SEGURIDAD EN EL CICLO DE VIDA DE DESARROLLO DE SOFTWARE.

CAPACITACIÓN PARA PERSONAL DE LA DIRECCIÓN GENERAL DE SISTEMAS

- PLANIFICACIÓN DE LA PRIMERA ETAPA -

- OBJETIVOS GENERALES:

- Concientizar a los desarrolladores y a los usuarios en materia de seguridad en el software y los datos, con vistas a las buenas prácticas de desarrollo de software y de acuerdo a las implicancias legales.
- Relevar las metodologías de trabajo actuales en la Dirección General de Sistemas (DGS) y tomar conocimiento de las posibilidades de incorporar mejores prácticas y de las limitaciones reales, con el objeto de elaborar políticas y procedimientos que rijan las actividades de seguridad en el ciclo de vida de desarrollo de software (SCVDS/SSDLC).
- Brindar herramientas y pautas de seguridad a los desarrolladores y administradores.
- Establecer formalmente la necesidad de efectuar pruebas de seguridad del software.
- Incluir formalmente controles de seguridad en las aplicaciones, en las infraestructuras que las soportan y en los datos que se procesan, con el fin de monitorear el cumplimiento de las políticas de seguridad de la información, normativas y procedimientos relacionados..
- A largo plazo, definir el proceso para el desarrollo seguro y la elaboración de métricas de la seguridad en el software.

- OBJETIVOS CAPACITACIÓN 2012:

- Exponer conceptos generales del desarrollo seguro de software, de forma tal de que sirvan de guía para el equipo de trabajo durante todo el ciclo de vida de desarrollo del software.
- Explicitar la normativa más comúnmente utilizada para enmarcar el trabajo de desarrollo seguro de software.
- Presentar los lineamientos para la documentación de la gestión de archivos logs de los sistemas informáticos administrados por la Dirección General de Sistemas.

- RESPONSABLES DEL DICTADO:

- Evangelina Giuriati.
- Mauro Meloni.

- MODALIDAD:

- Presencial.

- DESTINATARIOS:

- Personal de la DGS.

- CARGA HORARIA:

- 6 encuentros teórico-prácticos (1 vez por semana) de 3 horas cada uno.

- REQUISITOS PREVIOS:

- Sin requisitos previos, aunque es recomendable haber asistido a las capacitaciones "Ciclo de Conferencias en Seguridad de la Información" y al seminario-taller "Riesgo versus Seguridad Informática".

- FORMA DE EVALUACIÓN:

- La primera etapa de capacitación tendrá evaluaciones, de los contenidos ofrecidos, durante las prácticas efectuadas en el transcurso de los encuentros.

- RECURSOS:

- Presentaciones.
- Videos.
- Internet.

- LUGAR:

- UNLu Sede Central.

- FECHAS:

- 11/09/2012
- 18/09/2012
- 02/10/2012
- 16/10/2012
- 30/10/2012
- 06/11/2012

- HORARIO:

- 11 a 14 hrs.

- CONTENIDOS A DESARROLLAR:

- **1º Encuentro:** ***Presentación – Algunas normas en relación al SSDLC***
  - **Objetivos específicos:**

    Presentar la capacitación, sus objetivos y justificación técnica.
    Presentar el marco normativo y de estandarización que fundamenta y guía la incorporación de la seguridad de la información en el desarrollo de software.
  - **Temas:**

    - Presentación y objetivos de la capacitación.
    - Ley Nº 25326: Protección de los Datos Personales.(Art. 2º, 4º, 9º, 10º, 11º)
    - Disposición DNPDP Nº 11/2006.
    - Presentación del Modelo de Política de Seguridad de la Información 2012.
    - Normas ISO vinculadas a la seguridad de la información
    - Normas generales de control interno SIGEN.
    - Pautas de control interno para la gestión de recursos de información SIGEN.
    - Normas de control interno para tecnología de la información SIGEN.
    - Presentación de Open Web Application Security Project (OWASP).
    - Presentación de National Institute of Standards and Technology (NIST).

- **2º Encuentro:** ***Algunos conceptos básicos en seguridad de la información***
  - **Objetivos específicos:**

    - Dar a conocer los conceptos técnicos relacionados con la gestión de riegos de los activos y procesos de información.

  - **Temas:**

    - Conceptos básicos de la gestión de riesgos.
    - Fundamentos de la seguridad en el SDLC.
    - Importancia de formalizar los requerimientos de seguridad en el SDLC.
    - Documentación e importancia de su comunicación al personal involucrado.
    - Cláusulas del Modelo de Política de Seguridad de la Información: Gestión de accesos; Adquisición, desarrollo y mantenimiento de sistemas.

- **3º Encuentro: Introducción al desarrollo seguro de software: aspectos técnicos. Parte I**
  - **Objetivos específicos:**
    - Presentar la técnica de modelado de amenazas para aplicaciones.
    - Mostrar los beneficios de corregir problemas de seguridad en las primeras etapas del ciclo de desarrollo de software.
  - **Temas:**
    - Introducción a la técnica de modelado de amenazas.
    - Métodos STRIDE y DREAD.
    - Herramienta Threat Analysis & Modeling (TAM).
    - Introducción a los ataques a aplicaciones.

- **4º Encuentro:** ***Introducción al desarrollo seguro de software: aspectos técnicos. Parte II***
  - **Objetivos específicos:**
    - Mostrar los riesgos más críticos y comunes en las aplicaciones web.
    - Dar a conocer los criterios de codificación segura para disminuir el riesgo en las aplicaciones.
  - **Temas:**
    - Riesgos de seguridad en aplicaciones web: OWASP Top 10 .
    - Prácticas de codificación segura.

- **5º Encuentro:** ***Registro de actividades y seguridad de la información***
  - **Objetivos específicos:**
    - Concientizar sobre la necesidad de monitorear los registros de actividades de los sistemas informáticos.
    - Brindar pautas para el desarrollo de los procedimientos de gestión de registros de actividades.
  - **Temas:**
    - Concepto de archivos de actividades y auditoría.
    - Cláusulas del Modelo de Política de Seguridad de la Información: Gestión de accesos; Gestión de comunicaciones y operaciones.
    - Normas generales de control interno SIGEN.
    - Pautas de control interno para la gestión de recursos de información SIGEN-
    - Presentación de las pautas para formular el procedimiento de gestión de registros de auditoría.
    - Presentación de herramientas para automatizar la gestión de registros log.

- **6º Encuentro:** ***Pruebas de seguridad***
  - **Objetivos específicos:**
    - Presentar el concepto de pruebas de seguridad, sus tipos y aplicaciones.
    - Dar a conocer algunas pautas para la implementación de seguridad de la información durante la etapa de prueba de software.
  - **Temas:**
    - Pruebas de seguridad. Concepto y tipos.
    - Las pruebas de seguridad y su relación con el recurso de hábeas data.
    - Cláusulas del Modelo de Política de Seguridad de la Información en relación con la separación de ambientes y funciones: Gestión de comunicaciones y operaciones).
    - Pasaje del ambiente de desarrollo al ambiente de producción.
    - Las pruebas en relación con el control de cambios y el mantenimiento de los sistemas informáticos.

- REFERENCIAS Y BIBLIOGRAFÍA RECOMENDADA:

- Disposición DNPDP 11/06. Recuperado en el mes de agosto de 2012 del sitio web de la Dirección Nacional de Protección de Datos Personales:
http://www.jus.gob.ar/datos-personales/normativa.aspx

- Documentos de OWASP Foundation: **https://www.owasp.org/**

- Guías NIST serie SP 800: **www.nist.gov/**

- Ley 25326. Recuperado en el mes de agosto de 2012 del sitio web de la Dirección Nacional de Protección de Datos Personales: **http://www.jus.gob.ar/datos-personales/normativa.aspx**

- Maggiore, M. ; Prandini, M.(2010). *Normas internacionales y nacionales vinculadas a la seguridad de la información.* Buenos Aires: Osmar D. Buyatti

- Normas generales de control interno. Documento recuperado en el mes de agosto de 2012 del sitio web de la Sindicatura General de la Nación **http://www.sigen.gov.ar/normativa.asp**

- Normas de control interno para tecnología de la información. Documento recuperado en el mes de

agosto de 2012 del sitio web de la Sindicatura General de la Nación:
http://www.sigen.gov.ar/normativa.asp

- Política de seguridad de la información ICIC/PS - 2012. Recuperado del sitio web del Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad: **http://www.icic.gob.ar**

- Sitio web de la familia de normas ISO 27000: **www.27000.org/**

- Sitio web del Departamento de Seguridad Informática de la UNLu:
www.seguridadinformatica.unlu.edu.ar