

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

**FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN  
CCPG1003 – INFORMATION ASSURANCE AND SECURITY  
EXAMEN 2 - SEGUNDA EVALUACIÓN - II TÉRMINO 2016-2017/ Febrero 17, 2017**

**Nombre:** \_\_\_\_\_ **Matrícula:** \_\_\_\_\_

COMPROMISO DE HONOR: Al firmar este compromiso, reconozco que el presente examen está diseñado para ser resuelto de manera individual, que puedo usar un lápiz o esferográfico; que sólo puedo comunicarme con la persona responsable de la recepción del examen; y, cualquier instrumento de comunicación que hubiere traído, debo apagarlo y depositarlo en la parte anterior del aula, junto con algún otro material que se encuentre acompañándolo. Además, no debo usar calculadora alguna, consultar libros, notas, ni apuntes adicionales a los que se entreguen en esta evaluación. Los temas debo desarrollarlos de manera ordenada.  
Firmo el presente compromiso, como constancia de haber leído y aceptado la declaración anterior. "Como estudiante de ESPOL me comprometo a combatir la mediocridad y actuar con honestidad, por eso no copio ni dejo copiar".

\_\_\_\_\_  
Firma

**Tiempo de duración: 2 horas**

**Tema 1 (12 puntos)**

Responda a las siguientes preguntas de opción múltiple:

1. ¿Cuál de los siguientes ejemplos constituye un "acto deliberado de violación a la privacidad de las personas"?
  - a. Error humano
  - b. Ataque DDoS
  - c. Shoulder surfing
  - d. Extorsión
  
2. ¿Cuál es el objetivo de la fase de Mantenimiento en un proceso de desarrollo de una política de seguridad?
  - a. Distribuir adecuadamente la política dentro de la organización
  - b. Revisar los documentos de política en la fecha de revisión especificada
  - c. Redactar una propuesta a la dirección en la que se indiquen los objetivos de la política
  - d. Presentar el documento a un organismo de aprobación
  
3. ¿Cuál de los siguientes es un término legal que describe cuando una compañía (o individuo) toma acciones razonables relacionadas con la seguridad para evitar la responsabilidad legal?
  - a. Benchmarking
  - b. Best practice
  - c. Due care
  - d. Gold standard
  
4. ¿Cuál de las siguientes políticas especifica que dos sitios web no deberían interferir entre ellos, al menos que ambos lo deseen?
  - a. Seguridad para VPN
  - b. Extranet
  - c. Acceptable encryption
  - d. Mismo origen

## Tema 2 (18 puntos)

Conteste a las siguientes preguntas de respuestas múltiples y *justifique en máximo 5 líneas* sus respuestas.

1. Suponga que implementa un servicio Web enteramente en Java y que el entorno de Java no tiene errores. Si para sus consultas a la base de datos tiene cuidado de utilizar siempre declaraciones preparadas, seleccione **todos** los tipos de ataques para los cuales usted siente certeza de estar protegido.
  - a. Buffer overflow
  - b. Cross-Site Request Forgery (CSRF)
  - c. SQL injection
  - d. XSS
  
2. Suponga que un desarrollador implementa un navegador web completo en Java. El navegador no utiliza una base de datos, y nuevamente asuma que no hay defectos en el entorno Java. Seleccione **todos** los tipos de ataques para los cuales usted siente certeza de estar protegido.
  - a. Buffer overflow
  - b. Cross-Site Request Forgery (CSRF)
  - c. SQL injection
  - d. XSS