EFICIENCIA GERENCIAL Y PRODUCTIVIDAD S.A.C.
Av. Del Pinar N° 134, Edificio el Pinar II, Oficina 803, Chacarilla del Estanque, Santiago de Surco, Lima, Perú
Teléfonos: +51 372-1441 | 372-1415
www.gerenciayproductividad.com

DIPLOMADO

EN

SEGURIDAD DE INFORMACIÓN EMPRESARIAL

Introducción.-

Hoy en día lo impensado está a la vuelta de la esquina. Los sistemas informáticos en las organizaciones, en cualquier momento pueden recibir un ciberataque y comprometer seriamente a sus sistemas de información tales como: base de datos, redes computacionales, servidores, servicios, dispositivos móviles y sistemas electrónicos. Los ataques cibernéticos generados por manos criminales están siempre latentes y en cualquier momento pueden ponerse de manifiesto.

Las empresas tienen que estar preparadas para poder proteger sus sistemas de información. Si se presenta un ciberataque de cualquier índole, la firma debe tener la capacidad de poder rápidamente actuar y mitigar el incidente.

El tema de cloudcomputing con todos los aspectos que comprende tales como servicios de aprovisionamiento, almacenamiento, infraestructura de procesamiento, servicios de soporte cloud, seguridad perimétrica y de red cloud, tienen que estar protegidos adecuadamente contra ciberataques y posibles daños cibernéticos.

Este diplomado está orientado a desarrollar las distintas competencias que deben instaurarse en una empresa para estar preparada con el fin de enfrentar a los ciberataques de distintas modalidades.

Resultados Esperados del Diplomado.-

El participante al terminar el Diplomado, habrá adquirido las siguientes competencias:

- Entender cómo opera un sistema de seguridad de información empresarial bajo la nueva óptica del ISO 27001:2021.
- Conocer cómo se gestiona el riesgo en una organización bajo la óptica del ISO 31000:2018.
- Conocer como aplica la ciberseguridad a cloud computing.
- Saber gestionar e instaurar controles de seguridad de información.
- Conocer los aspectos legales, regulatorios, la ley de protección de datos personales y su impacto en la seguridad de información.
- Entender cómo se realiza una auditoría a sistemas de seguridad de información.

Estructura del Diplomado.-

El diplomado consta de seis cursos (Ver Figura Nº 1), cada uno tiene una duración de 9 horas. Todo el programa dura 54 horas. El participante recibirá un certificado por cada curso al que atienda. Al completar los cinco cursos, se otorgará un certificado por haber culminado el programa completo del diplomado y haberlo aprobado.

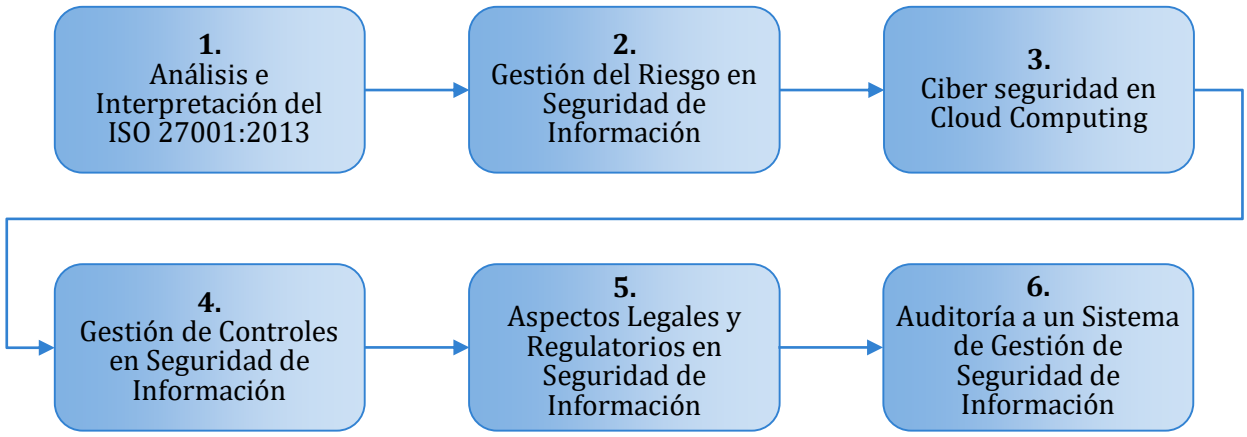
Habrá un examen después de cada curso. Para graduarse el participante debe haber aprobado cada uno.

Horario: El Diplomado se desarrolla en su totalidad bajo la modalidad "Online", de 7:00PM a 10:00PM, hora de Lima, Perú.

Plataforma: Zoom

Figura Nº 1

Estructura del Diplomado en Seguridad Empresarial



Metodología.-

Se utilizarán "técnicas de aprendizaje acelerado", para generar toda una dinámica que facilite el proceso de enseñanza-aprendizaje. Todo esto se complementará con juegos de simulación.

Cada participante recibirá un material de lectura, el cual se convertirá en una referencia importantísima, para su constante consulta en el futuro. Cada alumno debe tener a su disposición el estándar ISO 27001:2013.

DESCRIPCIÓN DEL DIPLOMADO

A continuación, se hace una breve descripción de los cursos que comprende el Diplomado en Sistemas de Gestión de la Seguridad Empresarial. (Ver Figura Nº 1).

Análisis e Interpretación del ISO 27001:2013

Propósito.-

El curso está orientado a entender los requerimientos del sistema de gestión de seguridad de información ISO 27001:2013. Se hará hincapié en los cambios que contempla el ISO 27001:2021 y el ISO 27002:2021.

Temario:

- Entender los requerimientos del ISO 27001:2013.
- Conocer la nueva estructura de controles en el ISO 27002:2021.
- Requerimientos focales y globales.
- Controles relacionados con ciberseguridad en el ISO 27002:2021.
- Aspectos de ciber defensa en el nuevo estándar.

Gestión del Riesgo en Seguridad de Información

Propósito.-

El curso tiene la finalidad de desarrollar las competencias para entender el proceso de valuación del riesgo en un contexto de seguridad de información. Se usará como enfoque metodológico el ISO 31000:2018.

Temario:

- Valuación del riesgo: análisis y evaluación.
- Dinámica y enfoque metodológico del ISO 31000:2018
- Metodología para la identificación de ciber riesgos.
- Enfoque metodológico para la medición del riesgo residual.
- Identificación de opciones de tratamiento y elaboración de un plan de tratamiento del riesgo.

Ciber Seguridad en Cloud Computing

Propósito.-

El curso tiene la finalidad de desarrollar las competencias para entender los aspectos de seguridad de los activos que residen en servicios tercerizados basados en nube. Se usará como enfoque metodológico las buenas prácticas existentes en la industria.

Temario:

- Identificación de tipos de infraestructura tercerizadas.
- Estándares y buenas prácticas entorno a la seguridad de la información para servicios tercerizados.
- Modelo de gestión de ciberseguridad basada en funciones.
- Modelo de gestión de controles para servicios en nube.

Gestión de Controles en Seguridad de Información

Propósito.-

El curso está orientado a entender los distintos controles del nuevo estándar ISO 27002:2021. Se hará énfasis en la naturaleza del control, su implantación y gestión.

Temario:

- Estructura de controles en el nuevo modelo ISO 27002:2021.
- Nueva categorización de controles: personas, físicos, tecnológicos y organizacionales.
- Análisis e interpretación de los controles más relevantes.
- Indicadores para medición del desempeño de controles.
- Implantación de los controles.

Aspectos Legales y Regulatorios en Seguridad de Información

Propósito.-

El curso tiene la finalidad de desarrollar las competencias para entender los aspectos legales y regulatorios en la que debe de operar la seguridad de la información. Se usará como enfoque metodológico las disposiciones emitidas por el país.

Temario:

- Aspecto legal entorno a la protección de datos personales.
- Evaluación de impacto a la privacidad.
- Aspecto legal entorno a los delitos informáticos.
- Convenio internacional entorno a delitos informáticos.
- Aspectos regulatorios, a nivel de banca y seguros, en seguridad de la información.

Auditoría a un Sistema de Gestión de Seguridad de Información

Propósito.-

El curso está orientado a desarrollar las competencias para auditar de una manera eficaz y eficiente un sistema de gestión de seguridad de información. Se hará hincapié en aspectos de planificación, ejecución y evaluación de una auditoría.

Temario:

- Auditorías a sistemas de gestión de seguridad de información.
- Criterios de auditoría, identificación de hallazgos.
- Planificación de auditorías: plan de auditoría y listas de chequeo.
- Ejecución de auditorías: recolección de información y entrevistas.
- Evaluación de auditorías: Contenido de un informe de auditoría.

Plana Docente del Programa

Alberto G. Alexander, Ph.D The University of Kansas, M.A. Northern Michigan University. Auditor Líder Certificado ante IRCA en: Sistemas de Gestión de Calidad, Seguridad de la Información y en Continuidad del Negocio. Certificado en Gestión de Resilencia y en Auditoría ante el BRCCI de Estados Unidos.

Miembro del Business Continuity Institute (MBCI).

Experiencias internacionales en asesoría a empresas y en auditoría en los estándares: ISO 9001, ISO 27001, ISO 20000 y en ISO 22301. El Dr. Alexander ha asistido a diversas compañías en variadas industrias, implementando y llevándolas a obtener la certificación internacional.

Ha publicado los siguientes libros: La Mala Calidad y Su Costo, Addison Wesley, 1994, USA. Implementación del ISO 9000, Addison Wesley, 1995, USA. Manual para Documentar Sistemas de Calidad Prentice Hall, 1999, México. Metodología para la Mejora Continua, Prentice Hall, 2002, México. Diseño y Gestión de un Sistema de Gestión de Seguridad de Información ISO 27001:2005 Alfa Omega, Colombia 2007.

En septiembre del 2009, el Business Continuity Journal, Volume three, Issue four de Inglaterra, publicó su artículo: Metodología para el desarrollo del Business Impact Analysis. En 2016 la Revista Continuity Central del Business Continuity Institute, de Inglaterra, le publicó los siguientes artículos: "A Methodology for Developing a Business Continuity Strategy", "Operations Resumption Planning: A Managerial Approach", "Planning and Managing Exercises for Business Continuity Management Arrangements". "Maintenance of a Business Continuity Management System: A Managerial Approach." En el 2017 la Revista Continuity Central del Business Continuity Institute, Inglaterra, le publicó: "Enterprise Risk Management and Business Continuity" y "Methodology for Developing a Business Impact Analysis.". En el año 2018, la Revista Continuity Central del Business Continuity Institute, Inglaterra, le publicó el artículo: "Implementing Enterprise Risk Management".

El libro más reciente del Dr. Alexander, es: "Business Continuity Management Process" publicado bajo el sello de Amazon, 2018. EE.UU.

La Revista Continuity Central del Business Continuity Institute, publicó la lista de los 10 artículos publicados durante el 2017, que más se leyeron. El artículo "Enterprise Risk

Management and Business Continuity", del Dr. Alexander, quedó como el Segundo artículo más leído.

En el 2018, el artículo "Implementing Enterprise Risk Management", del Dr. Alexander, quedo entre los 15 artículos más leídos, publicados por La Revista Continuity Central.

El Dr. Alexander ha realizado auditorías de certificación representando a empresas certificadoras en: Sistemas de Gestión de Calidad, Sistemas de Continuidad del Negocio, Sistemas de Seguridad de Información y en Sistemas de Gestión de Servicios de Tecnología de Información.

Formó parte del grupo de profesionales que fundo "CENTRUM Católica", la escuela de negocios de la Pontificia Universidad Católica del Perú. Durante su gestión, desempeñándose como Director Académico, dirigió los proyectos de implantación y certificación del ISO 9001 en todos los programas académicos de la Institución, así como la instauración y acreditación de la Escuela de Negocios, con el estándar The Association of MBA´s "AMBA".

Es un tutor aprobado IRCA para el dictado de Programas de Auditor Líder en estos estándares. También es tutor aprobado para el dictado de los cursos del Business Continuity Institute.

Actualmente es el Director Gerente de Eficiencia Gerencial y Productividad S.A.C. Empresa Internacional ofreciendo servicios de capacitación gerencial y de asesoría empresarial. www.gerenciayproductividad.com

Es profesor en la Escuela de Negocios de Postgrado de la Universidad ESAN. Lima, Perú.

Ángela Marina Pattini

Maestría en Gestión de la Seguridad de Información Empresarial, Universidad de Barcelona y OBS Business School, España. Maestría en Sistemas de Información, Universidad Simón Bolívar, Caracas, Venezuela. Ingeniero en Electrónica, IUPFAN, Maracay, Venezuela. Posee una amplia experiencia internacional en el diseño e implantación de Sistemas de Gestión de Seguridad de Información, Sistema de Gestión Continuidad del Negocio, Sistemas de Gestión de Calidad y en Sistemas de Gestión de Servicios de Tecnología de Información.

Auditor líder certificado, IRCA en Sistemas de Gestión de Seguridad de Información, Continuidad del Negocio y Sistemas de Gestión de Calidad. Experiencia realizando certificaciones a empresas bajo el estándar ISO 27001:2013 y bajo el esquema ISO 22301:2019. Gerente de Operaciones y consultor principal de Eficiencia Gerencial y Productividad S.A.C. sus actividades de consultaría y de auditoría, las complementa como profesora en la Escuela de Negocios de Postgrado de la Universidad ESAN. Lima, Perú.

Gustavo Vallejo La Torre

Es bachiller en Ingeniería Empresarial y de Sistemas graduado en la Universidad San Ignacio de Loyola, Lima, Perú.

Cuenta con certificaciones en protección de datos personales (IAITG-AENOR), gestión de riesgos (G31000), gestión por procesos (ESAN), gobierno de TI (COBIT 5), seguridad de la información (Tecnológico de Monterrey), auditor líder en continuidad de negocios (BSI) y seguridad de la información (IRCA), y metodología de estrategia e innovación (LEGO Serious Play). Así mismo, cuenta con cursos de especialización en arquitectura empresarial (TOGAF), GRC (OCEG) y gestión de identidades (Novell y Oracle).

Es un profesional con más de 20 años de experiencia laboral a nivel internacional, en tecnologías de información, seguridad de la información, continuidad del negocio, riesgo operacional y procesos de negocio. Ha realizado servicios de consultorías y auditorías en sectores tales como: público, militar, salud, banca, minería, telecomunicaciones, retail y seguros.

Consultor asociado de EGP.