**PRUEBA DE LA CAJA NEGRA – POST TEST**

1. **DATOS GENERALES**

|  |  |
| --- | --- |
| **INDICADOR** | Seguridad del proceso de transferencias interbancarias |
| **TIPO** | POSTEST |
| **DEFINICIÓN** | La prueba de caja negra es una técnica donde se busca la verificación de las funcionalidades del software sin tomar como referencia la estructura del código interno. |
| **DESCRIPCIÓN** | El objetivo es verificar que la transacción sea firmada digitalmente, y que los datos transmitidos no hayan sido alterados. Para ello, el API REST utiliza un HSM que valida tanto la firma como el contenido de cada petición. |
| **VALIDADOR** | Mamani Jiménez, Richard Walter |
| **FECHA** | 01/08/2025 |

1. **CASOS DE PRUEBA**

|  |  |
| --- | --- |
| **SEGURIDAD** | CP01. Validación de transacción mediante firma digital |

1. **RESULTADO ESPERADO**

|  |  |
| --- | --- |
| **SEGURIDAD** | El proceso de transferencias interbancarias debe demostrar la seguridad con la que cuenta el API REST para realizar la validación mediante firma digital. |

1. **REALIZACIÓN DE PRUEBA**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre** | Validación de transacción mediante firma digital | **Código de caso de prueba** | **CP01** |
| **Propósito** | Validar que, la transacción haya sido firmada digitalmente y los datos que se envíen o se reciben no hayan sido alterados, para ello el API REST utiliza el HSM para verificar la firma digital y el contenido de la petición. | | |
| **Pre requisito** | Se requiere que previamente se haya importado de Firma Digital en el HSM. | | |
| **Pasos** | 1. Tener una transacción con el formato definido y firmado digital | | |
| **Softwares implicados** | API REST, HSM | | |
| **Ruta** | **Entrada / Acción / Condición** | **Salida esperada** | **Estado** |
| /api/pinoperaciones/desencriptacioncce  Método: POST  SOFTWARE:  API REST | {   "payload":"",   "protected":"eyJhbGciOiJSUzI1NiIsIng1dCI6IjdJTFpDeGF4aTVGTEpoaHYxalZRdEZuSnZWZyJ9",    "signature":"d0438FLIB\_47yfSNt-Ms5X0\_DQ\_oKjXmHcpsaGrTkBTskaUNn3UaGBjHkSe2PH2yki9xjL4wFA4l-0\_qFrqBdnPt-S3H-UMv3Q3yZKrtn8GjdVsDA2WBgINvLfxeoDZdhw5UgsN6gdjrxGfs9hY-F1eDOF\_MnR3jhfB\_B4FnRulLDpwFD3SEe5J\_-boJSIdnqDXDH2YmoAHKur\_fMgSd06R2kOrXPy6FOmWsdom0vrAIkYLkiyqn4umltt1Gb-Gp7PVJJNt3XWlApE\_uIsPyj-orb\_f8CIVCM3LeXxgBn\_iK3qVfV\_6H7gZzYfreY0OyjX-gJkFFBXawSQLC6YaJ3w"  } | El API REST en su endpoint de validación responde con código 200 y la trama desencriptada indicando que está correcto:  {      "codigo": **null**,      "mensaje": **null**,      "datos": {          "resultado": "1",          "mensaje": "{\"AV2\":{\"debtorParticipantCode\":\"0813\",\"creditorParticipantCode\":\"0813\",\"creationDate\":\"20241104\",\"creationTime\":\"180405\",\"terminalId\":\"ABC00001\",\"retrievalReferenteNumber\":\"110418040571\",\"trace\":\"000204\",\"debtorId\":\"78956325\",\"debtorIdCode\":\"2\",\"transactionType\":\"320\",\"channel\":\"15\",\"creditorCCI\":\"81300121110200937057\",\"debtorTypeOfPerson\":\"N\",\"currency\":\"604\",\"instructionId\":\"2024110418040508138115000204\",\"branchId\":\"0813\"}}"      }  } |  |
| /api/pinoperaciones/desencriptacioncce  Método: POST  SOFTWARE:  API REST | {    "payload":"",    "protected":"eyJhbGciOiJSUzI1NiIsIng1dCI6IjdJTFpDeGF4aTVGTEpoaHYxalZRdEZuSnZWZyJ9",    "signature":"d0438FLIB\_47yfSNt-Ms5X0\_DQ\_oKjXmHcpsaGrTkBTskaUNn3UaGBjHkSe2PH2yki9xjL4wFA4l-0\_qFrqBdnPt-S3H-UMv3Q3yZKrtn8GjdVsDA2WBgINvLfxeoDZdhw5UgsN6gdjrxGfs9hY-F1eDOF\_MnR3jhfB\_B4FnRulLDpwFD3SEe5J\_-boJSIdnqDXDH2YmoAHKur\_fMgSd06R2kOrXPy6FOmWsdom0vrAIkYLkiyqn4umltt1Gb-Gp7PVJJNt3XWlApE\_uIsPyj-orb\_f8CIVCM3LeXxgBn\_iK3qVfV\_6H7gZzYfreY0OyjX-gJkFFBXawSQLC6YaJ3w"  } | El API REST en su endpoint de validación responde con código 200, pero indica en el json el código de error:  {      "codigo": **null**,      "mensaje": **null**,      "datos": {          "resultado": "0",          "mensaje": "ERR3"      }  } |  |







