**Pauta de Evaluación Sumativa**

| **Nombre** | *Estudiante o Integrantes de un equipo de trabajo* | | |
| --- | --- | --- | --- |
| **Sección** |  | **Fecha** |  |

| **Categoría** | **% Logro** | **Puntaje** | **Descripción** |
| --- | --- | --- | --- |
| Excelente Dominio (ED) | 100% | 7 | Dominio esperado para el indicador, se considera como el punto óptimo para cualificar como competente. |
| Alto dominio (AD) | 80% | 5.6 | Se observan pequeñas dificultades o errores para el completo dominio del indicador. |
| Dominio Aceptable (DA) | 60% | 4.2 | Suficiencia de logro en el dominio del indicador, se considera como el mínimo aceptable para cualificar como competente. |
| Dominio en Proceso (DP) | 30% | 2.1 | Se observan varias dificultades o errores para el dominio del indicador. |
| Dominio por conseguir (DC) | 0% | 1 | Se observan un escaso, nulo o incorrecto dominio del indicador. |

1. **PAUTA DE EVALUACIÓN.**

| **Indicadores de logro** | **NIVELES Y PORCENTAJE DE LOGRO** | | | | |
| --- | --- | --- | --- | --- | --- |
| **ED**  **100%** | **AD**  **80%** | **DA**  **60%** | **DP**  **30%** | **DC**  **0%** |
| **Dimensión I: Políticas de seguridad en desarrollo de código seguro** | | | | | |
| 1. Realiza políticas de seguridad en desarrollo de código seguro y el uso de este, basada en un texto cohesionado que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. | **7 puntos** | **5.6 puntos** | **4.2 puntos** | **2.1 puntos** | **0 puntos** |
| Realiza correctamente las políticas de seguridad en desarrollo de código seguro y el uso de este, basada en un texto cohesionado que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. | Realiza mayoritariamente políticas de seguridad en desarrollo de código seguro y el uso de este, basada en un texto cohesionado que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. | Realiza en mediano alcance políticas de seguridad en desarrollo de código seguro y el uso de este, basada en un texto cohesionado que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. | Realiza vagamente políticas de seguridad en desarrollo de código seguro y el uso de este, basada en un texto cohesionado que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. | No realiza políticas de seguridad en desarrollo de código seguro y el uso de este, basada en un texto cohesionado que le permita sensibilizar al cliente o usuario respecto del marco de trabajo para la organización. |
| 1. Es capaz de levantar los requerimientos y procesos necesarios desde la organización para el desarrollo de políticas de ciber seguridad. | **7 puntos** | **5.6 puntos** | **4.2 puntos** | **2.1 puntos** | **0 puntos** |
| Es capaz de levantar completamente los requerimientos y procesos necesarios desde la organización para el desarrollo de políticas de ciber seguridad. | Es capaz de levantar mayoritariamente los requerimientos y procesos necesarios desde la organización para el desarrollo de políticas de ciber seguridad. | Es capaz de levantar medianamente los requerimientos y procesos necesarios desde la organización para el desarrollo de políticas de ciber seguridad. | Es capaz de levantar vagamente los requerimientos y procesos necesarios desde la organización para el desarrollo de políticas de ciber seguridad. | No es capaz de levantar los requerimientos y procesos necesarios desde la organización para el desarrollo de políticas de ciber seguridad. |
| 1. Reconoce las políticas relacionadas con la ciber seguridad como mecanismo para ser aplicado en la organización. | **7 puntos** | **5.6 puntos** | **4.2 puntos** | **2.1 puntos** | **0 puntos** |
| Reconoce completamente las políticas relacionadas con la ciber seguridad como mecanismo para ser aplicado en la organización. | Reconoce mayoritariamente las políticas relacionadas con la ciber seguridad como mecanismo para ser aplicado en la organización. | Reconoce medianamente las políticas relacionadas con la ciber seguridad como mecanismo para ser aplicado en la organización. | Reconoce vagamente las políticas relacionadas con la ciber seguridad como mecanismo para ser aplicado en la organización. | No Reconoce las políticas relacionadas con la ciber seguridad como mecanismo para ser aplicado en la organización. |
| 1. Reconoce los estándares y buenas prácticas asociadas a ciberseguridad, necesarias para el desarrollo de código seguro. | **7 puntos** | **5.6 puntos** | **4.2 puntos** | **2.1 puntos** | **0 puntos** |
| Reconoce los completamente estándares y buenas prácticas asociadas a ciberseguridad, necesarias para el desarrollo de código seguro. | Reconoce mayoritariamente los estándares y buenas prácticas asociadas a ciberseguridad, necesarias para el desarrollo de código seguro. | Reconoce medianamente los estándares y buenas prácticas asociadas a ciberseguridad, necesarias para el desarrollo de código seguro. | Reconoce los vagamente estándares y buenas prácticas asociadas a ciberseguridad, necesarias para el desarrollo de código seguro. | No reconoce los estándares y buenas prácticas asociadas a ciberseguridad, necesarias para el desarrollo de código seguro. |
| 1. Es autocrítico en la revisión del cumplimiento de las normas y buenas prácticas en el ámbito de ciber seguridad. | **7 puntos** | **5.6 puntos** | **4.2 puntos** | **2.1 puntos** | **0 puntos** |
| Es autocrítico en la revisión del cumplimiento de las normas y buenas prácticas en el ámbito de ciber seguridad. | N/A | N/A | N/A | Es autocrítico en la revisión del cumplimiento de las normas y buenas prácticas en el ámbito de ciber seguridad. |