Universidad de Buenos Aires - Facultad de Ciencias Económicas - Gestion de Tecnologías Digitales
Profesor: Aníbal M. Mazza Fraquelli - SEGUNDO Parcial - Cuatrimestre 01-2026

Registro _____ Apellidos y nombres _____

Responda la siguientes preguntas. LEA adecuadamente la consigna y FUNDAMENTE su respuesta.

1. Un administrador de sistemas recibe accesos amplios para ejecutar un proyecto temporal, y al finalizar este conserva esos permisos durante meses. Explique qué principio de seguridad se está incumpliendo y cómo debería procederse.

2. Una entidad bancaria necesita identificar movimientos de cuenta que se aparten de los patrones habituales de cada cliente. Proponga un control adecuado, clasifíquelo según su naturaleza y mencione dos ejemplos concretos del mismo tipo.

3. Tras una corrupción de la base de datos, el área de sistemas restablece la operación a partir de la última copia íntegra disponible. Indique qué tipo de control se aplicó y cuál es su objetivo específico.

4. Un atacante logra modificar los importes registrados en las facturas almacenadas. Indique qué pilar de la tríada de seguridad (Confidencialidad, Integridad, Disponibilidad) se vio comprometido y qué medida lo habría protegido.

5. Luego de una campaña de correos fraudulentos simulados, una organización evalúa qué tan preparado está su personal. Explique qué papel cumple la concientización en la gestión de la seguridad y de qué manera podría medirse su efecto en este caso.

6. Para retirar dinero, un cliente utiliza su tarjeta, ingresa una clave personal y apoya su dedo en un lector. Identifique a qué factor de autenticación corresponde cada uno de estos elementos.

7. Una empresa afirma cumplir con una buena práctica de respaldo porque guarda tres copias de su información, aunque todas ellas residen en el mismo servidor. Indique si efectivamente cumple con la estrategia 3-2-1 y cómo debería corregirse el esquema.

8. Un corte eléctrico prolongado deja sin energía las instalaciones de un centro de atención telefónica que debe seguir respondiendo a sus clientes. Explique qué prevé el Plan de Continuidad del Negocio (Business Continuity Plan) para sostener la operación en estas condiciones.

9. Un especialista detecta una falla de seguridad en un sistema, la informa al fabricante y no la aprovecha. Otra persona descubre una falla similar y la utiliza para sustraer información. Distinga ambas conductas y vincúlelas con los conceptos de hacking y cracking.

10. En un equipo de desarrollo, la misma persona programa los cambios y los pone en producción sin que medie una revisión por parte de un tercero. Indique qué principio de control se está vulnerando y por qué resulta riesgoso.

11. Una persona recibe una llamada de alguien que dice pertenecer al área de soporte técnico y le solicita sus credenciales para "resolver un incidente". Identifique el tipo de amenaza involucrada y qué defensa correspondería.

12. Luego de detectar la presencia de un programa malicioso, el equipo de sistemas lo elimina y aplica una actualización que cierra la vulnerabilidad que permitió su ingreso. Indique qué tipo de control representa esta acción y en qué momento del incidente interviene.

13. Antes de salir a producción, se necesita verificar que un sistema sea capaz de sostener diez mil usuarios conectados de forma simultánea sin degradar su rendimiento. Indique qué tipo de prueba corresponde realizar y por qué.

14. Un proyecto avanza directamente desde el análisis hacia la puesta en producción, sin atravesar la etapa de pruebas. En el marco del ciclo de vida de los sistemas, indique qué etapa se omitió y qué riesgo se asume.

15. Un producto estándar de gestión no contempla un proceso específico y particular de la empresa que lo adquiere. Indique qué análisis permite identificar esa brecha (Fit-Gap) y qué opciones surgen para resolverla.

16. Un área usuaria solicita modificar el código de un software estándar para obtener un reporte a la medida de sus necesidades. Analice una ventaja y una desventaja de avanzar con esa customización.

17. A pocos días de la puesta en producción, distintas áreas continúan solicitando cambios sobre el alcance del sistema. Indique qué medida corresponde aplicar y fundamente su utilidad.

18. Un proveedor cumple con la disponibilidad comprometida del servicio, pero los usuarios se quejan de que el sistema responde con lentitud. Indique qué tipo de acuerdo aborda específicamente esta dimensión del rendimiento y en qué se distingue del acuerdo de nivel de servicio.

19. El servidor que aloja la base de datos de una empresa se encuentra accesible de forma directa desde internet, sin ninguna capa intermedia de protección. Explique cómo se aplicaría el principio de mínima exposición para corregir esta situación.

20. Un centro de datos presenta acceso libre del personal y carece de control de temperatura y de protección contra incendios. Proponga dos controles físicos adecuados y justifique su pertinencia.

Universidad de Buenos Aires - Facultad de Ciencias Económicas - Gestion de Tecnologías Digitales
Profesor: Aníbal M. Mazza Fraquelli - SEGUNDO Parcial - Cuatrimestre 01-2026

Registro _____ Apellidos y nombres _____

Responda la siguientes preguntas. LEA adecuadamente la consigna y FUNDAMENTE su respuesta.

1. El servidor que aloja la base de datos de una empresa se encuentra accesible de forma directa desde internet, sin ninguna capa intermedia de protección. Explique cómo se aplicaría el principio de mínima exposición para corregir esta situación.

2. Luego de detectar la presencia de un programa malicioso, el equipo de sistemas lo elimina y aplica una actualización que cierra la vulnerabilidad que permitió su ingreso. Indique qué tipo de control representa esta acción y en qué momento del incidente interviene.

3. Una organización elabora una política de uso aceptable de los recursos informáticos y capacita a su personal sobre ella. Indique a qué categoría de control corresponde esta iniciativa y fundamente la clasificación.

4. La nómina de clientes de una empresa termina en manos de un competidor. Indique qué pilar de la tríada de seguridad (Confidencialidad, Integridad, Disponibilidad) se vio afectado y proponga una medida preventiva que lo habría evitado.

5. Al finalizar su jornada, un empleado deja la sesión de su equipo abierta y notas con datos sensibles sobre el escritorio. Relacione esta conducta con la noción de factor humano y con las políticas de seguridad que deberían aplicarse.

6. Una empresa almacena las plantillas biométricas del iris de sus empleados sin aplicarles ningún tipo de cifrado. Identifique el riesgo legal que esto implica y qué control debería incorporarse.

7. Un sistema crítico debe poder volver a estar operativo en un máximo de dos horas y la organización no puede permitirse perder más de quince minutos de información ante una contingencia. Explique cómo se traducen estas exigencias en el diseño del Plan de Recuperación ante Desastres.

8. Una organización necesita restaurar su información lo más rápido posible y, de ser posible, con un único conjunto de respaldo adicional a la copia base. Indique qué tipo de copia conviene utilizar (diferencial o incremental) y justifique la decisión.

9. Una empresa utiliza un software sin actualizar desde hace tiempo, y un atacante recorre la red en busca de sistemas con esa falla. Distinga, en este caso concreto, qué constituye la vulnerabilidad y qué constituye la amenaza.

10. Una organización debe priorizar la atención de sus riesgos: uno es muy poco probable pero de impacto catastrófico, y otro es frecuente pero de impacto leve. Explique cómo deberían ponderarse considerando la relación entre probabilidad e impacto.

11. Una persona accede sin autorización a la casilla de correo electrónico de otra y revisa su contenido. Indique a qué marco corresponde en términos de la seguridad de la información.

12. Antes de salir a producción, se necesita verificar que un sistema sea capaz de sostener diez mil usuarios conectados de forma simultánea sin degradar su rendimiento. Indique qué tipo de prueba corresponde realizar y por qué.

13. Un auditor de sistemas examina directamente el código fuente que implementa los controles internos de una aplicación. Indique a qué tipo de auditoría corresponde este abordaje (caja blanca o caja negra) y fundamente.

14. En el marco de una auditoría, se verifica el saldo real de una cuenta confrontándolo con la documentación de respaldo. Explique qué se evalúa mediante una prueba sustantiva en este caso.

15. Una organización encara un proyecto de gran envergadura y alto riesgo, que requiere evaluar y atender los riesgos en cada ciclo de avance antes de continuar. Indique qué metodología de gestión resulta apropiada y por qué.

16. Un proyecto cuenta con una lista de cincuenta requisitos y un plazo que no permite abordarlos todos. Explique cómo se priorizarían aplicando la técnica MoSCoW.

17. Tras una experiencia desfavorable con un proveedor externo, una empresa decide reconstruir internamente la capacidad de desarrollo que había tercerizado. Indique qué estrategia de aprovisionamiento representa esta decisión y qué implica.

18. Una empresa contrata un servicio de software en la nube en modalidad de software como servicio (Software as a Service). Analice quién resulta responsable de la seguridad de los datos que el cliente carga en la plataforma.

19. Un cambio urgente se aplica directamente sobre el sistema en producción sin pasar por ningún proceso de aprobación. Indique el riesgo que esto genera y cuál sería el proceso correcto de gestión de cambios.

20. Una vez estabilizado el nuevo sistema, su operación deja de gestionarse como un proyecto y pasa a formar parte de la rutina diaria. Explique qué se entiende por operación habitual (Business As Usual) y qué cambia respecto de la etapa anterior.

Universidad de Buenos Aires - Facultad de Ciencias Económicas - Gestion de Tecnologías Digitales
Profesor: Aníbal M. Mazza Fraquelli - SEGUNDO Parcial - Cuatrimestre 01-2026

Registro _____ Apellidos y nombres _____

Responda la siguientes preguntas. LEA adecuadamente la consigna y FUNDAMENTE su respuesta.

1. En un sistema, un mismo usuario posee un perfil que le permite solicitar nuevos accesos y, a la vez, aprobarlos. Explique cómo se articulan los principios de mínimos privilegios y de segregación de funciones para corregir esta situación.

2. Una empresa busca tanto impedir como detectar los accesos indebidos a su red interna. Proponga un control preventivo y un control detectivo apropiados para cada objetivo, e indique a qué momento del incidente responde cada uno.

3. Frente a un ataque, una organización aísla el sistema afectado, luego restaura la información desde sus respaldos y, finalmente, corrige la vulnerabilidad que lo originó. Clasifique cada una de las tres acciones según el tipo de control que representa.

4. Un ataque de denegación de servicio satura el sitio de una empresa y lo deja fuera de línea durante horas. Indique qué pilar de la tríada de seguridad (Confidencialidad, Integridad, Disponibilidad) resulta afectado y proponga una medida de mitigación.

5. En una organización se observa que el personal reutiliza las mismas contraseñas en distintos sistemas internos y externos. Explique cómo debería abordarse este problema desde la concientización y desde las políticas de seguridad.

6. Una política obliga a cambiar la contraseña todos los meses exigiendo combinaciones complejas, y como resultado los usuarios terminan anotándolas en papel. Analice si la política es efectiva y proponga una alternativa.

7. Diseñe un esquema de respaldo conforme a la estrategia 3-2-1 para una pequeña empresa, describiendo cómo se distribuirían las copias y por qué esa distribución resulta una buena práctica.

8. Un incendio afecta simultáneamente las oficinas donde trabaja el personal y la sala de servidores de una compañía. Distinga qué aspectos del problema atiende el Plan de Continuidad del Negocio y cuáles atiende el Plan de Recuperación ante Desastres.

9. Un programa malicioso cifra los archivos de una organización y exige un rescate económico para devolver el acceso. Identifique el tipo de software malicioso involucrado y qué control de tipo recuperatorio reduciría su impacto.

10. En una caja, una misma persona registra los movimientos, los concilia y los autoriza. Indique qué principio de control se vulnera y proponga un rediseño del circuito.

11. Una persona recibe una llamada de alguien que dice pertenecer al área de soporte técnico y le solicita sus credenciales para "resolver un incidente". Identifique el tipo de amenaza involucrada y qué defensa correspondería.

12. Antes de salir a producción, se necesita verificar que un sistema sea capaz de sostener diez mil usuarios conectados de forma simultánea sin degradar su rendimiento. Indique qué tipo de prueba corresponde realizar y por qué.

13. Una persona prueba un formulario de carga de datos sin conocer la lógica interna del programa, evaluando únicamente las salidas frente a distintas entradas. Indique qué técnica de prueba está aplicando y qué busca verificar.

14. Durante el desarrollo de un sistema, el programador comete una equivocación en el código, lo que provoca que el programa deje de calcular correctamente un total y que el usuario observe un resultado incorrecto en pantalla. Distinga, en este caso, qué constituye el error, qué la falla y qué el defecto.

15. Un producto se entrega a los usuarios con una cantidad elevada de defectos que afectan su uso. Explique qué función cumple el aseguramiento de la calidad (Quality Assurance) y cómo habría contribuido a prevenir esta situación.

16. Antes de liberar una nueva versión a la totalidad de los usuarios, una empresa decide habilitarla primero a un pequeño porcentaje de ellos. Indique qué estrategia de despliegue representa esta decisión y qué ventaja ofrece.

17. Una organización debe trasladar la información de un sistema antiguo a uno nuevo, con riesgo de pérdida o inconsistencia de datos. Indique qué proceso corresponde a esta tarea y qué cuidados deberían tomarse.

18. Inmediatamente después de la puesta en producción de un sistema, comienzan a aparecer incidencias que requieren atención intensiva. Indique a qué etapa corresponde este período y qué implica para el equipo.

19. Un proveedor no cumple con el tiempo de respuesta ante incidentes que había acordado con su cliente. Explique qué establece el acuerdo de nivel de servicio (Service Level Agreement) y qué corresponde frente al incumplimiento.

20. Una organización carece de políticas claras y de un tono ético definido desde la dirección, lo que se refleja en prácticas informales en todos sus niveles. Explique qué se entiende por ambiente de control y por qué en este caso resulta deficiente.

Universidad de Buenos Aires - Facultad de Ciencias Económicas - Gestion de Tecnologías Digitales
Profesor: Aníbal M. Mazza Fraquelli - SEGUNDO Parcial - Cuatrimestre 01-2026

Registro _____ Apellidos y nombres _____

Responda la siguientes preguntas. LEA adecuadamente la consigna y FUNDAMENTE su respuesta.

1. El servidor que aloja la base de datos de una empresa se encuentra accesible de forma directa desde internet, sin ninguna capa intermedia de protección. Explique cómo se aplicaría el principio de mínima exposición para corregir esta situación.

2. En una organización conviven controles que actúan antes de que ocurra un incidente, otros durante su transcurso y otros con posterioridad. Ubique un control para cada uno de esos momentos y clasifíquelo según corresponda.

3. Una organización elabora una política de uso aceptable de los recursos informáticos y capacita a su personal sobre ella. Indique a qué categoría de control corresponde esta iniciativa y fundamente la clasificación.

4. Describa una situación de seguridad en la que se vean comprometidos de manera simultánea los tres pilares de la tríada (Confidencialidad, Integridad, Disponibilidad) e identifique cómo se afecta cada uno.

5. Un empleado disconforme con la organización decide filtrar información confidencial a la que tiene acceso por su función. Clasifique esta amenaza según su origen y su intencionalidad, e indique qué control habría reducido el riesgo.

6. Un sistema utiliza únicamente la huella dactilar como único medio para autenticar a los usuarios. Analice el riesgo de depender de un solo factor y recomiende una mejora basada en la autenticación de múltiples factores (Multi-Factor Authentication).

7. Un sistema de pequeño tamaño cuenta con espacio de almacenamiento suficiente y prioriza que la restauración sea lo más simple y directa posible. Indique qué tipo de copia de respaldo conviene utilizar y por qué.

8. Una organización elaboró su Plan de Recuperación ante Desastres pero nunca lo puso a prueba. Explique el riesgo que esto implica y qué buena práctica debería adoptarse.

9. Ante una vulnerabilidad detectada, un parche correctivo se aplica de manera urgente (hot-fix) y directa sobre el ambiente de producción. Indique el riesgo de este proceder y cómo deberían gestionarse las correcciones y parches de emergencia.

10. En el área de tecnología, un único administrador posee acceso total a todos los sistemas, sin ningún tipo de límite ni separación de responsabilidades. Explique cómo se aplicarían los principios de mínimos privilegios y de segregación de funciones para corregirlo.

11. La dirección de una empresa considera que la seguridad de la información se resuelve simplemente con la compra de un programa antivirus. Explique por qué este enfoque es insuficiente y qué abarca realmente la ciberseguridad.

12. Antes de salir a producción, se necesita verificar que un sistema sea capaz de sostener diez mil usuarios conectados de forma simultánea sin degradar su rendimiento. Indique qué tipo de prueba corresponde realizar y por qué.

13. Una organización debe distinguir entre una revisión realizada por su propio equipo y otra realizada por un tercero independiente. Diferencie, en este caso, una auditoría interna de una auditoría externa.

14. Un sistema debe cumplir estas exigencias: "emitir facturas a los clientes", "tener actualizadas las cuentas corrientes", "saber lo límites de crédito" y "responder a cada consulta en menos de dos segundos". Clasifique cada una como requisito funcional o no funcional y fundamente.

15. Un producto se entrega a los usuarios con una cantidad elevada de defectos que afectan su uso. Explique qué función cumple el aseguramiento de la calidad (Quality Assurance) y cómo habría contribuido a prevenir esta situación.

16. Un área solicita la aprobación de un proyecto sin presentar una justificación de sus costos ni de sus beneficios esperados. Indique qué documento falta y para qué sirve.

17. Un proyecto comienza a ejecutarse sin una reunión inicial que alinee a los participantes y defina expectativas. Indique qué actividad se omitió y qué consecuencia puede tener.

18. Una organización debe capacitar a quinientos usuarios sobre un nuevo sistema, pero dispone de recursos limitados de instrucción. Indique qué estrategia de capacitación resulta conveniente y por qué.

19. Un cambio urgente se aplica directamente sobre el sistema en producción sin pasar por ningún proceso de aprobación. Indique el riesgo que esto genera y cuál sería el proceso correcto de gestión de cambios.

20. En el control de accesos de una empresa coexisten una norma que define quién puede ingresar a cada área y un mecanismo informático que valida las credenciales. Distinga, en este caso, a qué tipo de seguridad corresponde.