولات سیستم های کنترل صنعتی
 - آسیب پذیری آئورورا (Aurora)
 - آسیب پذیری بوریاس (Boreas)
 - نحوه شناسایی سیستم های کنترل صنعتی آسیب پذیر از طریق اینترنت
 - آشنایی با انواع تهدیدات و مخاطرات امنیتی در سیستم های کنترل صنعتی
 - بررسی انواع حملات سازمانی در شبکه های صنعتی
 - بررسی مشکلات امنیتی در معماری، سیستم کنترلی، تجهیزات و بستر ارتباطی شبکه های صنعتی



- بررسی چالش های امنیتی سیستم های کنترل صنعتی
- معرفی روش های جلوگیری از تهدیدات امنیتی سیستم های کنترل صنعتی
- بررسی رویکرد واکنشی به امنیت سایبری در سیستم های کنترل صنعتی
- تاریخچه حملات سایبری به سیستم های کنترل صنعتی
- استانداردهای امنیتی سیستم های کنترل صنعتی
 - ISO
 - CPNI
 - NIST
 - NERC
 - DHS
 - DOE
 - ISA
- امنیت سیستم های کنترل صنعتی و زیرساخت های حیاتی در سایر کشورها (مطالعه موردی)
- بررسی امنیت در سیستم های کنترل صنعتی و سامانه های فناوری اطلاعات
 - بررسی وصله های امنیتی در سیستم های کنترل صنعتی و سامانه های فناوری اطلاعات
 - بررسی پیچیدگی های سیستم های کنترل صنعتی نسبت به سامانه های فناوری اطلاعات
- امنیت سیستم های کنترل صنعتی
 - فاکتورهای بروز آسیب پذیری در سیستم های کنترل صنعتی
 - مسایل امنیتی مربوط به ارتباط شبکه های کنترل فرایند سیستم های صنعتی با شبکه داخلی سازمان
 - مسایل امنیتی مربوط به طراحی، استقرار و بهره برداری از سیستم های کنترل صنعتی
 - مسایل امنیتی مربوط به پروتکل های اختصاصی سیستم های کنترل صنعتی
 - مسایل امنیتی مربوط به دسترسی های غیرمجاز به نرم افزارهای کنترل کننده سیستم های کنترل صنعتی
 - مسایل امنیتی مربوط به کارمندان ناراضی داخل سازمان
 - مسایل امنیتی مربوط به رسانه های ارتباطی سیستم های کنترل صنعتی (سیستم تلفن سوئیچ عمومی، ارتباطات بیسیم و اینترنت)
- الزامات مراکز بالادستی کشور در خصوص امن سازی سیستم های کنترل صنعتی
- بررسی متدولوژی های مدیریت مخاطرات سایبری سیستم های کنترل صنعتی
- روش های اجرایی فراهم آوری امنیت در سیستم های کنترل صنعتی
 - نحوه تدوین خط مشی ها، روش های اجرایی و دستورالعمل های امنیتی
 - بررسی نقش مدیریت مخاطره در امن سازی سیستم های کنترل صنعتی
 - چگونگی وضع کنترل های امنیتی در سیستم های کنترل صنعتی
 - چگونگی ایمن سازی برنامه های سیستم کنترل صنعتی
 - چگونگی امن سازی تجهیزات ارتباطی سیستم های کنترل صنعتی
 - چگونگی امن سازی محیط های ذخیره، پردازش و بازیابی اطلاعات سیستم های کنترل صنعتی
 - چگونگی طراحی ضمانت نامه های اجرایی مناسب در سیستم های کنترل صنعتی
 - چگونگی به کارگیری سیستم های اخطاردهی و گزارش نقض ها و نقص ها در سیستم های کنترل صنعتی
 - روش های احراز هویت در سیستم های کنترل صنعتی



- آشنایی با سیستم ها و تجهیزات امنیتی سیستم های کنترل صنعتی
- چگونگی سنجش اثربخشی کنترل های امنیتی سیستم های کنترل صنعتی
- آموزش و آگاهی رسانی امنیتی در شبکه های صنعتی
- نحوه امن سازی دسترسی های از راه دور به سیستم های کنترل صنعتی
- امنیت فیزیکی و محیطی سیستم های کنترل صنعتی
- نحوه تشکیل گروه های واکنش به رخدادها و حوادث امنیتی در شبکه های صنعتی
- چگونگی تدوین طرح های تداوم کسب و کار (BCP) و بازیابی از وضعیت خرابی (DRP) در سیستم های کنترل صنعتی
- آشنایی با معماری های امنیتی مرجع در امن سازی سیستم های کنترل صنعتی
- نحوه برطرف سازی آسیب پذیری های امنیتی محصولات سیستم های کنترل صنعتی
- آشنایی با نحوه تهیه و تدوین چک لیست های امنیتی سیستم های کنترل صنعتی
- بررسی استراتژی های دفاع در عمق در امن سازی سیستم های کنترل صنعتی
- انجمن ها و مؤسسات پژوهشی در حوزه امن سازی سیستم های کنترل صنعتی.

۲,۳ ممیز امنیت سایبری

امروزه امنیت اطلاعات، یکی از چالش های اصلی در عصر فناوری اطلاعات محسوب میشود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تخریب، تغییر، تحریف، انکار و افشا یک ضرورت انکار ناپذیر برای تمامی سازمان ها به شمار میرود. شدت این حملات گاهی به حدی است که حتی سازمان هایی با بهترین زیرساخت های امنیتی هم نمی توانند تضمین کنند که هیچ گاه اقدامات بدخواهانه بر روی شبکه آنها اتفاق نخواهد افتاد. از سوی دیگر، با رشد تصاعدی جرایم سایبری و افزایش حملات درون سازمانی در ماه های اخیر، امنیت اطلاعات به عنوان عنصری حیاتی در بقای کسب و کار سازمان ها تبدیل شده است. از اینرو، اتخاذ راهبردهایی به منظور حساسی و ممیزی امنیتی تمام سطوح سازمانی جهت شناسایی نقاط آسیب پذیر و برطرف سازی آنها قبل از وقوع هر تهدیدی، از اهمیت بسیار ویژه ای برخوردار است. بنابراین لازم است در مراحل مختلف، ممیزی های دوره ای و موردی از وضعیت امنیت سایبری سازمان به عمل آید.

در این دوره آموزشی، مخاطبان آموزش های لازم را در خصوص ممیزی امنیت سایبری سازمان ها و شرکت های مطبوع خویش یا سایر سازمان ها، منطبق با رویه ها و استانداردهای مربوطه و همچنین قوانین بالادستی کشورمان فرا میگیرند.

سرفصل ها و محتوای این دوره عبارت است از:

- معرفی کلی فرایند ممیزی امنیت سایبری
- بررسی استانداردها و بهروشه های ممیزی امنیت سایبری
- آشنایی با مراحل اجرایی ممیزی امنیت سایبری
- اصول مهم در تشکیل تیم های ممیزی و وظایف هر یک از اعضای آن
- نحوه تهیه چک لیست های ممیزی امنیت سایبری (در حوزه های مختلف مورد بررسی، شامل شبکه محلی و گسترده ، LAN & WAN) ارتباطات، عملیات، فیزیکی، افراد و مرکز داده)
- چگونگی تهیه برنامه ممیزی امنیت سایبری (Cyber Security Audit Plan)
- اصول و تکنیک های مصاحبه، مشاهده و بررسی شواهد و مستندات در ممیزی امنیت سایبری
- نحوه بررسی مستندات و اسناد در ممیزی ای امنیتی
- آشنایی با نکات کلیدی در اثربخشی فرایند ممیزی
- معرفی روش های بهره گیری از رویکردهای روانشناختی در ممیزی های امنیت سایبری



- آشنایی با تکنیک گزارش نویسی فرایند ممیزی امنیت سایبری
- آشنایی با فرایند گزارش دهی عدم انطباق ها
- نمونه فرم ها و چک لیست های ممیزی امنیت سایبری.

۲.۴ ارزیابی و مدیریت مخاطرات سایبری

امروزه با گسترش شدید و قریب الوقوع تهدیدات پیشرفته امنیتی بر ضد سازمان ها، ارزیابی و مدیریت مخاطرات امنیت اطلاعات یکی از دغدغه های اصلی در عصر فناوری اطلاعات محسوب میشود. با رشد یکباره این تهدیدات، امروز بیش از هر زمان دیگری، بقا و دوام سازمان ها به حفاظت مناسب از دارایی ها و برطرف سازی آسیب پذیری ها بستگی دارد. از اینرو، امنیت دارایی های اطلاعاتی و حفظ سرمایه های سازمانی، برای تمام سازمان ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است.

در این دوره آموزشی، با نگاهی متفاوت به ارزیابی و مدیریت مخاطرات امنیت اطلاعات و با تمرکز اصلی بر فعالیت های عملی، فراگیران در یک تجربه مشترک که آمیخته با فعالیت های گروهی است ضمن بررسی سناریوهای مختلف و پیچیده مربوط به مخاطرات، با روش های شناسایی، طبقه بندی و ارزش گذاری دارایی ها آشنا شده و اصول ارزیابی و مدیریت مخاطرات سایبری را بر اساس استانداردها و بهترین تجربه های جهانی فرا میگیرند.

سرفصل ها و محتوای این دوره عبارت است از:

- آشنایی با مفاهیم اصلی امنیت اطلاعات
- بررسی متدولوژی مدیریت دارایی ها
 - نحوه شناسایی دارایی ها
 - چگونگی شناسایی وضعیت دارایی های اطلاعاتی
 - نحوه شناسایی فرایندها و حوزه های کسب و کار
 - نحوه شناسایی سرویس های ارائه شده در هر یک از حوزه های کسب و کار
 - نحوه طبقه بندی دارایی های شناسایی شده
 - چگونگی تعیین مسئول (مالک) برای هر دارایی
 - سازوکارهای تعیین سطح دسترسی افراد به دارایی ها بر اساس ماتریس های کنترل دسترسی
- بررسی متدولوژی ارزیابی مخاطرات امنیتی
 - معرفی استانداردهای مطرح در حوزه ارزیابی مخاطرات امنیت اطلاعات
 - نحوه انتخاب و تعیین متدولوژی مناسب ارزیابی مخاطرات امنیت اطلاعات
 - تعیین شیوه ارزش دهی به دارایی ها
 - تعیین شیوه ارزش گذاری دارایی های با روابط متقابل
 - توصیف ارزش دهی به هر یک از دارایی ها بر مبنای پارامترهای محرمانگی، صحت و دسترس پذیری
 - معرفی آسیب پذیری ها و نحوه بررسی و اولویت بندی آنها
 - تعیین شیوه آنالیز ضربه (Impact Analysis) و پیامدهای تهدیدات
 - تعیین شیوه دستیابی به احتمال وقوع تهدیدات
 - تعیین شیوه ارزیابی و تعیین مخاطره
 - تعیین اولویت بندی مخاطره و استراتژی های مدیریت مخاطرات



- بررسی عوامل مهم در ارزش گذاری دارایی ها
- نحوه محاسبه ارزش کل دارایی ها
- شناسایی و بررسی آسیب پذیری های دارایی ها
- شناسایی و بررسی تهدیدات دارایی ها
- بررسی انواع تهدیدهای متعارف (مصادیق محیطی و انسانی)
- نحوه تعیین لیست تهدیدات ذاتی
- نحوه تعیین لیست تهدیدات واقعی
- نحوه تهیه جدول تهدیدات به تفکیک دارایی ها
- نحوه تهیه جدول تهدیدات به تفکیک رخدادها
- تعیین احتمال وقوع تهدیدها بر اساس متدولوژی ارزیابی مخاطره
- بررسی عوامل مورد توجه در تعیین احتمال وقوع تهدیدات
- شناسایی و تحلیل پیامد وقوع تهدیدها
- محاسبه و تعیین میزان مخاطره هر تهدید، برای هر یک از دارایی ها
- راهبردهای مدیریت مخاطرات
- آشنایی با گزینه های مناسب جهت برخورد با مخاطرات شناسایی شده
- چگونگی تعیین استراتژی مناسب جهت مدیریت مخاطرات
- بررسی انواع گزینه های برخورد با مخاطرات
- عوامل مؤثر در انتخاب گزینه های برخورد با مخاطرات
- نقش هزینه های پیشگیری از مخاطره، در تعیین استراتژی مناسب
- تعیین معیار و سطح قابل قبول مخاطرات
- تعیین شیوه مناسب برخورد با مخاطرات باقی مانده
- معرفی بهترین تجربه های جهانی در حوزه مدیریت مخاطرات سایبری
- اتخاذ کنترل های امنیتی
- معرفی نرم افزارها و ابزارهای مدیریت مخاطرات.

۲.۵ مدیریت حوادث سایبری

با پیشرفت و گسترش روز افزون فناوری اطلاعات و ارتباطات در دنیای امروز، بحث حفاظت از داده ها اهمیت ویژه ای یافته است . هر چه راه های دسترسی و روش های ارتباطی افزایش می یابد مسأله حفاظت از امنیت اطلاعات نیز مهم تر و پیچیده تر میشود . وجود حفره ها و نقص های امنیتی در سیستم های فناوری اطلاعات، همواره مورد توجه افراد سودجو بوده است به طوری که در مقاطعی از زمان، سرعت افزایش تعداد حملات صورت گرفته، از سرعت پیشرفت و گسترش سیستم ها بسیار بیشتر است. بنابراین با نگاهی به آمار منتشر شده و وضعیت فعلی پیشرفت فناوری اطلاعات، وجود مراکزی مستقل برای تأمین امنیت فضای تبادل اطلاعات در سازمان ها امری حیاتی و ضروری به نظر میرسد.

امروزه بیشتر سازمان ها دریافته اند که یک راهکار امنیتی واحد برای تأمین امنیت سیستم ها وجود ندارد بلکه باید از استراتژی امنیتی چند لایه بهره گرفت . یکی از لایه هایی که بیشتر سازمان ها در استراتژی امنیتی خود در نظر میگیرند ایجاد یک مرکز مدیریت



رخدادهای امنیتی و تشکیل تیم پاسخگویی به رخدادهای امنیتی رایانه است که در سازمان های ایرانی با نام گوهر شناخته میشود. هدف از ایجاد مرکز مدیریت رخدادهای امنیتی و تشکیل این تیم، فراهم آوری قابلیت ارزیابی، پاسخگویی و آموختن از رخدادهای امنیتی اطلاعات است. این مرکز با مدیریت صحیح رخدادهای امنیتی در سازمان میتواند کمک شایانی را به سازمان ها در کاهش صدمات مالی و مهم تر از همه، وجهه و شهرت آن سازمان کند.

در این دوره آموزشی، مخاطبان ضمن آشنایی با چارچوب ها و اصول ایجاد تیم های امداد رایانه ای در سازمان های ایرانی، با روش های اجرایی طراحی، تشکیل و راه اندازی این تیم ها به صورت کامل آشنا شده و می توانند تیم های امداد رایانه ای را در سازمان های خویش پیاده سازی کنند.

سرفصل ها و محتوای این دوره عبارت است از:

- تشکیل و راه اندازی مرکز گوهر
 - معرفی مرکز گروه واکنش هماهنگ رخداد (گوهر)
 - اسناد بالادستی الزام آور کشور در خصوص تشکیل مرکز گوهر در سازمان ها
 - اهداف راه اندازی مرکز گوهر
 - مزایای راهان دازی مرکز گوهر
 - مأموریت ها و وظایف مرکز گوهر
 - سطوح پیاده سازی مرکز گوهر
 - مراحل تکامل مراکز گوهر
- گام های راه اندازی و تشکیل مرکز گوهر در سازمان
 - جایگاه مرکز گوهر در چارت سازمان و ارتباط آن با سایر واحدها
 - ساختار مرکز گوهر و تیم های آن
 - نقش ها و مسئولیت های افراد
 - تعیین مکان فیزیکی مرکز گوهر
- تعاملات مرکز گوهر
 - نحوه تعامل مرکز گوهر با مرکز عملیات امنیت (SoC)
 - نحوه تعامل مرکز گوهر با سایر گوهرها
 - نحوه تعامل مرکز گوهر با مراکز ماهر و آپا
 - نحوه تعامل مرکز گوهر با ذی نفعان سازمان (همکاران، مشتریان، بیمه گذاران، اشخاص سوم و غیره)
 - نحوه تعامل مرکز گوهر با سازمان های بالادستی، نهادهای امنیتی و قانون گذار
- سرویس های امنیتی مرکز گوهر
 - خدمات پیشگیرانه
 - خدمات واکنشی
 - خدمات مدیریت کیفی امنیت
- فراهم آوری امنیت مرکز گوهر
 - امنیت شبکه



- امنیت فیزیکی
- امنیت منابع انسانی
- ابزارها و نرم افزارهای مورد استفاده در مرکز گوهر
- مدیریت رویدادها و حوادث امنیتی در گوهر
 - چرخه مدیریت رخدادهای و حوادث امنیتی در گوهر
 - چگونگی گردش کار بین تیم های گوهر
 - نحوه رصد و تشخیص نفوذ به سازمان
 - نحوه شناسایی رخدادهای امنیتی در سازمان
 - نحوه شناسایی آسیب پذیری ها
 - نحوه جمع آوری گزارشات و هشدارها از تجهیزات شبکه و سامانه های امنیتی
- ارزیابی و تصمیم گیری درباره رویدادها و حوادث امنیتی در گوهر
 - نحوه تعیین متدولوژی رسیدگی به حوادث امنیتی
 - نحوه تدوین طرح ارزیابی و تصمیم اولیه
 - نحوه تدوین طرح ارزیابی و تأیید رویدادهای امنیتی
 - نحوه تدوین طرح رده بندی رویدادهای امنیتی
- پاسخگویی به رویدادها و حوادث امنیتی در گوهر
 - نحوه تدوین طرح پاسخگویی به حوادث امنیتی
 - نحوه تعیین اقدامات لازم در خصوص پاسخگویی فوری به حوادث امنیتی
 - نحوه تعیین اقدامات لازم در خصوص پاسخگویی ثانویه به حوادث امنیتی
 - نحوه تعیین اقدامات لازم در خصوص پاسخگویی ها با موقعیت های ویژه
 - نحوه تعیین طرح محدودسازی اثرات نامطلوب حوادث امنیتی
 - چگونگی طراحی زیرساخت های سازمانی مطلوب و مورد نیاز برای پاسخگویی به رویدادهای امنیتی
 - نحوه تدوین طرح استمرار کسب و کار
 - نحوه تعیین متدولوژی مناسب جهت روز آمد کردن اطلاعات رویدادهای امنیتی
 - نحوه تعیین کنترل های امنیتی در رابطه با رویدادهای امنیتی
 - نحوه تعیین متدولوژی ارزیابی کنترل های امنیتی به کار گرفته شده
 - نحوه تعیین روش تحلیل امور قانونی امنیت اطلاعات
- نحوه اعلام هشدار در مورد رخدادهای امنیتی
- نحوه تهیه فرم های مورد نیاز مرکز گوهر
- فرایندهای ترمیم و بازیابی از حوادث در گوهر
- چگونگی اشتراک گذاری اطلاعات و پایگاه دانش حوادث
- گزارش دهی رویدادها و حوادث امنیتی در گوهر
 - نحوه گزارش دهی رخدادهای امنیتی به گوهر
 - نحوه گزارش دهی رخدادهای امنیتی از گوهر به سایر نهادها



- یادگیری از رویدادها و حوادث امنیتی در گوهر
 - نحوه تدوین برنامه های آموزشی و آگاهی رسانی
 - نحوه تدوین متدولوژی مستندسازی رویدادهای امنیتی
 - نحوه تدوین روش بازنگری های مدیریتی امنیت اطلاعات
 - نحوه تدوین طرح واره بهبود در کاربرد نظارت امنیت اطلاعات
- ویژگیها و ساختار پرتال سازمانی مرکز گوهر
- روشهای ارزیابی و ممیزی عملکرد مرکز گوهر
- معرفی بهترین الگوها و استانداردهای جهانی در خصوص راه اندازی و تشکیل مرکز گوهر.

۲.۶ طراحی و پیاده سازی سیستم مدیریت امنیت اطلاعات (ISMS)

امروزه با گسترش تهدیدها و حوادث امنیتی در سطح سازمان ها، امنیت دارایی های اطلاعاتی برای تمام سازمان ها امری حیاتی بوده و مستلزم یک مدیریت اثربخش است. استاندارد ISO/IEC 27001:2013 زمینه مناسبی را برای طراحی و استقرار سیستم مدیریت امنیت اطلاعات و ارزیابی آن در سازمان ها و بهره گیری از منافع این رویکرد، فراهم کرده است.

در این دوره آموزشی، مخاطبان آموزش های لازم را در خصوص ایجاد، پیاده سازی، استقرار و ممیزی داخلی سیستم مدیریت امنیت اطلاعات (ISMS) مبتنی بر نیازها و الزامات مختص کسب و کار خود و منطبق با رویه ها و استانداردهای ISO/IEC 27001:2013 و ISO/IEC 27002:2013 که البته مطابق با الزامات ملی کشورمان، بومی سازی شده اند فرا میگیرند.

سرفصل ها و محتوای این دوره عبارت است از:

- تعاریف، اصطلاح ها و واژگان امنیت اطلاعات و سیستم مدیریت
- آشنایی با سیستم مدیریت امنیت اطلاعات و استانداردهای خانواده ISMS
- معرفی اصول، مفاهیم و الزامات سیستم مدیریت امنیت اطلاعات
- چرخه بهبود مستمر امنیت اطلاعات
- چگونگی تعیین دامنه (Scope) سیستم مدیریت امنیت اطلاعات
- چگونگی تعیین نقش ها و مسئولیت ها
- نحوه شناسایی نیازمندیهای امنیت اطلاعات
- اصول مستندسازی در ISMS و چگونگی تهیه مستندات الزامی
- انتخاب و پیاده سازی کنترل ها و اهداف کنترلی استاندارد ISO/IEC 27001:2013
- نحوه تدوین و طراحی خط مشی ها، روش های اجرایی و طرح های امنیت اطلاعات
- شناسایی و ارزیابی مخاطرات امنیت اطلاعات
- چگونگی برنامه ریزی، تهیه، اجرا و گزارش دهی وقایع امنیت اطلاعات
- روش های مدیریت مخاطرات امنیت اطلاعات
- مدیریت حوادث امنیتی در طرح تداوم کسب و کار
- تهیه برنامه های آموزشی و آگاهی رسانی امنیتی
- فرایند ممیزی داخلی و اصول انتخاب ممیزان
- نحوه اجرای طرح ممیزی داخلی امنیت اطلاعات



- چگونگی تهیه چک لیست های ممیزی
- اقدامات اصلاحی و پیشگیرانه و رفع عدم انطباق ها
- نحوه ممیزی شخص سوم و فرایند ثبت و صدور گواهینامه ISO/IEC 27001:2013
- نمونه پروژه ها و فایل های مربوط به پیاده سازی سیستم مدیریت امنیت اطلاعات.

۲.۷ سرممیزی سیستم مدیریت امنیت اطلاعات

امروزه امنیت اطلاعات، یکی از چالش های اصلی در عصر فناوری اطلاعات محسوب میشود و حفاظت از اطلاعات در برابر دسترسی غیرمجاز، تخریب، تغییر، تحریف و انکار، یک ضرورت انکارناپذیر به شمار میرود. از اینرو، استاندارد ISO/IEC 27001:2013 زمینه مناسبی را برای بهره گیری از این رویکرد در سازمان ها فراهم نموده است. پس از پیاده سازی و استقرار سیستم مدیریت امنیت اطلاعات (ISMS) در سازمان، لازم است که انطباق آن با کنترل ها و الزامات این استاندارد بین المللی بررسی شود.

در این دوره آموزشی، مخاطبان آموزش های لازم را در خصوص ممیزی شخص سوم سیستم مدیریت امنیت اطلاعات، منطبق با رویه ها و استانداردهای مربوطه و همچنین قوانین بالادستی کشورمان فرا میگیرند.

سرفصل ها و محتوای این دوره عبارت است از:

- معرفی کلی سیستم مدیریت امنیت اطلاعات
- سازوکارهای مدیریت مخاطرات امنیتی در سیستم های مدیریتی امنیت اطلاعات
- معرفی مراحل اجرایی سیستم مدیریت امنیت اطلاعات
- بررسی استانداردهای ممیزی سیستم مدیریت امنیت اطلاعات
- آشنایی با مراحل اجرایی ممیزی
- نحوه تهیه چک لیست های ممیزی
- چگونگی تهیه برنامه ممیزی (Audit Plan)
- فرایندهای مربوط به مرور مستندات سیستم مدیریت امنیت اطلاعات و ممیزی مرحله اول
- اصول مهم در اثربخشی فرایندی ممیزی
- اصول تشکیل تیم های ممیزی و وظایف هر یک از اعضای آن
- چگونگی بررسی الزامات استاندارد
- فرایند گزارش دهی عدم انطباق ها
- بهره گیری از رویکردهای روانشناختی در ممیزی مرحله دوم
- اصول و تکنیک های مصاحبه، مشاهده و بررسی مستندات سیستم مدیریت امنیت اطلاعات
- اصول گزارش نویسی فرایند ممیزی
- بررسی الزامات مرکز مدیریت راهبردی افتا در خصوص ممیزی سیستم مدیریت امنیت اطلاعات
- فرایند صدور گواهینامه سیستم مدیریت امنیت اطلاعات
- نمونه فرم ها و چک لیست های ممیزی سیستم مدیریت امنیت اطلاعات



۲.۸ مدیریت راهبردی امنیت اطلاعات

گسترش روز افزون تهدیدات و افزایش حملات سایبری به سازمان ها در سال های اخیر، بیانگر آن است که شیوه های دفاع فعلی در برابر این تهدیدات دیگر جوابگو نیست و سازمان ها نیازمند بکارگیری تدابیر اصولی تری در این حوزه هستند. امروزه یکی از مهمترین راهکارها در خصوص مدیریت امنیت اطلاعات و پاسخگویی مناسب به تهدیدات سایبری، استفاده از الگوهای راهبردی امنیت اطلاعات است.

در این دوره آموزشی، مخاطبان ضمن آشنایی با الزامات، نیازمندی ها، استانداردها و بهروش های راهبردی امنیت اطلاعات در سازمان میتوانند امنیت اطلاعات را در سازمان های خویش، مدیریت و راهبری کنند.

سرفصل ها و محتوای این دوره عبارت است از:

- آشنایی با اصول و مفاهیم راهبردی امنیت اطلاعات
 - اصطلاح ها و تعاریف مهم امنیت اطلاعات
 - مثلث سه گانه امنیت اطلاعات و نحوه ارتباط اجزای آن با یکدیگر
 - مثلث عملکرد، راحتی استفاده و امنیت و اصول رعایت آن در سازمان ها
 - اصول امنیت اطلاعات
 - چرخه تداوم امنیت در سازمان
 - مفاهیم امنیت راهبردی و راهبری امنیت
 - دارایی و دارایی های اطلاعاتی در راهبری امنیت
 - روش های شناسایی دارایی ها
 - بهروش ها و بهترین درس آموزه های امنیت اطلاعات
- آشنایی با الزامات و نیازمندی های امنیت اطلاعات
 - الزامات کلیدی امنیت اطلاعات
 - اصول مدیریت امنیت اطلاعات
 - نیازمندی های امنیت اطلاعات بهینه
 - آسیب پذیری ها و تهدیدات امنیتی
 - چالش های فراهم آوری امنیت اطلاعات در سازمان ها
- آشنایی با فرایندهای ارزیابی و مدیریت مخاطرات امنیت اطلاعات
 - متدولوژی های مدیریت دارایی ها
 - شیوه های ارزشدهی به دارایی ها
 - شیوه ارزشگذاری دارایی های با روابط متقابل
 - متدولوژی های ارزیابی مخاطرات امنیت اطلاعات
 - استانداردهای مطرح در حوزه ارزیابی مخاطرات امنیت اطلاعات
 - آسیب پذیری ها و نحوه بررسی و اولویت بندی آنها
 - سازوکارهای تبیین آنالیز ضربه (Impact Analysis) و پیامدهای تهدیدات
 - شیوه های دستیابی به احتمال وقوع تهدیدات



- روش های ارزیابی و تعیین مخاطره برای هر دارایی
- روش های اولویت بندی مخاطرات
- روش های شناسایی و بررسی آسیب پذیری های دارایی ها
- روش های شناسایی و بررسی تهدیدات دارایی ها
- استراتژی های مطرح در مدیریت مخاطرات
- روش تعیین معیار و سطح قابل قبول مخاطرات
- روش های اتخاذ کنترل های امنیتی
- بهترین تجربه های جهانی در حوزه مدیریت مخاطرات
- بررسی جایگاه افراد، فرایندها و فناوری ها در راهبرد امنیت اطلاعات سازمان
- چگونگی تعریف نقش ها و مسئولیت های راهبردی امنیت اطلاعات در سازمان
 - نقش ها و مسئولیت های راهبردی امنیت اطلاعات
 - چگونگی تعریف این نقش ها و مسئولیت ها
- اصول راهبری و مدیریت امنیت اطلاعات در سازمان های ایرانی
 - اصول راهبردی امنیت اطلاعات در حوزه راهبری فناوری اطلاعات و امنیت
 - جایگاه مدیریت امنیت راهبردی در سازمان
 - نقش امنیت راهبردی در فراهم آوری دفاع فعال در سازمان
 - حوزه های مورد توجه در امنیت راهبردی
 - رویکردهای امنیت راهبردی
 - مزایای امنیت راهبردی
 - مشکلات و چالش های امنیت راهبردی
- راهکارهای مدیریت راهبردی امنیت اطلاعات در سازمان
 - مدیریت عملیات
 - مدیریت ظرفیت
 - مدیریت تغییرات
 - مدیریت ارتباطات
 - مدیریت دسترسی
 - مدیریت دارایی ها
 - مدیریت منابع انسانی
 - مدیریت امنیت اطلاعات
 - مدیریت خدمات شخص سوم
- نکات قابل توجه در راهبردهای مدیریتی امنیت فیزیکی و محیطی سیستم های اطلاعاتی
- معرفی استانداردها و بهروش های موجود در حوزه مدیریت راهبردی امنیت اطلاعات
- راهبردهای طراحی و پیاده سازی کنترل های امنیتی در سازمان
 - راهبردهای کنشی امنیت اطلاعات



- راهبردهای واکنشی امنیت اطلاعات
- راهبردهای مبتنی بر بلوغ امنیت اطلاعات سازمانی
- راهبردهای مبتنی بر استانداردهای امنیتی
- راهبردهای معرفی شده در چارچوب های امنیتی
- راهبردهای مبتنی بر بهترین شیوه های اجرایی
- چگونگی تطبیق و بررسی انطباق کنترل های امنیتی پیاده سازی شده در سازمان با استانداردهای امنیت اطلاعات
- اصول مستندسازی در امنیت اطلاعات راهبردی
 - مستندات الزامی امنیت اطلاعات
 - استانداردهای مستندسازی امنیت اطلاعات
 - نکات قابل توجه در مستندسازی امنیتی
 - روشهای نسخه گذاری مستندات امنیتی
 - اصول به روز رسانی مستندات امنیتی
- اصول تدوین برنامه پاسخ دهی به حوادث امنیت اطلاعات
 - انواع روش های پاسخ دهی به حوادث امنیتی
 - نحوه تدوین طرح پاسخ دهی به حوادث امنیتی
 - نحوه تعیین اقدامات لازم در خصوص پاسخگویی فوری به حوادث امنیتی
 - نحوه تعیین اقدامات لازم در خصوص پاسخگویی ثانویه به حوادث امنیتی
 - نحوه تعیین اقدامات لازم در خصوص پاسخگویی ها با موقعیت های ویژه
 - نحوه تعیین طرح محدودسازی اثرات نامطلوب حوادث امنیتی
 - چگونگی طراحی زیرساخت های سازمانی مطلوب و مورد نیاز برای پاسخگویی به رویدادهای امنیتی
 - نحوه تعیین متدولوژی مناسب جهت روز آمد کردن اطلاعات رویدادهای امنیتی
 - نحوه تعیین روش تحلیل امور قانونی امنیت اطلاعات
- اصول تدوین برنامه های تداوم کسب و کار و بازیابی از فاجعه
 - استانداردهای و بهترین شیوه های اجرایی تداوم کسب و کار و بازیابی از فاجعه
 - اصول مهم در تدوین برنامه های کسب و کار و بازیابی از فاجعه در سازمان
 - چگونگی تدوین برنامه های مدیریت تداوم کسب و کار و بازیابی از فاجعه در سازمان
 - معرفی روش های اندازه گیری کارایی برنامه های تداوم کسب و کار و بازیابی از فاجعه
- اصول تدوین خط مشی ها، دستورالعمل ها و روش های اجرایی امنیت اطلاعات در سازمان
 - چگونگی تدوین خط مشی ها، دستورالعمل ها و روش های اجرایی امنیت اطلاعات
 - بررسی تفاوت هر یک از این اسناد با یکدیگر
 - چگونگی سنجش اثربخشی این اسناد
 - نحوه بازنگری این اسناد
 - معرفی منابع و وبگاه های اسناد از قبل تدوین شده
 - اصول طراحی و اجرای برنامه های آموزشی و آگاهی رسانی امنیتی.



۲.۹ دفاع فعال سایبری

امروزه با گسترش تهدیدات و مخاطرات امنیتی، حتی سازمان هایی با بهترین زیرساخت های امنیتی هم نمیتوانند تضمین نمایند که اقدامات یا عملیات بدخواهانه بر روی شبکه آنها رخ نخواهد داد. هنگامی که حوادث امنیتی به وقوع می پیوندند، برای یک سازمان، حیاتی است که راهکار مؤثری برای دفاع و همچنین پاسخگویی به آن حملات داشته باشد. سرعت تشخیص، تحلیل و پاسخگویی سازمان به حوادث امنیتی علاوه بر این که میتواند خسارت ناشی از حادثه را محدود سازد، هزینه بازیابی از آن حادثه را نیز به شدت کاهش میدهد.

در این دوره آموزشی، مخاطبان ضمن آشنایی با حملات پیشرفته سایبری، مهارت های مورد نیاز را جهت طراحی، پیاده سازی و مدیریت اجزای کلیدی امنیت شبکه های سازمانی، فرا گرفته و میتوانند از سازمان ها در برابر مخاطرات و تهدیدهای امنیتی پیشرفته محافظت کنند.

سرفصل ها و محتوای این دوره عبارت است از:

- آشنایی با مفاهیم کلیدی امنیت اطلاعات
- آشنایی با حملات سایبری و روش های نفوذ به سازمان ها
- آشنایی با اصول دفاع سایبری
- روش های ارزیابی فناوری های دفاع سایبری
- چگونگی تدوین، توسعه و پیاده سازی خط مشی های امنیتی
 - نحوه رعایت تعادل میان مخاطرات و نیازمندی های سازمان
 - نحوه شناسایی اهداف تضمین امنیتی
 - نحوه انتخاب فناوری های امنیتی
- راهکارهای انتخاب فناوری های امنیتی مناسب برای سازمان
- روشهای نصب و پیکربندی فناوری های امنیتی
 - دیواره آتش (Firewall)
- چگونگی پیکربندی دیواره آتش برای پشتیبانی از خدمات بیرونی
 - پشتیبانی از خدمات عمومی (HTTP & SMTP)
 - پالایش و مسدودسازی محتوای خطرناک
 - پالایش ترافیک های رمزنگاری شده
 - مدیریت سرویس های پیچیده (VOIP, Audio & Video)
- سازوکار ارائه خدمات ایمن بیرونی
 - پیاده سازی سرویس دهنده های عمومی قابل دسترس
 - ایجاد یک معماری امن برای مناطق نه چندان حفاظت شده (DMZ)
- روش های مجوزدهی دسترسی به خدمات داخلی
 - سفارشی سازی سرویس نام دامنه (DNS) برای معماری های دیواره آتش
 - پیکربندی سرویس ترجمه آدرس شبکه (NAT)



- ایجاد لیست های کنترل دسترسی برای برنامه های کاربردی و کاربران
 - سیستم های تشخیص و جلوگیری از نفوذ (IPS & IDS)
 - بکارگیری سیستم های تشخیص و جلوگیری از نفوذ
 - مکانیابی سیستم های تشخیص و جلوگیری از نفوذ در معماری شبکه سازمان
 - قراردعی حسگرهای عملیاتی در حالت پنهان
 - کشف نفوذ در سازمان
 - طراحی سیستم های تشخیص و جلوگیری از نفوذ سلسله مراتبی چند لایه ای در شبکه سازمان
 - مدیریت یکپارچه سیستم های تشخیص و جلوگیری از نفوذ توزیع شده
 - هشدارهای امنیتی
 - کاهش خطاهای مثبت و منفی
 - اعتباربخشی رویدادها و تشخیص حملات
 - فرایندهای پاسخ فعال به رویدادها و حوادث
 - ضدبدافزار
 - ضدویروس
 - پیکربندی کاربران راه دور شبکه های خصوصی مجازی (VPN)
 - ایجاد تونل های VPN
 - پشتیبانی از کاربران راه دور با پروتکل تونل زنی لایه ۲ (L2TP)
 - اتصال سایت های راه دور با پروتکل تونل زنی لایه ۳ (IPSec)
 - توسعه راه حل های کاربری
 - ارزیابی کاربران راه دور VPN
 - پیاده سازی سازوکارهای هویت سنجی کاربران راه دور VPN
 - الگوریتم های احراز هویت تونل های VPN
 - الگوریتم های رمزنگاری و درهم سازی تونل های VPN
 - ارزیابی امنیتی پروتکل های تونل زنی
 - روش های حفاظت از تونل های VPN
 - فناوری ها و تجهیزات سخت افزاری VPN
 - مدیریت گواهینامه های دیجیتال از طریق PKI
 - اصول یکپارچه سازی اجزای دفاعی سازمان
 - روش های کاهش تأثیر حملات سایبری
 - بررسی معماری های امنیتی شبکه
 - روش های دفاع عمقی
 - روش های اجرایی مقاوم سازی سیستم های عملیاتی سازمان.



۲.۱۰ راهبردهای امن سازی زیرساخت های حیاتی

همزمان با گسترش روز افزون فناوری های نوین در زیرساخت های حیاتی و منابع کلیدی کشورمان، مباحث مربوط به امنیت آنها نیز در عین وجود کارایی، از اهمیت بسیار بالایی برخوردار است چرا که هرگونه آسیب جدی به این زیرساخت های حساس میتواند لطمات جبران ناپذیری را برای آن سازمان ها و همچنین شمار زیادی از شهروندان در برداشته باشد.

در این دوره آموزشی، مخاطبان ضمن آشنایی کامل با زیرساخت های حیاتی و تجهیزات امنیتی مورد استفاده در آنها با راهکارهای امن سازی و تأمین امنیت در زیرساخت های حیاتی، مطابق با استانداردهای بین المللی و بهترین تجربه های جهانی آشنا شده و میتوانند طرح های جامع امنیتی را که دربرگیرنده نیازهای اصلی زیرساخت های حیاتی در کشورمان است، در این مراکز کلیدی، اجرا و پیاده سازی کنند.

سرفصل ها و محتوای این دوره عبارت است از:

- سازمان های حیاتی و غیرحیاتی
 - آیا میتوان میان سازمان های حیاتی و غیرحیاتی، تمایز قایل شد؟
 - تعاریف زیرساخت حیاتی
 - مهمترین جنبه های امنیتی سازمان های حیاتی
 - رویکرد شبکه ای به زیرساختهای حیاتی
 - متدولوژی های شناسایی و طبقه بندی زیرساخت های حیاتی
- آشنایی با سازمان های حیاتی و منابع کلیدی
 - طبقه بندی 18 گانه زیرساخت های حیاتی
 - حوزه های موجود در هر گروه از زیرساخت های حیاتی
 - سازمان ها و نهادهای مسئول حفاظت از هر گروه از زیرساخت های حیاتی
- زیرساخت های مهم فناوری اطلاعات در سازمان های حیاتی
 - دلایل اهمیت ویژه به فناوری اطلاعات در زیرساخت های حیاتی
 - نقش فناوری اطلاعات در تولیدات و خدمات زیرساخت های حیاتی
 - لزوم توجه به امنیت فناوری اطلاعات در زیرساخت های حیاتی
 - زیربخش های مهم فناوری اطلاعات در زیرساخت های حیاتی
- آشنایی با مفاهیم امنیت اطلاعات
 - اجزای اصلی امنیت اطلاعات
 - عناصر و مؤلفه های کلیدی امنیت اطلاعات
- اصطلاح ها و واژگان امنیت اطلاعات
- چرا امنیت اطلاعات در سازمان های حیاتی مهم است؟
 - جایگاه حفاظت از اطلاعات در بقای سازمان های حیاتی



- تهدیدها و مخاطرات متوجه زیرساخت های حیاتی
- روش های پاسخگویی به رخدادهای امنیتی در زیرساخت های حیاتی
- بردار تکامل حملات به سازمان های حیاتی در طول زمان
- سازوکارهای نفوذ به سازمان های حیاتی
- انواع بدافزارهای مشاهده شده در سازمان های حیاتی
- ضرورت توجه به امنیت اطلاعات در سازمان های حیاتی
 - نحوه گزارش رخدادهای امنیتی در زیرساخت های حیاتی
 - چگونگی تشخیص تهدیدات در زیرساخت های حیاتی
 - زمان های لازم برای تشخیص تهدیدات در زیرساخت های حیاتی
 - نقش دارایی های لیست نشده در بروز تهدیدات در زیرساخت های حیاتی
 - نواحی خطر متوجه زیرساخت های حیاتی
 - عوامل تأثیرگذار بر امنیت در زیرساخت های حیاتی
- ارتباط زیرساخت های حیاتی با فضای سایبر
 - تاریخچه حملات سایبری به سازمان های حیاتی
 - نمونه هایی از حمله سایبری به سازمان های حیاتی
 - آشنایی با انواع حملات در سازمان های حیاتی
 - مفاهیم و تعاریف حمله سایبری
 - اکسپلویت ها و سوءاستفاده از آسیب پذیری های سیستم
 - حملات قابل انجام در زیرساخت های حیاتی
- بررسی انواع حملات سازمانی در سازمان های حیاتی
 - حملات داخلی و حملات بیرونی به زیرساخت های حیاتی
 - اهداف و تأثیر حملات داخلی و بیرونی به زیرساخت های حیاتی
 - دیگر حملات شایع به زیرساخت های حیاتی
 - روش های جلوگیری و مقابله با حملات به زیرساخت های حیاتی
- آشنایی با انواع آسیب پذیری و نفوذ به سازمان های حیاتی
 - مفاهیم آسیب پذیری
 - عناصر تشکیل دهنده آسیب پذیری در سامانه های حیاتی
 - چهار روش اصلی برای نفوذ به سیستم های زیرساخت های حیاتی
 - متدولوژی نفوذ به شبکه سامانه های حیاتی
 - روش های جلوگیری از نفوذ به شبکه سامانه های حیاتی
- آشنایی با انواع آسیب پذیری و تهدیدات امنیتی سازمان ها
- دلایل توجه به امنیت سازمان های حیاتی
 - نقش حساس سازمان های حیاتی در خدمات رسانی
 - تهدیدات و حملات نوظهور در سازمان های حیاتی



- تأثیرات اقتصادی، فرهنگی و سیاسی
- پیامدهای ناشی از انتشار آسیب پذیری در زیرساخت های حیاتی
- ارزیابی عملکرد سازمان های حیاتی در شرایط بحرانی
- جنبه های امنیتی سازمان های حیاتی
 - دسترسی غیرمجاز به نرم افزارهای کنترل کننده سیستم های کنترل صنعتی
 - تأثیر کارمندان ناراضی، در بروز تهدیدات داخلی
 - مسایل مرتبط با امنیت ملی در حفاظت از زیرساخت های حیاتی
- مهمترین اولویت های نیازهای امنیتی سازمان های حیاتی
 - ارتباطات اضطراری در زیرساخت های حیاتی
 - ارزیابی خطر در زیرساخت های حیاتی
 - آموزش اولین پاسخ دهندگان در زیرساخت های حیاتی
 - امنیت سایبر در زیرساخت های حیاتی
 - امنیت بیومتریک و هویت سنجی در زیرساخت های حیاتی
- مهمترین مخاطرات امنیتی سازمان های حیاتی و روش های جلوگیری از آنها
- مخاطرات امنیتی کارمندان سازمان های حیاتی از دیدگاه SANS
- ضرورت توجه به آموزش کارکنان برای گزارش حوادث امنیتی
- چرا سازمان های حیاتی در برابر مخاطرات امنیت اطلاعات، آسیب پذیرند؟
- وظایف سازمان های حیاتی در مواجهه با مخاطرات امنیتی
 - نحوه شناسایی مخاطرات و جمع آوری شواهد وقوع رخدادهای امنیتی
 - اصول حاکم بر تدوین طرح تداوم خدمات سازمان های حیاتی
 - برنامه های بازیابی از وضعیت خرابی در زیرساخت های حیاتی
 - دارایی های حیاتی و دارایی های سایبری در زیرساخت های حیاتی
- پنج قدم مهم در مدیریت مخاطرات، بر اساس ISO/IEC ۲۷۰۰۵
- چالش های امنیتی فراروی سازمان های حیاتی
 - آسیب پذیری های موجود در تجهیزات مورد استفاده سازمان های حیاتی
 - مشکلات امنیتی معماری شبکه و سیستم های سازمان های حیاتی
 - مشکلات امنیتی استفاده از بسترهای فناوری اطلاعات
 - گزارشات مربوط به حملات و آسیب پذیری ها به زیرساخت های حیاتی
 - تناسب بین کنترل های امنیتی و رخدادهای امنیت سایبری در زیرساخت های حیاتی
 - پیاده سازی اقدامات جبرانی برای تهدیدهای جدید
 - نقش زمان در پاسخ دهی به تهدیدات
 - وظایف سازمان های یاری رسان در هنگام بروز تهدیدات امنیتی به زیرساخت های حیاتی
- مهمترین مشکلات امنیتی سازمان های حیاتی
- امنیت سازمان های حیاتی در آمریکا



- وظایف رئیس جمهور های پیشین در امنیت زیرساخت های حیاتی ملی
- جایگاه کنگره ملی در امنیت زیرساخت های حیاتی
- نقش امنیت سایبر در امنیت ملی آمریکا
- اقدامات اوباما در حوزه امن سازی زیرساخت های حیاتی آمریکا
- نیروهای نظامی سایبری آمریکا جهت حفاظت از زیرساخت های حیاتی
- فعالیت های تهاجمی ارتش سایبری آمریکا به زیرساخت های حیاتی سایر کشورها
- بررسی قانون حفاظت از زیرساخت های حیاتی در آمریکا
 - بررسی قانون بهبود امنیت سایبری زیرساخت های حیاتی
 - نکات کلیدی در قانون حفاظت از زیرساخت های حیاتی آمریکا
 - نحوه تعامل سازمان های دولتی و خصوصی برای اجرای این قانون
 - سیاست های ایالات متحده آمریکا در حفاظت از زیرساخت های حیاتی
 - استراتژی های امن سازی زیرساخت های حیاتی در این قانون
 - مشکلات فنی و عملیاتی اجرای این قانون
 - جایگاه متدولوژی، در مدیریت تهدیدات سایبری به آمریکا
- چارچوب امنیت رایانه آمریکا در زیرساخت های حیاتی
- آشنایی با سیستم های مدیریت امنیت در زیرساخت های حیاتی
- استانداردهای امنیت سازمان های حیاتی
 - ISO
 - NIST
 - IETF
- طرح ها و متدولوژی های کاهش مخاطره در زیرساخت های حیاتی
 - انواع مخاطرات امنیت اطلاعات مطرح در متدولوژی های مدیریت مخاطره زیرساخت های حیاتی
 - روش های مدیریت مخاطره در زیرساخت های حیاتی
 - انواع رویدادها و رخدادهای امنیتی در زیرساخت های حیاتی
 - سناریوهای امنیتی مطرح در تعیین سطح مخاطرات دارایی های موجود در زیرساخت های حیاتی
 - اصول مهم امنیت اطلاعات در تعیین سطح مخاطرات در زیرساخت های حیاتی
 - سناریوهای ارزیابی مخاطرات در متدولوژی های مدیریت مخاطره در زیرساخت های حیاتی
 - روش های برخورد با مخاطرات در متدولوژی های مدیریت مخاطره در زیرساخت های حیاتی
 - فرایندهای اصلی مدیریت مخاطرات در متدولوژی های مدیریت مخاطره در زیرساخت های حیاتی
 - روش های پاسخ به مخاطرات در زیرساخت های حیاتی
 - متدولوژی مدیریت مخاطرات در زیرساخت های حیاتی
 - چارچوب های مطرح در حوزه مدیریت مخاطرات در زیرساخت های حیاتی
- فرایندهای بهبود امنیت در زیرساخت های حیاتی
- استراتژی ها و راهکارهای جامع امن سازی سازمان های حیاتی
 - استراتژی ها و راهکارهای جامع NIST



- استراتژی های ملی چند کشور مورد مطالعه
- استراتژی ها و راهکارهای ایران در خصوص امن سازی زیرساخت های حیاتی
- بهترین تجربه های موجود در این حوزه
- راهبردهای امن سازی زیرساخت های حیاتی، در اسناد بالادستی کشور
- روش های اجرایی فراهم آوری امنیت در سازمان های حیاتی
- چگونگی پیاده سازی روش های اجرایی امنیتی در زیرساخت های حیاتی
- کنترل های حیاتی برای دفاع اثربخش سایبری در سازمان های حیاتی
- معماری های امنیتی و دفاع در عمق در زیرساخت های حیاتی
- استراتژی های امنیتی توافقی نامی های شخص سوم در زیرساخت های حیاتی
- مستندسازی امنیتی در حوزه زیرساخت های حیاتی
 - انواع سندهای امنیتی
 - اصول کلی در مستندسازی امنیتی
 - الزامات یک سند امنیتی
 - سیستم کدگذاری سندهای امنیتی
 - استانداردهای موجود در حوزه مستندسازی امنیتی
- امنیت سایبری در سازمان های حیاتی؛ جنگ و دفاع سایبری
- چند نکته مهم در امنیت اطلاعات سازمان های حیاتی
- امن سازی سیستم های کنترل صنعتی مورد استفاده در زیرساخت های حیاتی
- قوانین حقوقی در رابطه با امنیت زیرساخت های حیاتی در ایران
- انجمن ها و مؤسسات پژوهشی در حوزه امن سازی سازمان های حیاتی
- بررسی اسناد و راهنما های امنیتی NIST
- آشنایی با فعالیت های DHS در حوزه مدل سازی امنیت میهن
- بهترین تجارب جهانی در رابطه با امن سازی سازمان های حیاتی ملی
- آشنایی با توانمندی های نظامی جمهوری اسلامی ایران در حوزه دفاع از سازمان های حیاتی
- مخفف واژگان و اصطلاحات مورد استفاده در زیرساخت های حیاتی.



۲.۱۱ مدل بلوغ امنیت اطلاعات

مدل بلوغ امنیت، ابزاری برای سنجش سطح بلوغ امنیت یک سازمان است. بدون استفاده از مدل بلوغ، تصمیم گیری درباره وضعیت فعلی امنیت سازمان و برنامه ریزی جهت ارتقای آن بسیار دشوار است. در واقع، مدل بلوغ امنیت نشان میدهد که فعالیت های امنیتی سازمان، تا چه حد به بهبود وضعیت امنیت در آن سازمان کمک کرده است و نقاط ضعف امنیتی در چه بخش هایی وجود دارند.

در این دوره آموزشی، شرکت کنندگان با متدولوژی ها و معیارهای اندازه گیری بلوغ امنیت اطلاعات در سازمان آشنا میشوند.

سرفصل ها و محتوای این دوره عبارت است از:

- مفهوم بلوغ مدیریت امنیت اطلاعات
- آشنایی با فرایندها و معیارهای امنیت اطلاعات
- سطوح بلوغ امنیت اطلاعات
- شناسایی شاخص های سنجش میزان بلوغ امنیت اطلاعات
- به کارگیری معیارهای سنجش میزان بلوغ فرایندهای امنیت اطلاعات و اهداف امنیتی
- مدل فرایندی بلوغ مدیریت امنیت اطلاعات
- روش های مدیریت مخاطرات امنیتی
- مدیریت استراتژیک امنیت اطلاعات
- مدیریت تاکتیکی امنیت اطلاعات
- مدیریت عملیاتی امنیت اطلاعات
- نقش مدیریت استراتژیک تاکتیکی و عملیاتی در ارتقای بلوغ امنیت اطلاعات.

۲.۱۲ امنیت کاربر رایانه (CSCU)

هر کاربر رایانه باید روش حفاظت از داراییهای اطلاعاتی خود و نحوه اتصال ایمن به سیستمهای دیگر را در شبکه بداند. دوره آموزشی، CSCU دانش امنیت اطلاعات و شبکه یک کاربر رایانه را در استفاده از منابع رایانههای در داخل شبکه سازمان و یا حین اتصال به اینترنت ارتقا میدهد. اخذ گواهینامه این دوره، بیانگر آن است که دارنده این مدرک، شایستگی و دانش استفاده از مهارتهای شبکههای رایانههای را دارا بوده و مفاهیم ضروری امنیت اطلاعات را میداند.

سرفصل ها و محتوای این دوره عبارت است از:

- مقدمه ای بر اساس امنیت اطلاعات
- نحوه امن سازی سیستم عامل
- حفاظت از سیستم ها توسط ضدویروس ها
- رمزنگاری اطلاعات



- تهیه نسخه پشتیبان و بازیابی اطلاعات
- امنیت در اینترنت
- امن سازی ارتباطات در شبکه
- امن سازی تبادلات آنلاین
- امن کردن ارتباطات پست الکترونیک
- تهدیدهای مهندسی اجتماعی و راهکارهای مقابله با آن
- امنیت در شبکه های اجتماعی
- امنیت اطلاعات و انطباق های قانونی
- امن سازی تلفن های همراه.

۲.۱۳ تهدیدها و آسیب های فضای مجازی

همزمان با گسترش فناوری اطلاعات و ابزارهای دیجیتال در زندگی روزمره شهروندان، پیشگیری از آسیب ها و تهدیدات ناشی از این فناوری های هوشمند، به دغدغه بسیاری از مردم تبدیل شده است. از سوی دیگر، با رشد سریع شبکه های اجتماعی در طول چند سال گذشته، موج جدیدی از مخاطرات امنیتی، با هدف تغییر الگوی زندگی شهروندان شکل گرفته است که نیازمند آموزش تمام اقشار جامعه و همچنین توجه جدی به این مسأله است.

در این دوره آموزشی، مخاطبان ضمن آشنایی کامل با آسیب ها و تهدیدات شبکه های اجتماعی و فضای مجازی میتوانند با استفاده از راهکارها و رهنمودهای ارائه شده در خصوص امنیت در این شبکه های مجازی، از بروز مشکلات ناخواسته برای خود و خانواده شان جلوگیری کنند.

سرفصل ها و محتوای این دوره عبارت است از:

- شبکه های اجتماعی مجازی و بررسی تطبیقی کارکرد آنها از منظر محتوایی
- آسیب ها و تهدیدات اجتماعی، امنیتی، اقتصادی و سیاسی شبکه های اجتماعی
- آسیب ها و تهدیدات فردی ناشی از نقض حقوق کاربران در فضای مجازی
- شبکه های اجتماعی و آسیب های فردی و اجتماعی
- جرایم رایانه ای و حقوقی در شبکه های اجتماعی مجازی
- انواع مجرمان و اهداف جرایم رایانه ای در شبکه های اجتماعی
- اخلاق فناورانه در شبکه های اجتماعی مجازی
- امنیت کاربران در فضای مجازی
- چالش ها و تهدیدات نوظهور در شبکه های اجتماعی
- انتشار اطلاعات در شبکه های اجتماعی و پیامدهای فرهنگی و سیاسی آن
- نقش شبکه های اجتماعی در شکل گیری باندهای جاسوسی، جرم و فساد.



۲,۱۴ مدیریت امنیت اطلاعات در گزینش و استخدام کارکنان

رعایت اصول امنیتی در گزینش و استخدام کارکنان، برای افرادی که در فرایندهای اشتغال به کار کارمندان نقش دارند از اهمیت ویژه ای برخوردار است. شرکت کنندگان، در پایان این دوره علاوه بر آشنایی کامل با کنترل ها و الزام های امنیتی در مراحل گزینش، حین خدمت، تغییر شغل یا خاتمه استخدام کارکنان میتوانند امنیتی پایدار را برای مجموعه سازمانی خویش، از طریق اعمال کنترل های امنیتی خاص کارکنان به دست آورند.

سرفصل ها و محتوای این دوره عبارت است از:

- آشنایی با امنیت اطلاعات و الزام های امنیتی
- نحوه شناسایی نیازمندی های امنیت اطلاعات سازمان
- چگونگی برآورد مخاطرات امنیت اطلاعات مرتبط با کارکنان
- آشنایی با امنیت منابع انسانی، پیش از اشتغال و در مرحله گزینش
- آشنایی با ضوابط و شرایط استخدام کارکنان
- آشنایی با نحوه تنظیم تفاهم نامه های عدم افشای اطلاعات
- انتخاب و پیاده سازی کنترل های امنیتی خاص کارمندان
- چگونگی فراهم آوری امنیت اطلاعات در حین خدمت کارمندان
- آشنایی با نحوه تدوین فرایندهای انضباطی
- چگونگی تأمین امنیت اطلاعات پس از خاتمه استخدام یا تغییر شغل کارکنان.



۳ اطلاعات تماس

وب سایت: www.security.raja.ac.ir

تلفن ثابت: 021-66409288

ایمیل: IT@RAJA.AC.IR