Universidad Nacional de Luján
REPUBLICA ARGENTINA

UNIV. NAC. DE LUJAN - M.G.E.S.Y.A. - FOLIO 424

Nº DISPOSICION:

- NOMBRE DE LA ACTIVIDAD:

SEMINARIO-TALLER: RIESGO versus SEGURIDAD INFORMÁTICA

-Grupo de Trabajo

Mauro Meloni (Departamento de Seguridad Informática - UNLu)
Evangelina Giuriati (Departamento de Seguridad Informática - UNLu)

-Cantidad de Horas

Teóricas: 4
Práctica: 2

- MODALIDAD:

Presencial

- DESTINATARIOS:

Personal No Docente de la Universidad

- CANTIDAD MÁXIMA DE ASISTENTES:

35 personas

- CANTIDAD MÍNIMA DE ASISTENTES:

15 personas

- REQUISITOS PARA EL CURSADO:

Haber concurrido a las charlas en seguridad de la información, dentro del programa de capacitación interna para el personal no docente de la UNLu.

- CANTIDAD DE ENCUENTROS:

3 encuentros en Sede Central, de 2 horas de duración cada uno.

UNIV. NAC. DE LUJAN
FOLIO
425
M.G.E.S.Y.A.

- RECURSOS NECESARIOS:

PC con conexión a internet
Proyector
Lápices y hojas de papel

-OBJETIVOS:

Dar a conocer, dentro del marco de la psicología de la seguridad informática, la actitud de los usuarios frente a los riesgos percibidos y los riesgos reales a los que están expuestos los activos de seguridad de la información.
La actividad de taller tiene el propósito de brindar a los usuarios una visión general de la identificación y valoración de los riesgos a los que se exponen los activos de información según la subjetividad humana y según los procedimientos de seguridad informática.

- CONTENIDOS A DESARROLLAR:

-Seminario:

-La seguridad y el conocimiento convencional sobre el riesgo.
-Seguridad de la información.
-Concepto de activo de información, vulnerabilidad, amenaza, riesgo, daño.
-Concepto de integridad, confidencialidad y disponibilidad de los activos de información.
-Percepciones y realidades del riesgo.
-Aspectos contemplados por las personas para realizar concesiones en seguridad.
-El riesgo y el cerebro.
-Factores que afectan el riesgo:heurísticas y optimismo.
-Análisis de riesgo.

-Taller:

-Formar grupos (máximo 5 personas).
-Identificar entre 10 y 15 activos de información (críticos y no críticos) del lugar de trabajo de los participantes.
-Valorar los activos identificados.
-Identificar posibles vulnerabilidades de los activos.
-Identificar amenazas (naturales o humanas, intencionales o no) a la integridad, confidencialidad y disponibilidad de esos activos de información.
-Valorar los riesgos.
-Discusión de los casos planteados por cada grupo.

- FORMA DE EVALUACIÓN.

La instancia de evaluación se cumple mediante la actividad de taller.

UNIV. NAC. DE LUJAN
FOLIO
426
M.G.E.S.Y.A.

- BIBLIOGRAFIA

Modelo de Política de Seguridad de la Información . ONTI. Año 2005

"La Psicología de la seguridad". Bruce Schneier (2007). Paper traducido por seguridaddigital.info con la autorización de Bruce Schneier. La versión original puede encontrarse en inglés en: http://www.schneier.com/essay-155.html

- La documentación para los asistentes se encuentra disponible en el sitio web del Departamento de Seguridad Informática: http://www.seguridadinformatica.unlu.edu.ar