€TRAINING

استراتيجيات أمن الوثائق والمعلومات الإلكترونية

29 ديسمبر 2024 - 2 يناير 2025

القاهرة (مصر)

استراتيجيات أمن الوثائق والمعلومات الإلكترونية

رمز الدورة: J569 تاريخ الإنعقاد: 29 ديسمبر 2024 - 2 يناير 2025 دولة الإنعقاد: القاهرة (مصر) - التكلفة: 3520 يورو

مقدمة البرنامج التدريبي:

يهدف هذا البرنامج إلى تزويد المشاركين بالمعرفة والمهارات اللازمة لتأمين الوثائق والمعلومات الإلكترونية ضد المخاطر السيبرانية والهجمات الإلكترونية. حيث يركز على كيفية تطوير وتنفيذ استراتيجيات فعالة لحماية البيانات، وضمان السرية والنزاهة، وتطبيق أحدث تقنيات التشفير والحماية. ويشمل أيضاً تطبيقات عملية لحماية الوثائق الإلكترونية في البيئات المؤسسية.

أهداف البرنامج التدريبي:

في نهاية هذا البرنامج، سيكون المشاركون قادرين على:

- اكتشاف التهديدات والمخاطر التي تواجه الوثائق والمعلومات الإلكترونية.
- تطبيق تقنيات التشفير لحماية المعلومات والوثائق.
- تطوير سياسات أمنية لضمان حماية الوثائق الإلكترونية.
- إدارة صلاحيات الوصول لضمان حماية المعلومات الحساسة.
- تنفيذ خطط الاستجابة للطوارئ لضمان استمرارية العمل.

الفئات المستهدفة:

- مسؤولو تكنولوجيا المعلومات والأمن السيبراني.
- مدراء الوثائق والأرشفة.
- مدراء المخاطر.
- مسؤولو الموارد البشرية والإدارة.
- الموظفون في قسم حفظ وإدارة الوثائق الإلكترونية.

محاور البرنامج التدريبي:

الوحدة الأولى:

مقدمة في أمن الوثائق الإلكترونية:

- تعريف أمن الوثائق وأهميته في البيئة المؤسسية.
- التهديدات السيبرانية التي تواجه الوثائق الإلكترونية.
- مبادئ السرية والنزاهة والتوافر في حماية المعلومات.
- كيفية تقييم المخاطر والتهديدات الأمنية.
- الهجمات الإلكترونية وكيفية التصدي لها.

الوحدة الثانية:

تقنيات التشفير وحماية البيانات:

- أهمية التشفير في حماية البيانات الحساسة.
- أنواع التشفير المستخدمة في حماية الوثائق.
- كيفية استخدام التوقيع الإلكتروني لضمان سلامة الوثائق.
- إدارة مفاتيح التشفير وتأمين الوثائق الإلكترونية.

- دراسة حالة حول تطبيق تقنيات التشفير في المؤسسات الكبرى.

الوحدة الثالثة:

إدارة الصلاحيات والوصول إلى الوثائق الإلكترونية:

- تحديد الصلاحيات والتحكم في الوصول إلى الوثائق الحساسة.
- كيفية استخدام أنظمة إدارة الهوية للتحقق من المستخدمين.
- تقنيات إدارة حقوق المعلومات IRM لحماية الوثائق.
- تطبيق سياسات الوصول على المستويات المختلفة في المؤسسة.

الوحدة الرابعة:

استراتيجيات الحماية من الهجمات السيبرانية:

- كيفية حماية الوثائق الإلكترونية من الهجمات السيبرانية.
- تقنيات الدفاع المتقدم مثل جدران الحماية والأنظمة المضادة للاختراق.
- أهمية مراقبة الأنظمة واكتشاف الأنشطة غير المعتادة.
- طرق تطوير خطط استجابة للحوادث والتهديدات السيبرانية.
- تنفيذ خطط الطوارئ لضمان استمرارية العمل في حالات الاختراق.

الوحدة الخامسة:

السياسات والإجراءات الأمنية لإدارة الوثائق:

- كيفية تطوير سياسات أمنية شاملة لحماية الوثائق الإلكترونية.
- الامتثال للمعايير واللوائح الدولية المتعلقة بحماية المعلومات.
- تقييم فعالية السياسات الأمنية وتحسينها بشكل مستمر.
- دور تنفيذ دورات تدريبية للتوعية الأمنية بين الموظفين.
- مراقبة وتقييم الأنظمة لضمان الامتثال للسياسات الأمنية.